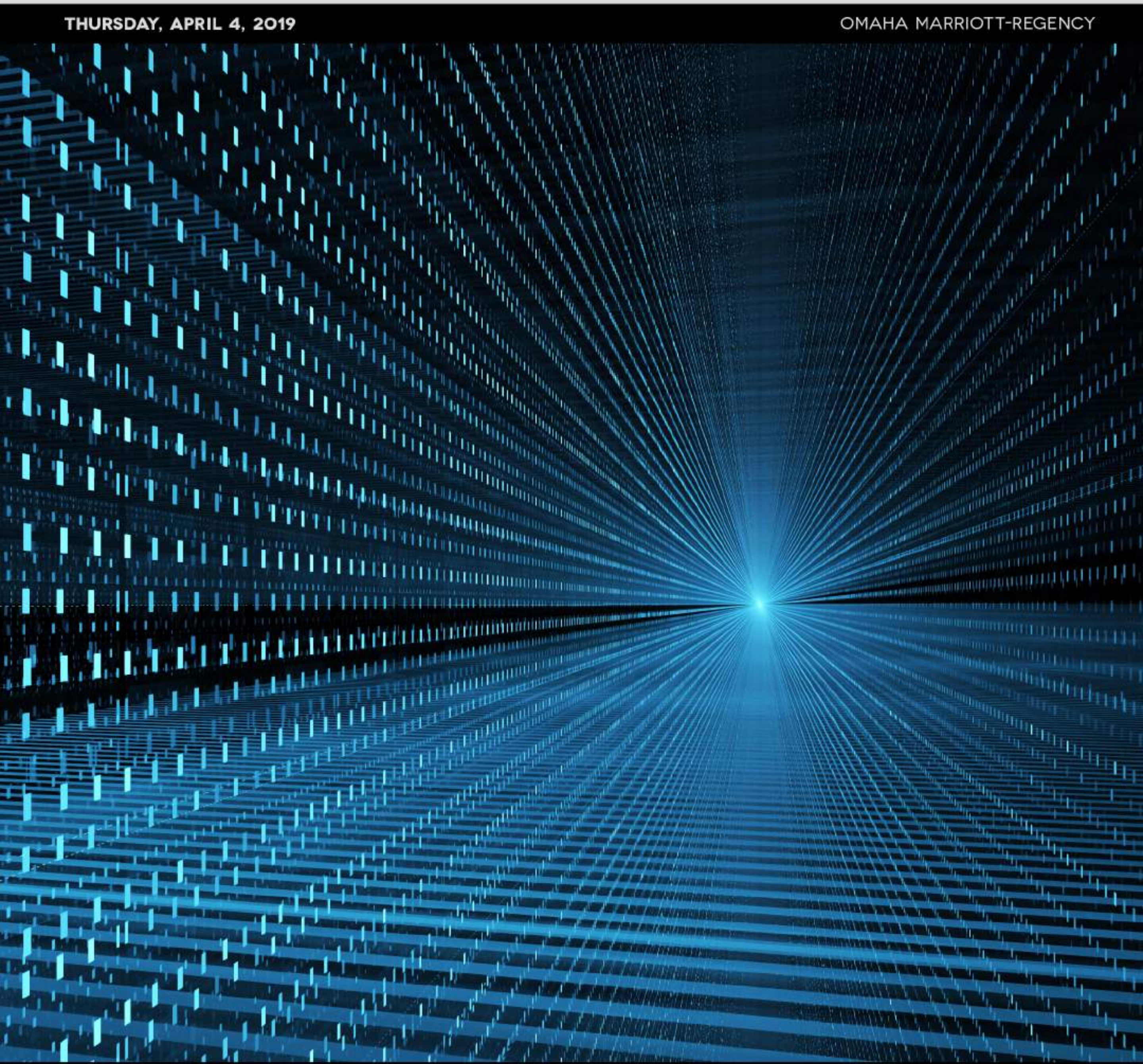
BAIRD HOLM LLP
TECHNOLOGY & DATA PROTECTION FORUM 2019

THURSDAY, APRIL 4, 2019

OMAHA MARRIOTT-REGENCY



BAIRDHOLM LLP
ATTORNEYS AT LAW

1700 FARNAM STREET, SUITE 1500 · OMAHA, NE 68102 · WWW.BAIRDHOLM.COM

Around the Data Protection World in 90 Minutes

Grayson J. Derrick, AriAnna C. Goldstein, Abigail T. Mohs and Sean T. Nakamoto

Data Protection

AROUND THE WORLD IN NINETY MINUTES

Grayson J. Derrick AriAnna C. Goldstein

Abigail T. Mohs Sean T. Nakamoto

BH | BAIRDHOLM

Itinerary

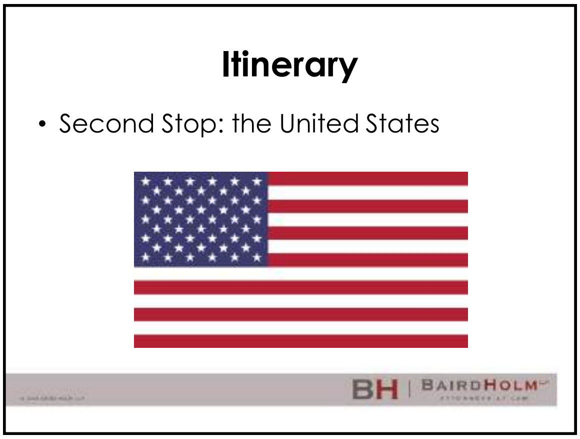
- First Stop: the European Union

BH | BAIRDHOLM

Itinerary

- Quick Detour

BH | BAIRDHOLM



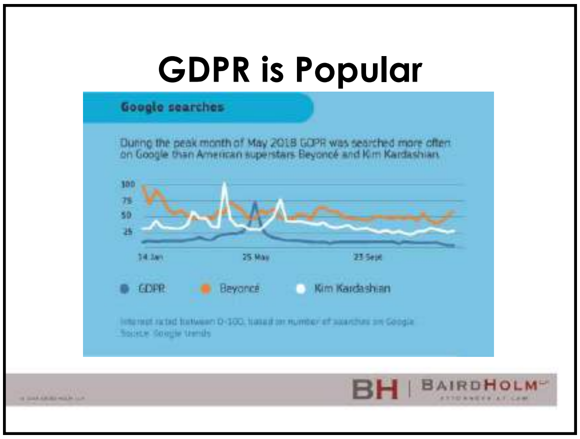
Itinerary

- Second Stop: the United States

Itinerary

- Final Stop: Nebraska

First Stop: The European Union and the GDPR

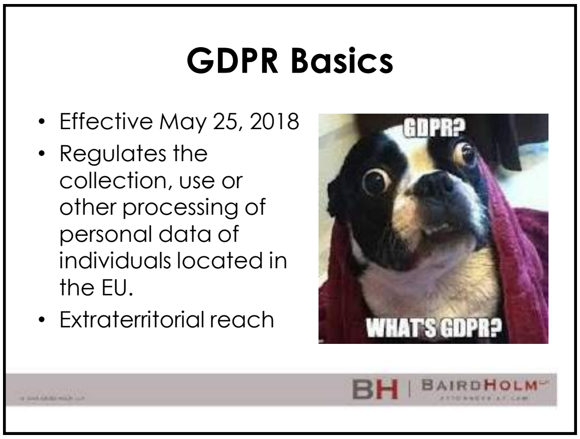


GDPR is Popular

Google searches

During the peak month of May 2018 GDPR was searched more often on Google than American superstars Beyoncé and Kim Kardashian.

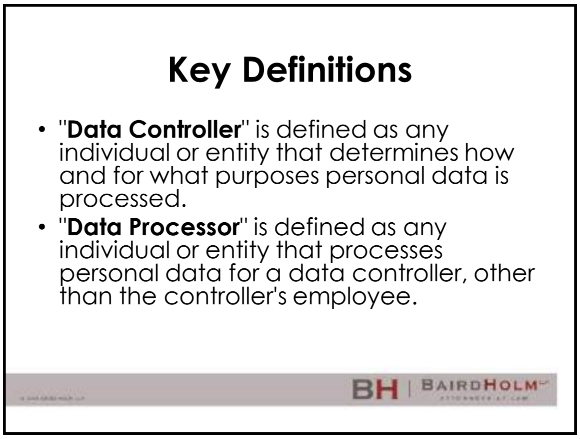
Interest rated between 0-100, based on number of searches on Google
Source: Google trends



GDPR Basics

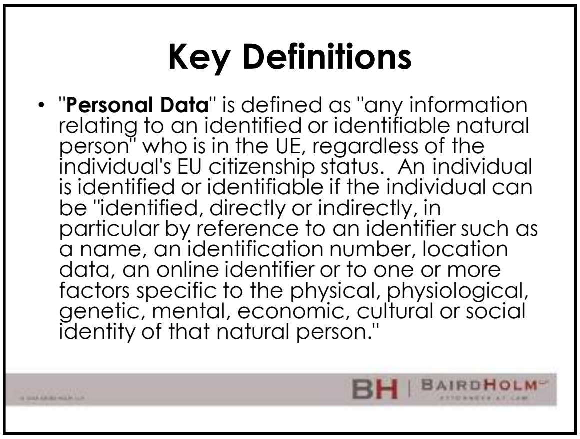
- Effective May 25, 2018
- Regulates the collection, use or other processing of personal data of individuals located in the EU.
- Extraterritorial reach

GDPR?
WHAT'S GDPR?



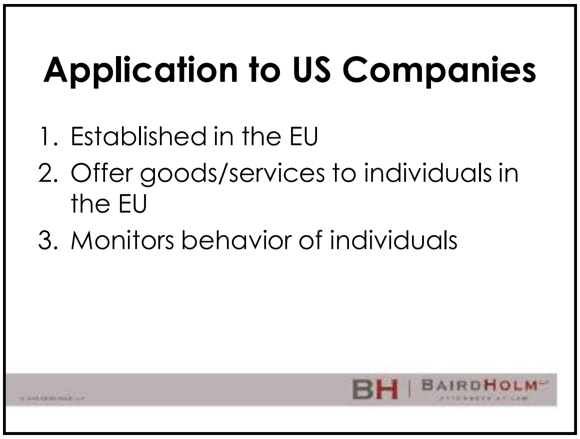
Key Definitions

- "**Data Controller**" is defined as any individual or entity that determines how and for what purposes personal data is processed.
- "**Data Processor**" is defined as any individual or entity that processes personal data for a data controller, other than the controller's employee.



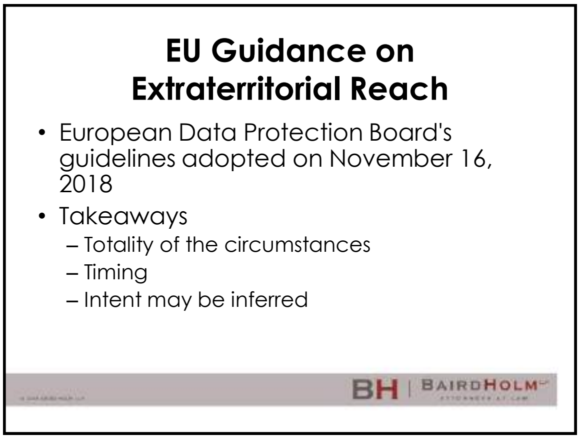
Key Definitions

- "**Personal Data**" is defined as "any information relating to an identified or identifiable natural person" who is in the UE, regardless of the individual's EU citizenship status. An individual is identified or identifiable if the individual can be "identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."



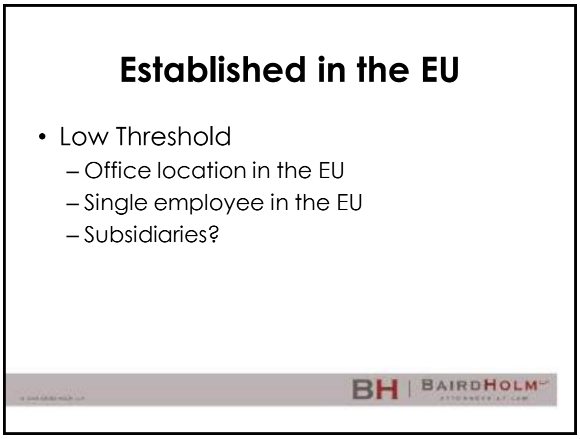
Application to US Companies

1. Established in the EU
2. Offer goods/services to individuals in the EU
3. Monitors behavior of individuals



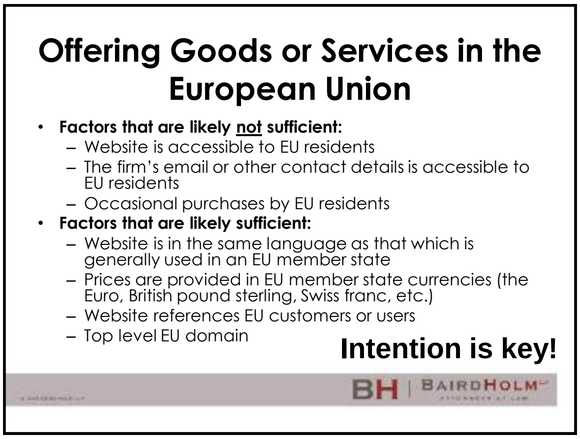
EU Guidance on Extraterritorial Reach

- European Data Protection Board's guidelines adopted on November 16, 2018
- Takeaways
  - Totality of the circumstances
  - Timing
  - Intent may be inferred



Established in the EU

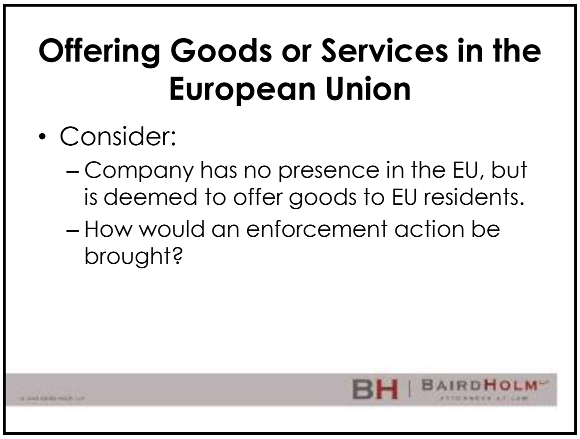
- Low Threshold
  - Office location in the EU
  - Single employee in the EU
  - Subsidiaries?



Offering Goods or Services in the European Union

- **Factors that are likely <u>not</u> sufficient:**
  - Website is accessible to EU residents
  - The firm's email or other contact details is accessible to EU residents
  - Occasional purchases by EU residents
- **Factors that are likely sufficient:**
  - Website is in the same language as that which is generally used in an EU member state
  - Prices are provided in EU member state currencies (the Euro, British pound sterling, Swiss franc, etc.)
  - Website references EU customers or users
  - Top level EU domain

Intention is key!



Offering Goods or Services in the European Union

- Consider:
  - Company has no presence in the EU, but is deemed to offer goods to EU residents.
  - How would an enforcement action be brought?

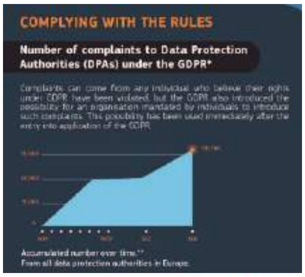
My Data Processor is in the EU

- Consider:
  - US company that is not established in the EU, nor does it market goods or services to EU residents, but it does use an EU based analytics company.
  - GDPR applicability?

How to Minimize the Application of the GDPR

- Marketing efforts (e.g., advertisements, promotions, behavioral tracking) are exclusively directed at non-GDPR markets.
- Do not provide information about goods or services in languages, other than U.S. English, that are generally used in one or more EU member states.
- Only provide pricing in, and only accept as payment, U.S. dollars.
- Clearly indicate that goods or services are not available to customers located in the EU.
- Utilize geoblocking to prevent EU IP addresses from accessing your website.
- Avoid, as practicable, providing travel instructions from the EU to Nebraska.
- Only provide contact details (e.g., mailing address, telephone number) based in the U.S.
- Utilize a generic top level domain (.com or .org) for your website.

GDPR a Year Later



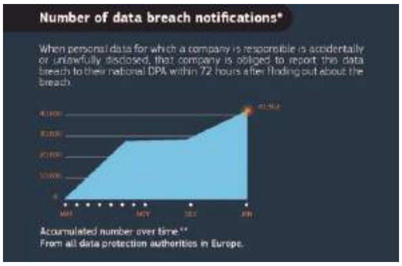
COMPLYING WITH THE RULES

Number of complaints to Data Protection Authorities (DPAs) under the GDPR*

Complaints can come from any individual who believe their rights under GDPR have been violated, but the GDPR also introduced the possibility for an organisation mandated by individuals to introduce such complaints. This possibility has been used immediately after the entry into application of the GDPR.

Accumulated number over time.**
From all data protection authorities in Europe.

GDPR a Year Later



When personal data for which a company is responsible is accidentally or unlawfully disclosed, that company is obliged to report this data breach to their national DPA within 72 hours after finding out about the breach.

Accumulated number over time.**
From all data protection authorities in Europe.

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

Penalties and Fines for Violating the GDPR

Art. 83 GDPR

General conditions for imposing administrative fines

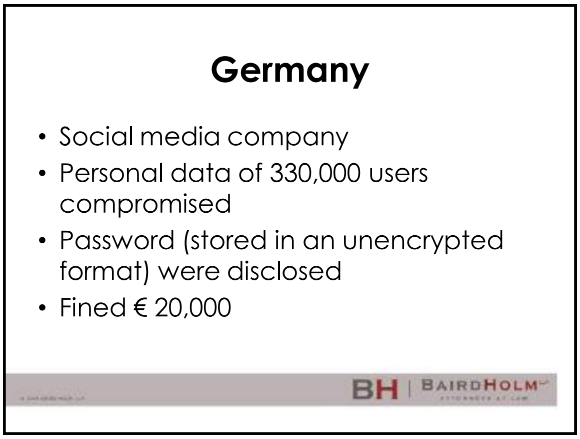
(1) Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

GDPR Fines

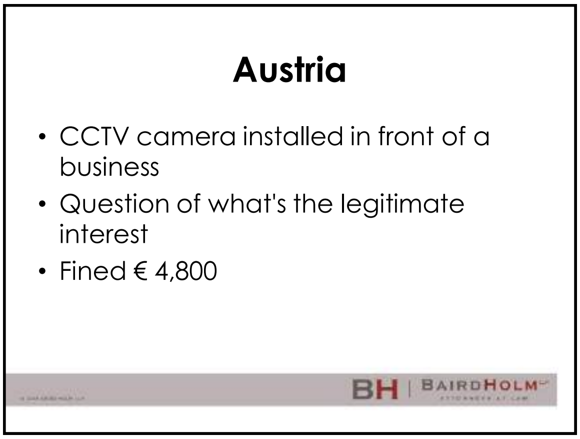
- Data protection authorities have already imposed fines in several cases
- Look at each example
- Takeaways

BH | BAIRDHOLM LLP ATTORNEYS AT LAW



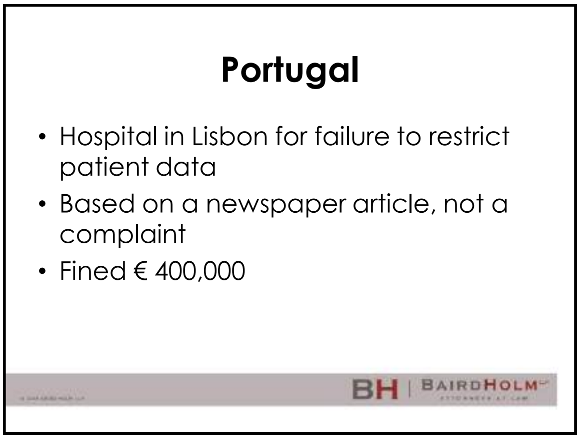
Germany

- Social media company
- Personal data of 330,000 users compromised
- Password (stored in an unencrypted format) were disclosed
- Fined € 20,000



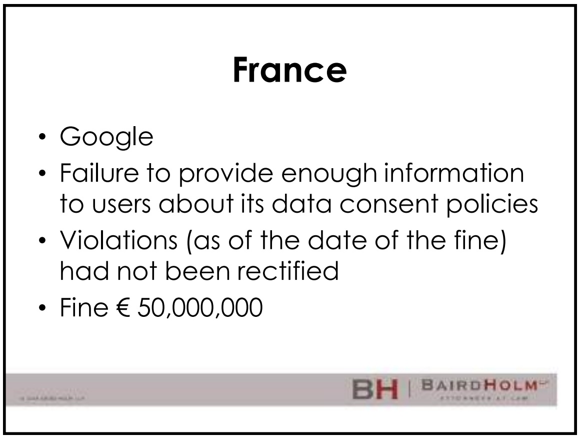
Austria

- CCTV camera installed in front of a business
- Question of what's the legitimate interest
- Fined € 4,800



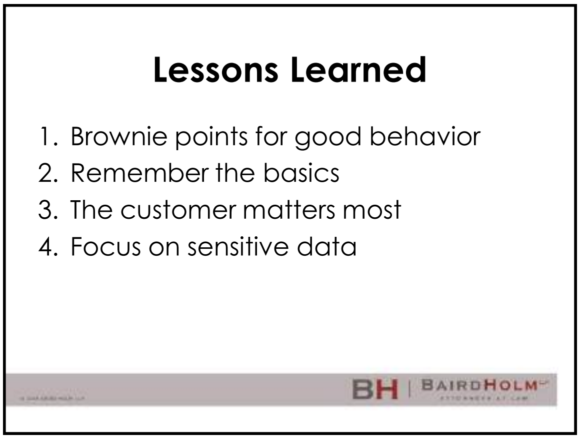
Portugal

- Hospital in Lisbon for failure to restrict patient data
- Based on a newspaper article, not a complaint
- Fined € 400,000



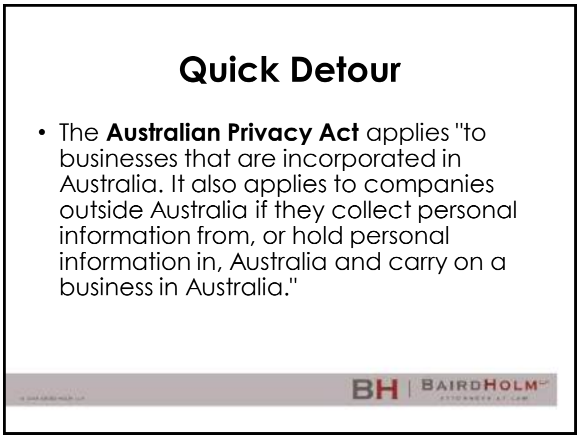
France

- Google
- Failure to provide enough information to users about its data consent policies
- Violations (as of the date of the fine) had not been rectified
- Fine € 50,000,000



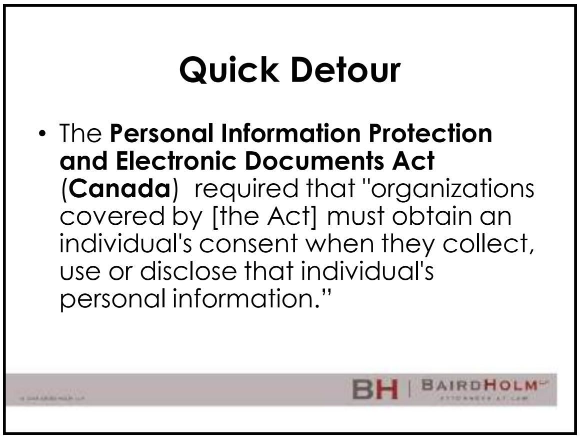
Lessons Learned

1. Brownie points for good behavior
2. Remember the basics
3. The customer matters most
4. Focus on sensitive data



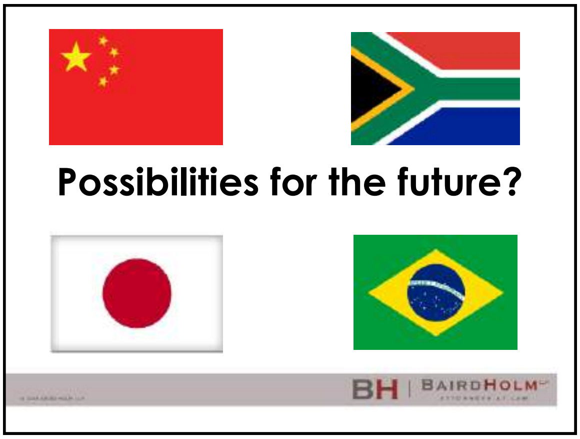
Quick Detour

- The **Australian Privacy Act** applies "to businesses that are incorporated in Australia. It also applies to companies outside Australia if they collect personal information from, or hold personal information in, Australia and carry on a business in Australia."



Quick Detour

- The **Personal Information Protection and Electronic Documents Act** (**Canada**) required that "organizations covered by [the Act] must obtain an individual's consent when they collect, use or disclose that individual's personal information."



Possibilities for the future?

Second Stop: The United States

Let's start in DC…

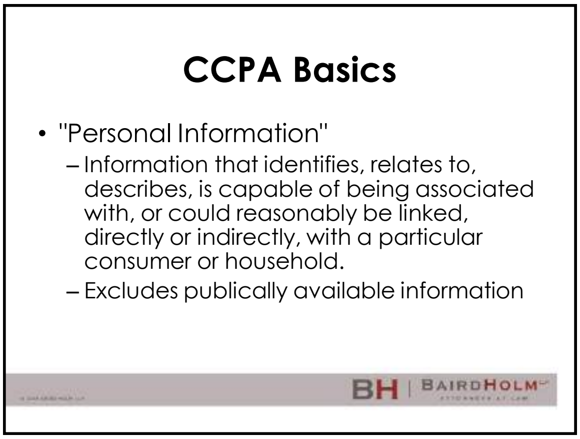
…and quickly head to California

CCPA Basics

- California Consumer Privacy Act
  - Signed into law June 2018
  - Requirements will not take effect until January 1, 2020
  - Attorney General must issue regulations between January 1, 2020 and July 2, 2020

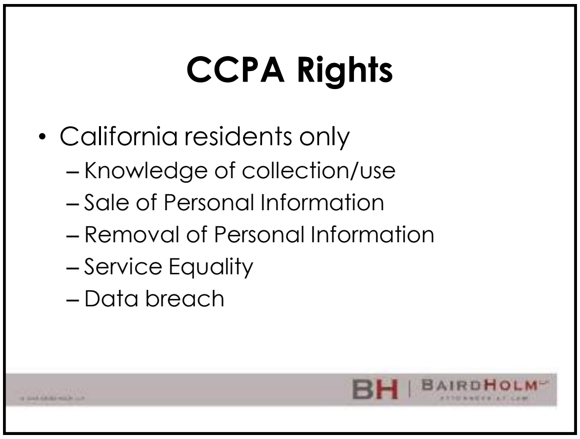
CCPA Basics

- Applicability
  - For-profit companies that both collect and process the Personal Information of California residents and do business in the State of California (physical presence not required in California);
  - AND, one the company meets one of the following:
    - The company must generate annual gross revenue in excess of $25 million,
    - The company must receive or share Personal Information of more than 50,000 California residents annually, or
    - The company must derive at least 50 percent of its annual revenue by selling the Personal Information of California residents.



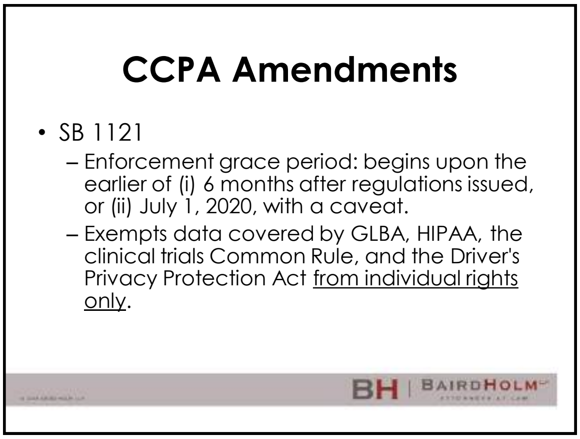
CCPA Basics

- "Personal Information"
  - Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
  - Excludes publically available information



CCPA Rights

- California residents only
  - Knowledge of collection/use
  - Sale of Personal Information
  - Removal of Personal Information
  - Service Equality
  - Data breach



CCPA Amendments

- SB 1121
  - Enforcement grace period: begins upon the earlier of (i) 6 months after regulations issued, or (ii) July 1, 2020, with a caveat.
  - Exempts data covered by GLBA, HIPAA, the clinical trials Common Rule, and the Driver's Privacy Protection Act from individual rights only.

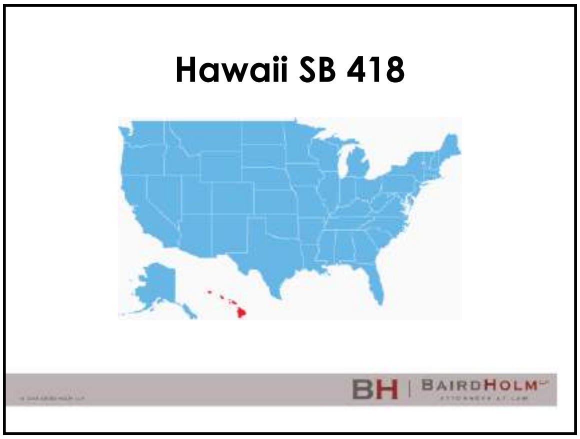
CCPA Amendments

- SB 1121 Technical Corrections
  - Clarification of Personal Information
  - Private right of action clarification
  - Civil penalty for privacy violations clarification
  - Preemption of local laws

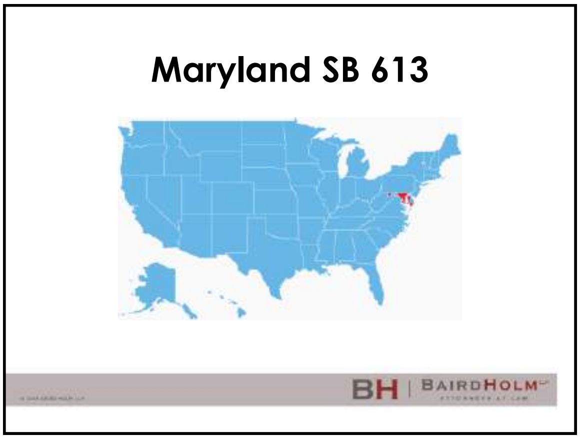
CCPA Remaining Issues

- Scope of Personal Information
- Ultimately Attorney General regulations are needed
- Business subject to CCPA should begin data mapping

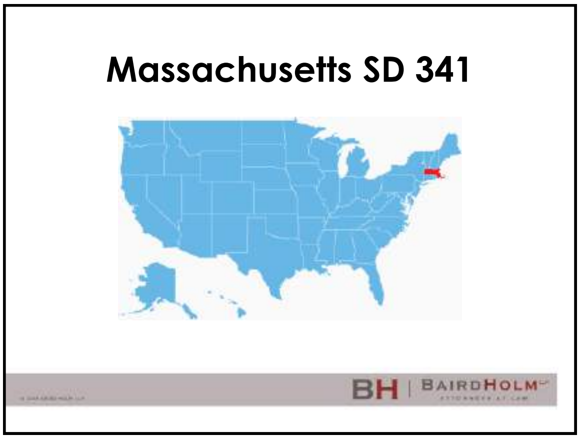
What About Other States?



Hawaii SB 418



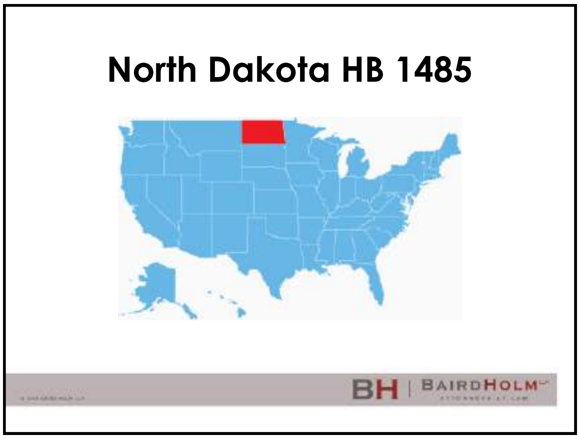
Maryland SB 613



Massachusetts SD 341

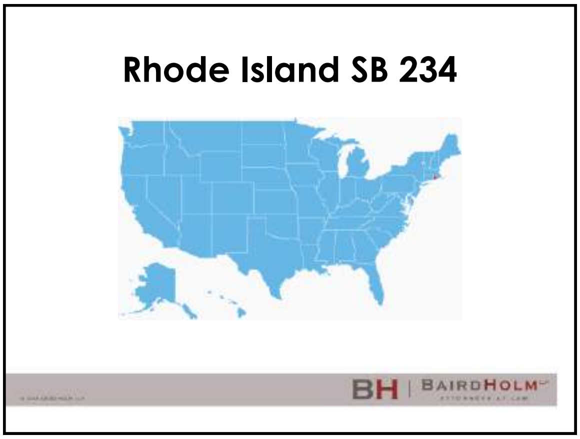
New Mexico SB 176

New York S 00224



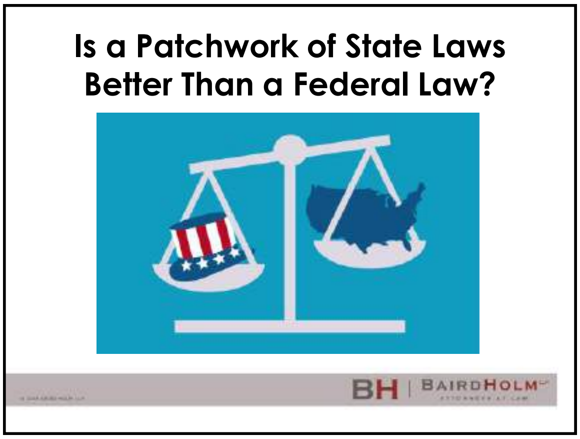
North Dakota HB 1485

Oregon HB 2866

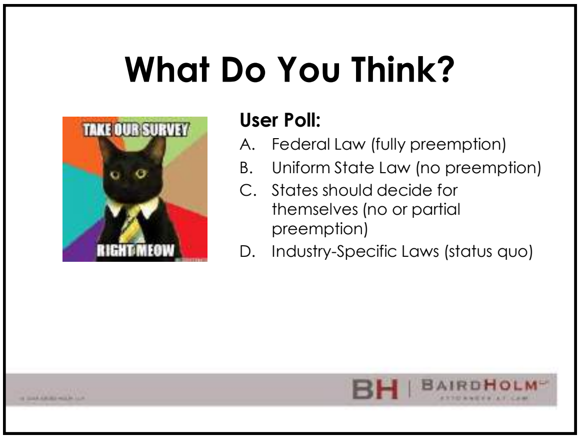


Rhode Island SB 234

Washington SB 5064



Is a Patchwork of State Laws Better Than a Federal Law?



What Do You Think?

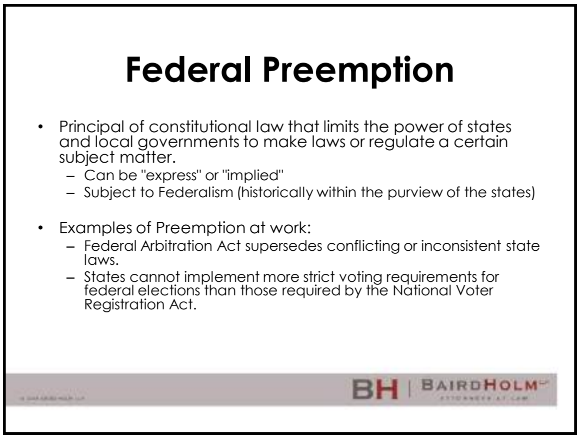
User Poll:

A. Federal Law (fully preemption)

B. Uniform State Law (no preemption)

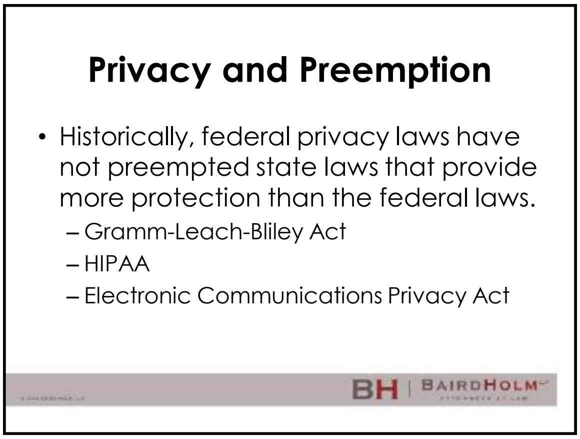
C. States should decide for themselves (no or partial preemption)

D. Industry-Specific Laws (status quo)



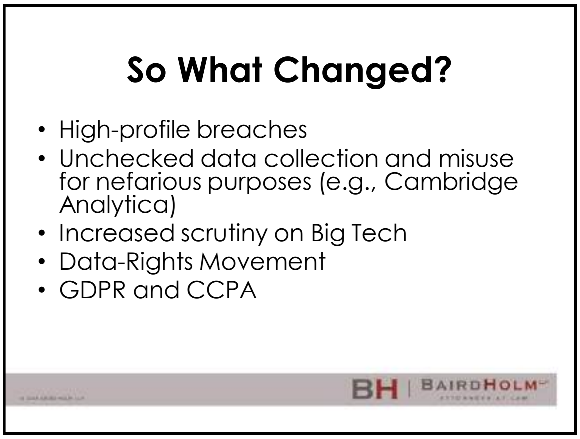
Federal Preemption

- Principal of constitutional law that limits the power of states and local governments to make laws or regulate a certain subject matter.
  - Can be "express" or "implied"
  - Subject to Federalism (historically within the purview of the states)
- Examples of Preemption at work:
  - Federal Arbitration Act supersedes conflicting or inconsistent state laws.
  - States cannot implement more strict voting requirements for federal elections than those required by the National Voter Registration Act.



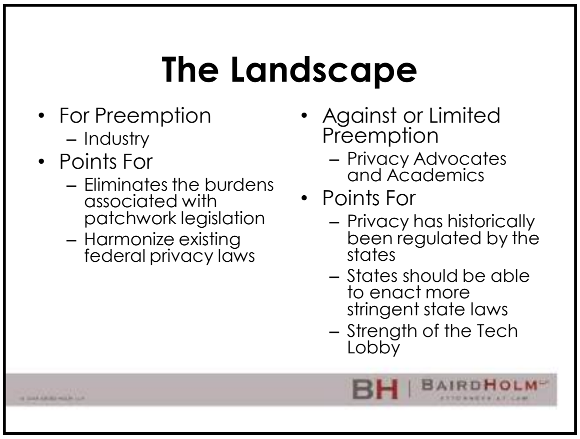
Privacy and Preemption

- Historically, federal privacy laws have not preempted state laws that provide more protection than the federal laws.
  - Gramm-Leach-Bliley Act
  - HIPAA
  - Electronic Communications Privacy Act



So What Changed?

- High-profile breaches
- Unchecked data collection and misuse for nefarious purposes (e.g., Cambridge Analytica)
- Increased scrutiny on Big Tech
- Data-Rights Movement
- GDPR and CCPA

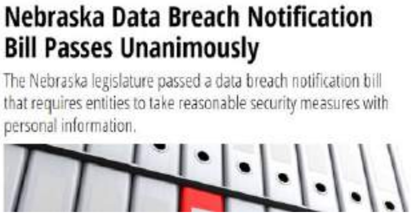


The Landscape

- For Preemption
  - Industry
- Points For
  - Eliminates the burdens associated with patchwork legislation
  - Harmonize existing federal privacy laws
- Against or Limited Preemption
  - Privacy Advocates and Academics
- Points For
  - Privacy has historically been regulated by the states
  - States should be able to enact more stringent state laws
  - Strength of the Tech Lobby

Survey Results!

Final Stop: Nebraska

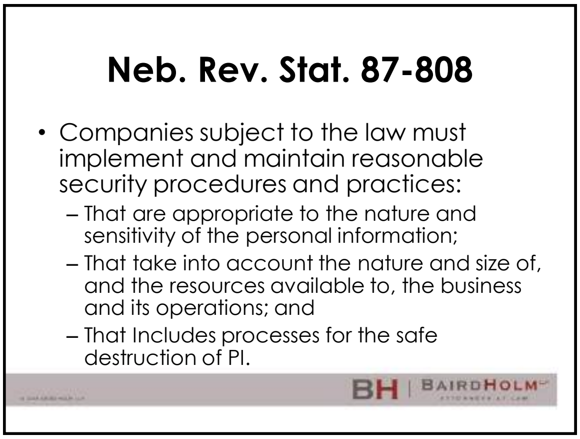


Nebraska Data Breach Notification Bill Passes Unanimously

The Nebraska legislature passed a data breach notification bill that requires entities to take reasonable security measures with personal information.

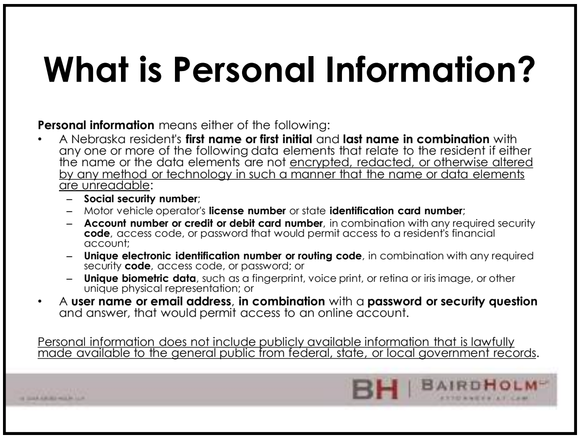
Neb. Rev. Stat. 87-808

- Applies to any company meeting all of the following:
  - – DOING BUSINESS in Nebraska;
  - – Owning, licensing, or maintaining computerized data that includes personal information;
  - – About a Nebraska resident.



Neb. Rev. Stat. 87-808

- Companies subject to the law must implement and maintain reasonable security procedures and practices:
  - That are appropriate to the nature and sensitivity of the personal information;
  - That take into account the nature and size of, and the resources available to, the business and its operations; and
  - That Includes processes for the safe destruction of PI.

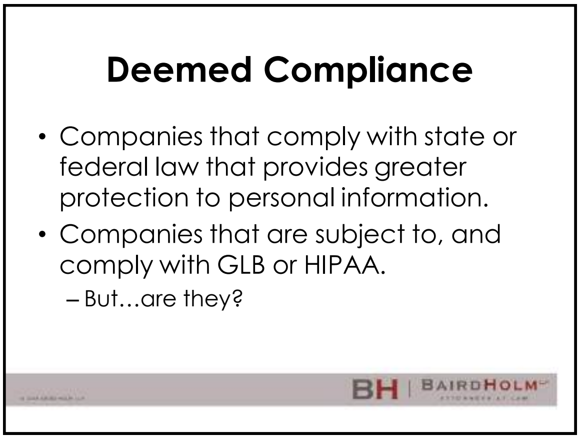


What is Personal Information?

Personal information means either of the following:

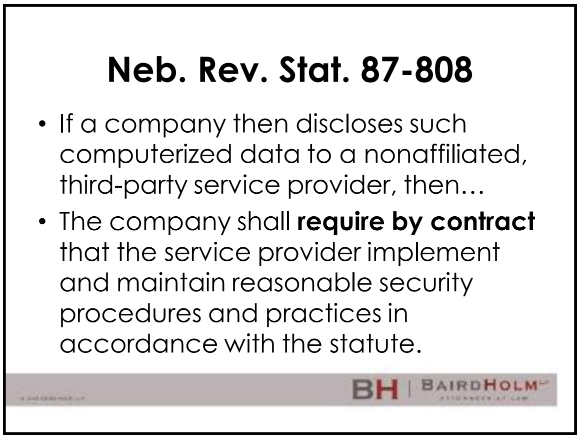
- A Nebraska resident's **first name or first initial** and **last name in combination** with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:
  - **Social security number**;
  - Motor vehicle operator's **license number** or state **identification card number**;
  - **Account number or credit or debit card number**, in combination with any required security **code**, access code, or password that would permit access to a resident's financial account;
  - **Unique electronic identification number or routing code**, in combination with any required security **code**, access code, or password; or
  - **Unique biometric data**, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or
- A **user name or email address**, **in combination** with a **password or security question** and answer, that would permit access to an online account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.



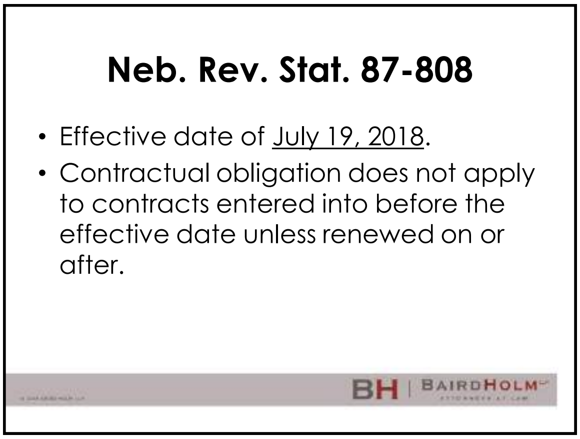
Deemed Compliance

- Companies that comply with state or federal law that provides greater protection to personal information.
- Companies that are subject to, and comply with GLB or HIPAA.
  - But…are they?



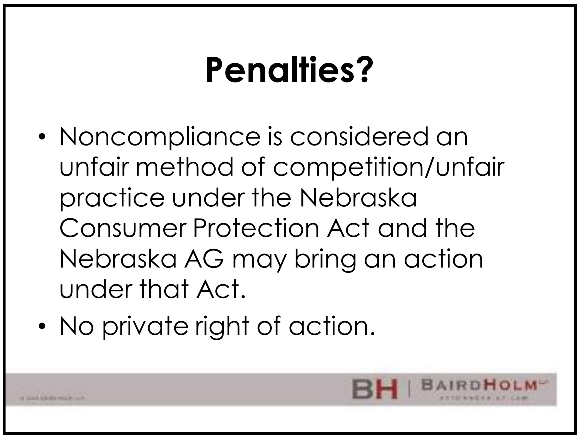
Neb. Rev. Stat. 87-808

- If a company then discloses such computerized data to a nonaffiliated, third-party service provider, then…
- The company shall **require by contract** that the service provider implement and maintain reasonable security procedures and practices in accordance with the statute.



Neb. Rev. Stat. 87-808

- Effective date of July 19, 2018.
- Contractual obligation does not apply to contracts entered into before the effective date unless renewed on or after.



Penalties?

- Noncompliance is considered an unfair method of competition/unfair practice under the Nebraska Consumer Protection Act and the Nebraska AG may bring an action under that Act.
- No private right of action.

Nebraska is Not Alone

- 17 states require similar security practices.
- 7 States require contractual assurances from third-party contractors.

BH | BAIRDHOLM

BH | BAIRDHOLM

Questions?

Grayson J. Derrick
gderrick@bairdholm.com
(402) 636 – 8229

Ari Goldstein
agoldstein@bairdholm.com
(402) 636 – 8236

Abigail T. Mohs
amohs@bairdholm.com
(402) 636 – 8296

Sean Nakamoto
snakamoto@bairdholm.com
(402) 636 – 8247

BH | BAIRDHOLM

BAIRD HOLM LLP
TECHNOLOGY & DATA
PROTECTION FORUM

Why Are We Still Talking about E-mails, Mobile Devices, and Cloud Vendors? Because They're STILL a Hot Topic (and the focus of many recent cyberattacks)

James E. O'Connor and Michael W. Chase

Why Are We Still Talking About E-mails, Mobile Devices, and Cloud Vendors?

Because They're *STILL* a Hot Topic (and the focus of many recent cyberattacks)

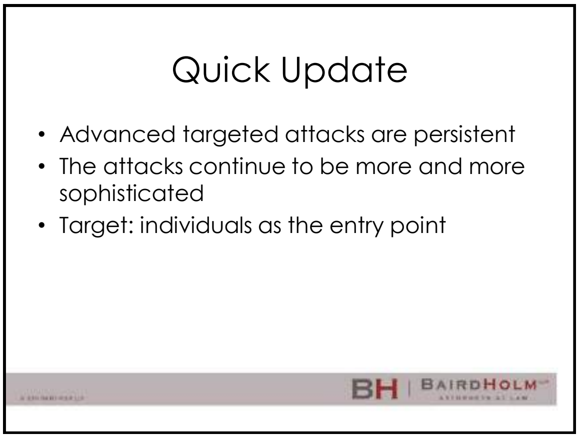
Michael W. Chase
James E. O'Connor

Agenda

- Recent breach experience
- On-going Cloud absorption
- Unique email considerations
- Best practices
  - Technical
  - Administrative
- Lessons learned

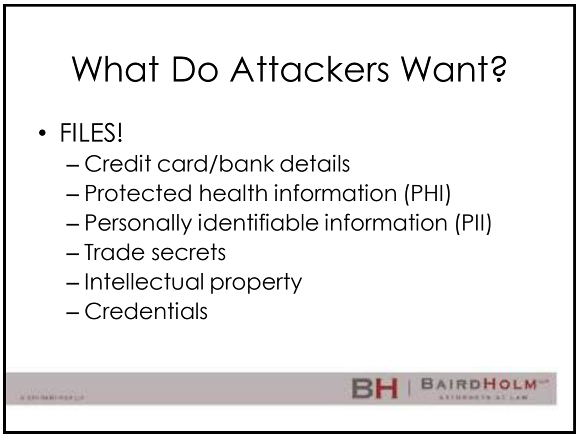
Quick Update

- Digital transformation is underway
- Many organizations are embracing new technologies, including multi-cloud deployments
- Data environments are increasingly complex
- Each environment requires a unique data security approach
- In the end, much sensitive data is *still* at risk



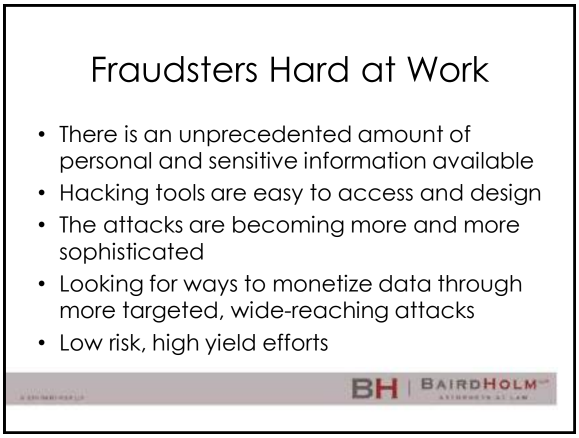
Quick Update

- Advanced targeted attacks are persistent
- The attacks continue to be more and more sophisticated
- Target: individuals as the entry point



What Do Attackers Want?

- FILES!
  - Credit card/bank details
  - Protected health information (PHI)
  - Personally identifiable information (PII)
  - Trade secrets
  - Intellectual property
  - Credentials



Fraudsters Hard at Work

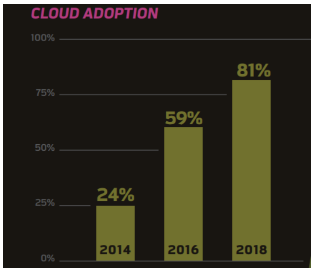
- There is an unprecedented amount of personal and sensitive information available
- Hacking tools are easy to access and design
- The attacks are becoming more and more sophisticated
- Looking for ways to monetize data through more targeted, wide-reaching attacks
- Low risk, high yield efforts

Faced With a Dilemma

- Explosion of data!
  - Cloud-based applications
  - Mobile devices
  - E-mail
- Think about your environment
- Convenience vs. Security
- Impact of moving to the cloud

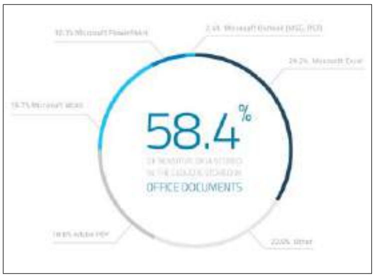
Source: https://www.seagate.com/our-story/data-age-2025/

On-going Cloud Absorption



Source: Adoption of Cloud https://wire19.com/over-half-of-organizations-have-now-deployed-office-365/

On-going Cloud Absorption



Source: McAfee Office 365 Adoption Rate https://www.skyhighnetworks.com/cloud-security-blog/7-charts-reveal-the-meteoric-rise-of-office-365/

Where Does *All* of your Data Reside?

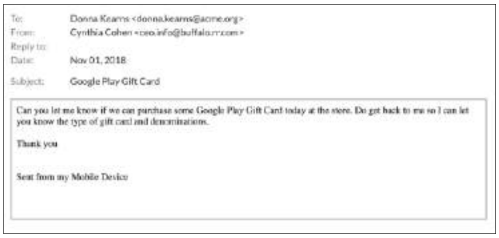
- Probably not all cloud-based
- Could reside in local servers, databases, office documents, files, and…

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

E-mail, E-mail, E-mail

- E-mail is the gateway
- Think about it from the hacker's perspective
  - Easy to mine company databases, websites, social media, etc.
  - Easy to craft personalized e-mails that appear to be from a known, trusted source

BH | BAIRDHOLM LLP ATTORNEYS AT LAW



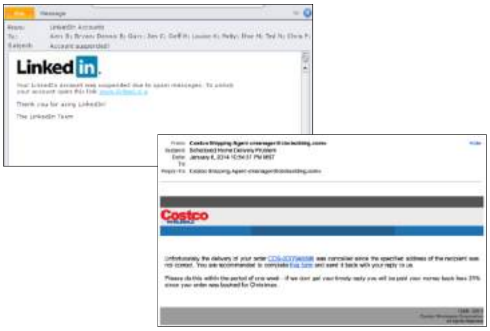
To: Donna Kearns <donna.kearns@acme.org>
From: Cynthia Cohen <ceo.info@buffalo.rr.com>
Reply to:
Date: Nov 01, 2018
Subject: Google Play Gift Card

Can you let me know if we can purchase some Google Play Gift Card today at the store. Do get back to me so I can let you know the type of gift card and denominations.

Thank you

Sent from my Mobile Device

BH | BAIRDHOLM LLP ATTORNEYS AT LAW



From: LinkedIn Accounts
To: [illegible]
Subject: Account suspended!

Your LinkedIn account was suspended due to spam messages. To unlock your account open this link [illegible]

Thank you for using LinkedIn!

The LinkedIn Team

From: Costco Shipping Agent [illegible]
Subject: Scheduled Home Delivery Problem
Date: January 8, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent [illegible]

Unfortunately the delivery of your order [illegible] was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

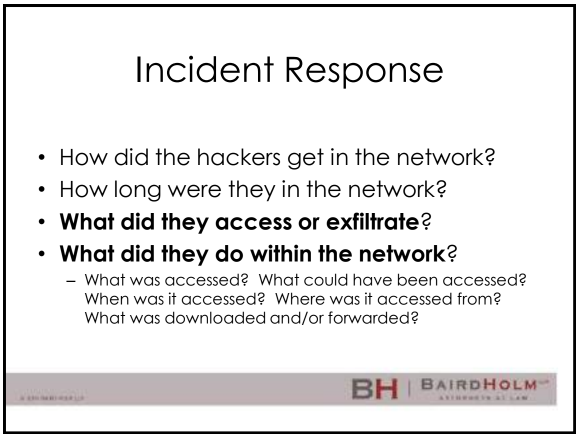
Please do this within the period of one week - if we don't get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

Phishing/Spam E-mails

- ~70% try to trick users into clicking on a malicious URL
- Malicious attachments also used
- Spam e-mail was the most common method for cyber criminals to spread malware in 2018

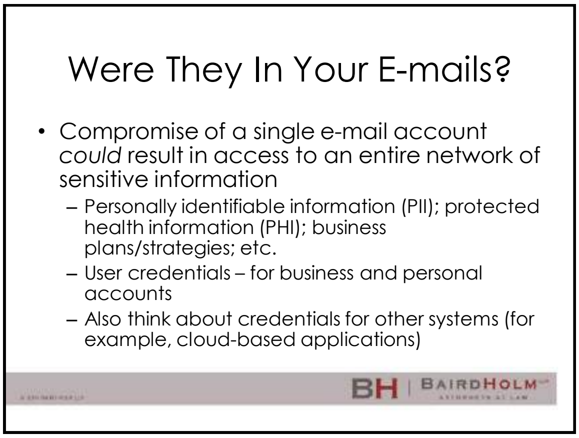
So You Clicked On The Link

- A ransom note appears – your files are encrypted and must pay a Bitcoin amount to decrypt the files
- Luckily, you've got a good backup policy and can promptly restore the system
- You know that *most* of your files (for example, electronic health records) are in a cloud-based application that was not affected by the ransomware
- So you activate your incident response plan



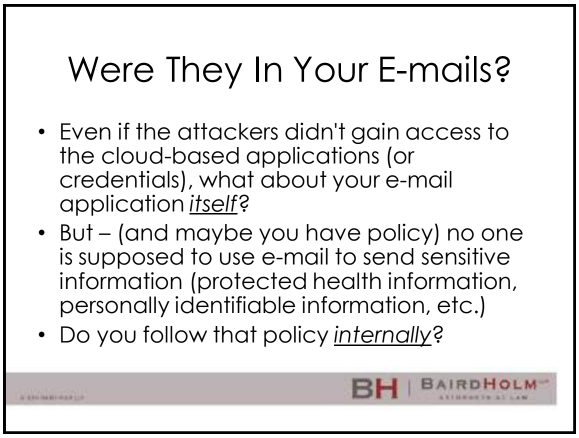
Incident Response

- How did the hackers get in the network?
- How long were they in the network?
- **What did they access or exfiltrate**?
- **What did they do within the network**?
  - What was accessed? What could have been accessed? When was it accessed? Where was it accessed from? What was downloaded and/or forwarded?



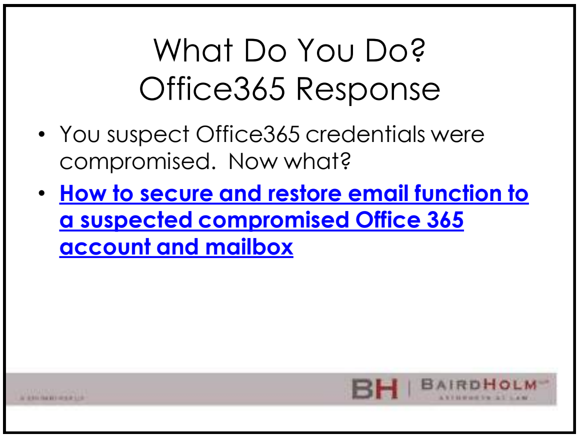
Were They In Your E-mails?

- Compromise of a single e-mail account *could* result in access to an entire network of sensitive information
  - Personally identifiable information (PII); protected health information (PHI); business plans/strategies; etc.
  - User credentials – for business and personal accounts
  - Also think about credentials for other systems (for example, cloud-based applications)



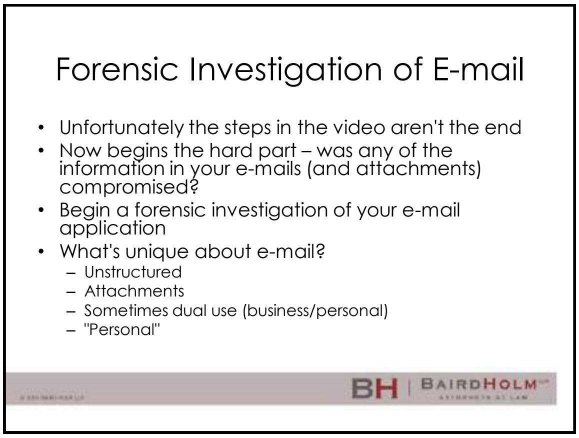
Were They In Your E-mails?

- Even if the attackers didn't gain access to the cloud-based applications (or credentials), what about your e-mail application *itself*?
- But – (and maybe you have policy) no one is supposed to use e-mail to send sensitive information (protected health information, personally identifiable information, etc.)
- Do you follow that policy *internally*?



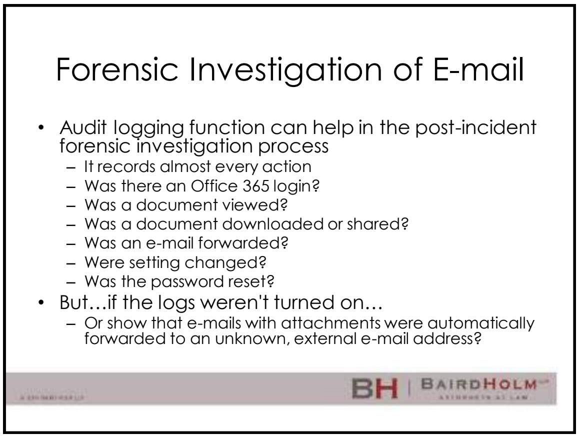
What Do You Do?
Office365 Response

- You suspect Office365 credentials were compromised. Now what?
- **How to secure and restore email function to a suspected compromised Office 365 account and mailbox**



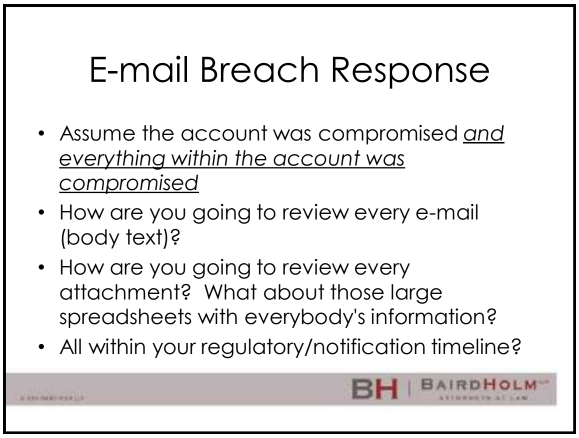
Forensic Investigation of E-mail

- Unfortunately the steps in the video aren't the end
- Now begins the hard part – was any of the information in your e-mails (and attachments) compromised?
- Begin a forensic investigation of your e-mail application
- What's unique about e-mail?
  - Unstructured
  - Attachments
  - Sometimes dual use (business/personal)
  - "Personal"



Forensic Investigation of E-mail

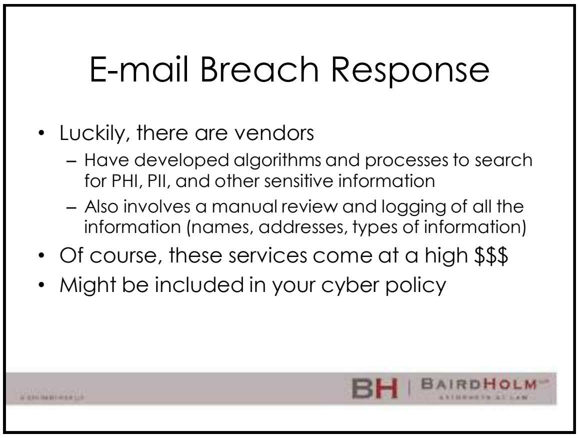
- Audit logging function can help in the post-incident forensic investigation process
  - It records almost every action
  - Was there an Office 365 login?
  - Was a document viewed?
  - Was a document downloaded or shared?
  - Was an e-mail forwarded?
  - Were setting changed?
  - Was the password reset?
- But…if the logs weren't turned on…
  - Or show that e-mails with attachments were automatically forwarded to an unknown, external e-mail address?



E-mail Breach Response

- Assume the account was compromised *and everything within the account was compromised*
- How are you going to review every e-mail (body text)?
- How are you going to review every attachment? What about those large spreadsheets with everybody's information?
- All within your regulatory/notification timeline?

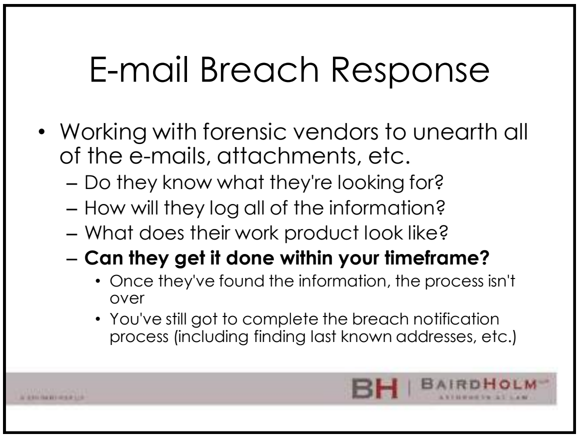
BH | BAIRDHOLM



E-mail Breach Response

- Luckily, there are vendors
  - Have developed algorithms and processes to search for PHI, PII, and other sensitive information
  - Also involves a manual review and logging of all the information (names, addresses, types of information)
- Of course, these services come at a high $$$
- Might be included in your cyber policy

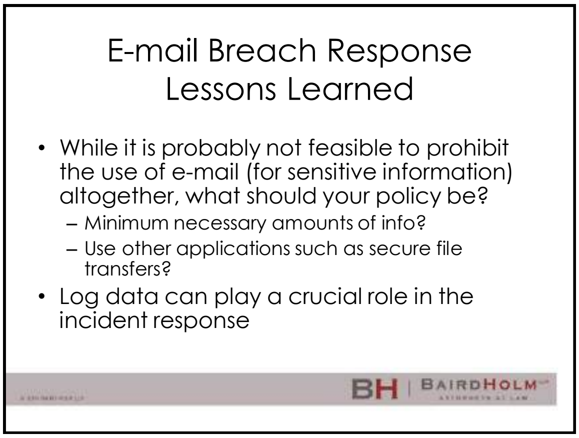
BH | BAIRDHOLM



E-mail Breach Response

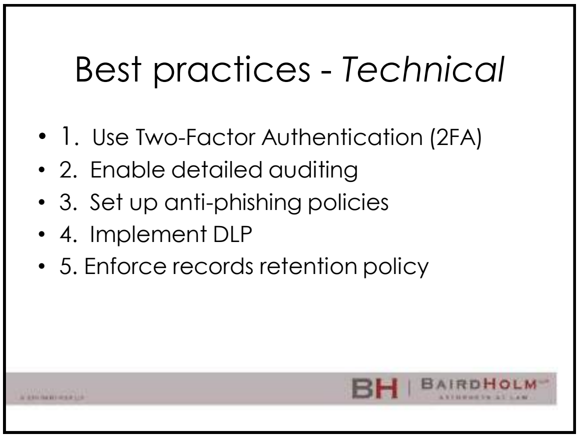
- Working with forensic vendors to unearth all of the e-mails, attachments, etc.
  - Do they know what they're looking for?
  - How will they log all of the information?
  - What does their work product look like?
  - **Can they get it done within your timeframe?**
    - Once they've found the information, the process isn't over
    - You've still got to complete the breach notification process (including finding last known addresses, etc.)

BH | BAIRDHOLM



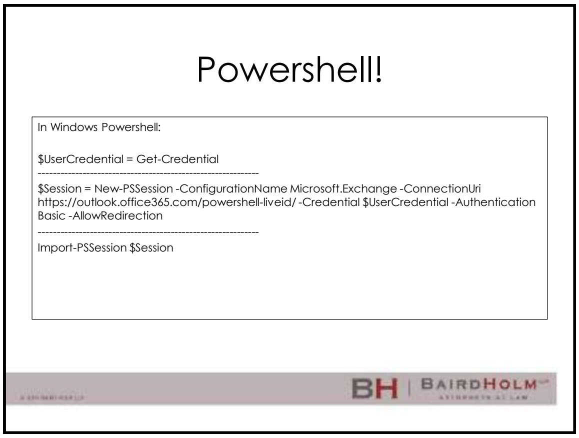
E-mail Breach Response Lessons Learned

- While it is probably not feasible to prohibit the use of e-mail (for sensitive information) altogether, what should your policy be?
  - Minimum necessary amounts of info?
  - Use other applications such as secure file transfers?
- Log data can play a crucial role in the incident response



Best practices - *Technical*

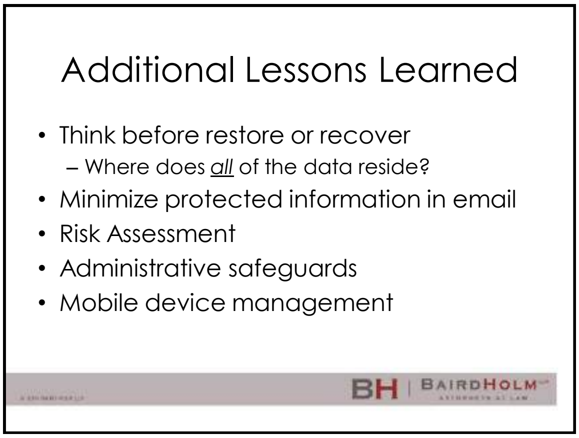
- 1. Use Two-Factor Authentication (2FA)
- 2. Enable detailed auditing
- 3. Set up anti-phishing policies
- 4. Implement DLP
- 5. Enforce records retention policy



Powershell!

```
In Windows Powershell:

$UserCredential = Get-Credential
-------------------------------------------------------
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication
Basic -AllowRedirection
-------------------------------------------------------
Import-PSSession $Session
```



Additional Lessons Learned

- Think before restore or recover
  - Where does *all* of the data reside?
- Minimize protected information in email
- Risk Assessment
- Administrative safeguards
- Mobile device management

Questions?

Michael W. Chase
mchase@bairdholm.com
(402) 636 – 8326

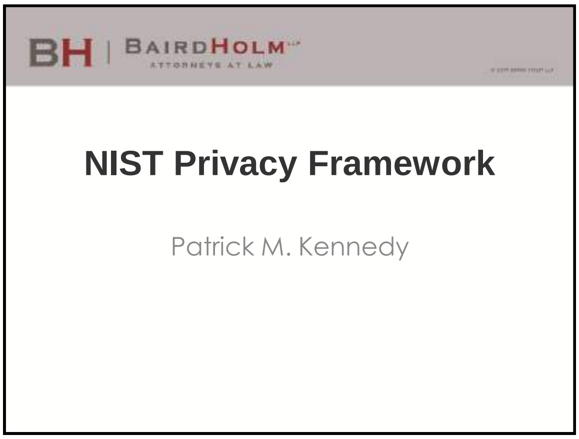
James E. O'Connor
joconnor@bairdholm.com
(402) 636 – 8332

Hot Topics

- **NIST Privacy Framework** - Patrick M. Kennedy
- **Blockchain Patent** - AriAnna C. Goldstein
- **HIPAA RFI Update** - Abigail T. Mohs
- **ICOs and the SEC** - Sean T. Nakamoto
- **Update from the Uniform Law Commission** - James E. O’Connor
- **Employment and Privacy** - Kelli P. Lieurance
- **Privacy, HIPAA, Health Apps, and the Apple Watch** - Kimberly A. Lammers
- **Genetic Information Testing, Biometrics, and Privacy** - Thomas S. Dean

Hot Topics

Panel of Baird Holm Attorneys



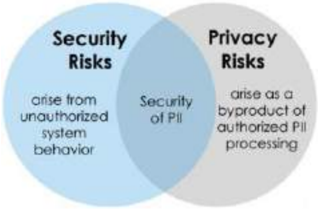
NIST Privacy Framework

Patrick M. Kennedy

Goals of NIST

- Develop voluntary, enterprise level tool for managing privacy risks
- Apply tool to diverse privacy needs
- Provide compatibility with applicable legal/regulatory regimes

Security and Privacy Risk Relationship


Security Risks
arise from unauthorized system behavior
Security of PII
Privacy Risks
arise as a byproduct of authorized PII processing

There is a clear recognition that security of PII plays an important role in the protection of privacy

Individual privacy cannot be achieved solely by securing PII

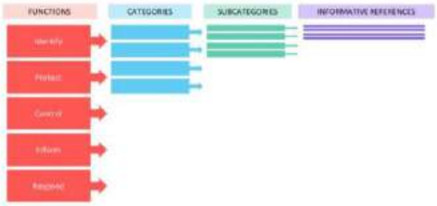
Authorized processing: system operations that handle PII (collection - disposal) to enable the system to achieve mission/business objectives

Source: HIMSS

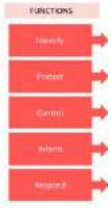
Development Status

- Kickoff: October 2018
- RFI: November 2018 – January 2019
- Discussion Draft: ~May 2019

Privacy Framework Core



Privacy Framework Core



Develop organizational understanding to manage privacy risk

Develop and implement appropriate data safeguards

Develop and implement appropriate activities to manage data with sufficient granularity

Develop and implement appropriate activities to inform individuals of how data is processed

Develop and implement appropriate activities to respond to a privacy breach

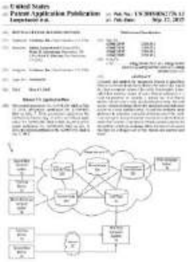
BH | BAIRDHOLM LLP ATTORNEYS AT LAW

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

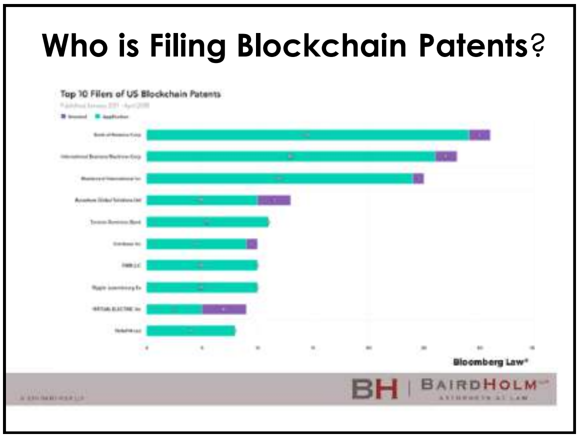
Blockchain Patents

AriAnna C. Goldstein

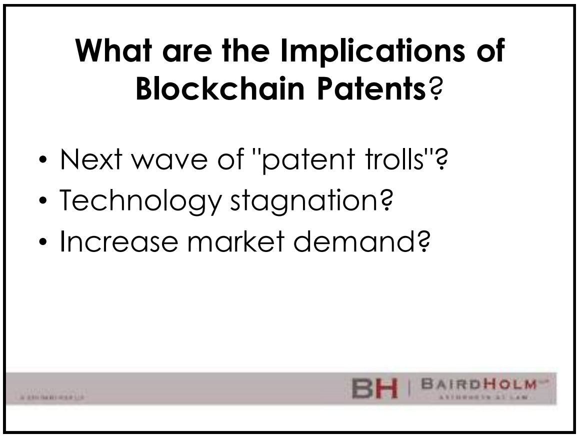
What are Blockchain Patents?


United States
Patent Application Publication

BH | BAIRDHOLM LLP ATTORNEYS AT LAW



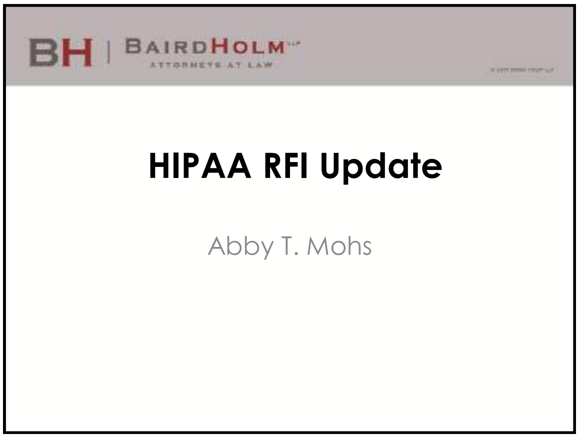
Who is Filing Blockchain Patents?



What are the Implications of Blockchain Patents?

- Next wave of "patent trolls"?
- Technology stagnation?
- Increase market demand?

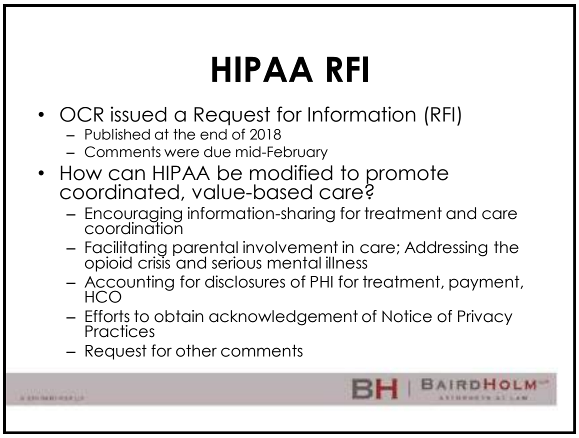
BH | BAIRDHOLM LLP ATTORNEYS AT LAW



BH | BAIRDHOLM LLP ATTORNEYS AT LAW

HIPAA RFI Update

Abby T. Mohs

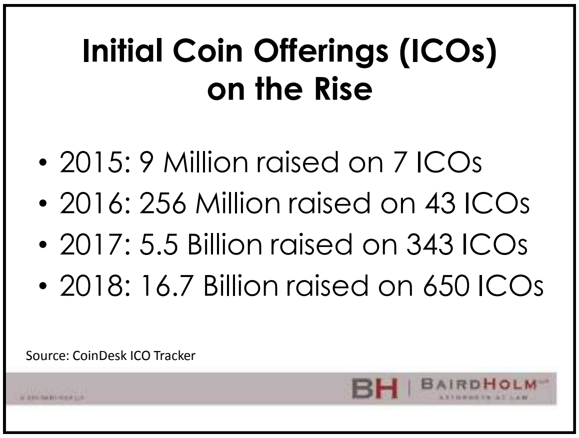


HIPAA RFI

- OCR issued a Request for Information (RFI)
  - Published at the end of 2018
  - Comments were due mid-February
- How can HIPAA be modified to promote coordinated, value-based care?
  - Encouraging information-sharing for treatment and care coordination
  - Facilitating parental involvement in care; Addressing the opioid crisis and serious mental illness
  - Accounting for disclosures of PHI for treatment, payment, HCO
  - Efforts to obtain acknowledgement of Notice of Privacy Practices
  - Request for other comments

ICOs and the SEC

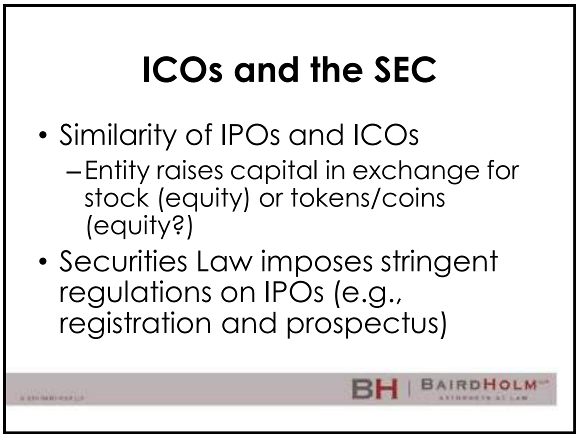
Sean T. Nakamoto



Initial Coin Offerings (ICOs) on the Rise

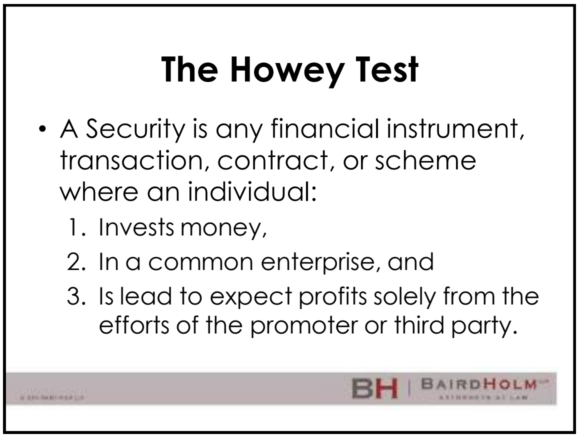
- 2015: 9 Million raised on 7 ICOs
- 2016: 256 Million raised on 43 ICOs
- 2017: 5.5 Billion raised on 343 ICOs
- 2018: 16.7 Billion raised on 650 ICOs

Source: CoinDesk ICO Tracker



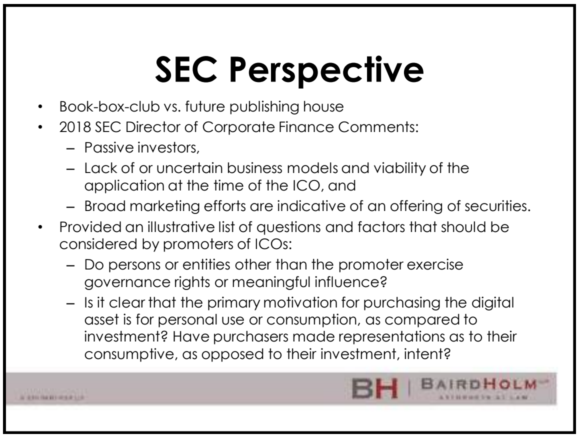
ICOs and the SEC

- Similarity of IPOs and ICOs
  - Entity raises capital in exchange for stock (equity) or tokens/coins (equity?)
- Securities Law imposes stringent regulations on IPOs (e.g., registration and prospectus)



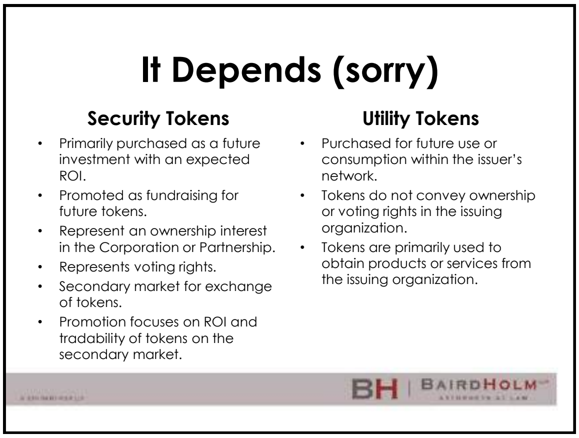
The Howey Test

- A Security is any financial instrument, transaction, contract, or scheme where an individual:
  1. Invests money,
  2. In a common enterprise, and
  3. Is lead to expect profits solely from the efforts of the promoter or third party.



SEC Perspective

- Book-box-club vs. future publishing house
- 2018 SEC Director of Corporate Finance Comments:
  - Passive investors,
  - Lack of or uncertain business models and viability of the application at the time of the ICO, and
  - Broad marketing efforts are indicative of an offering of securities.
- Provided an illustrative list of questions and factors that should be considered by promoters of ICOs:
  - Do persons or entities other than the promoter exercise governance rights or meaningful influence?
  - Is it clear that the primary motivation for purchasing the digital asset is for personal use or consumption, as compared to investment? Have purchasers made representations as to their consumptive, as opposed to their investment, intent?



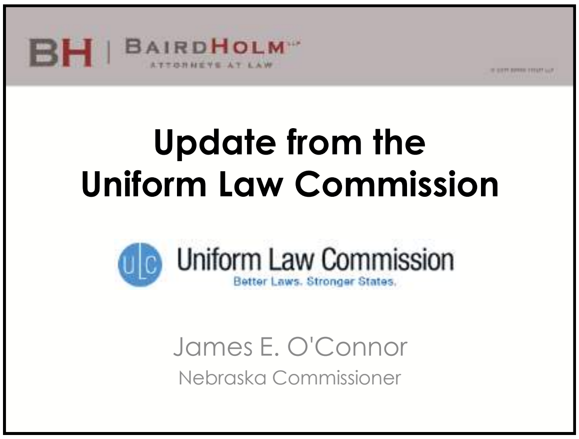
It Depends (sorry)

Security Tokens

- Primarily purchased as a future investment with an expected ROI.
- Promoted as fundraising for future tokens.
- Represent an ownership interest in the Corporation or Partnership.
- Represents voting rights.
- Secondary market for exchange of tokens.
- Promotion focuses on ROI and tradability of tokens on the secondary market.

Utility Tokens

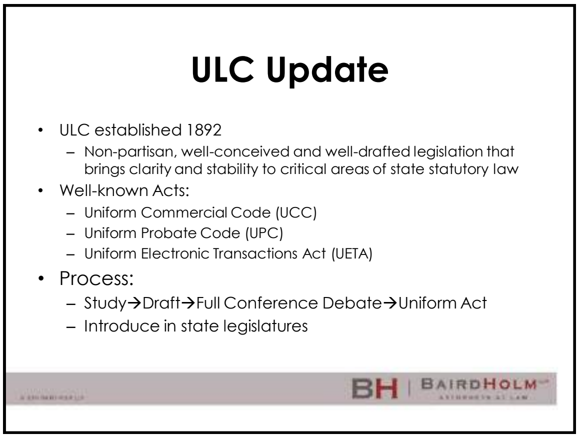
- Purchased for future use or consumption within the issuer's network.
- Tokens do not convey ownership or voting rights in the issuing organization.
- Tokens are primarily used to obtain products or services from the issuing organization.



Update from the Uniform Law Commission

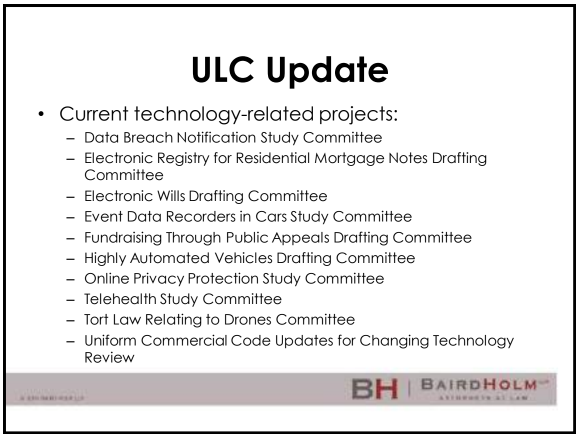
Uniform Law Commission
Better Laws. Stronger States.

James E. O'Connor
Nebraska Commissioner



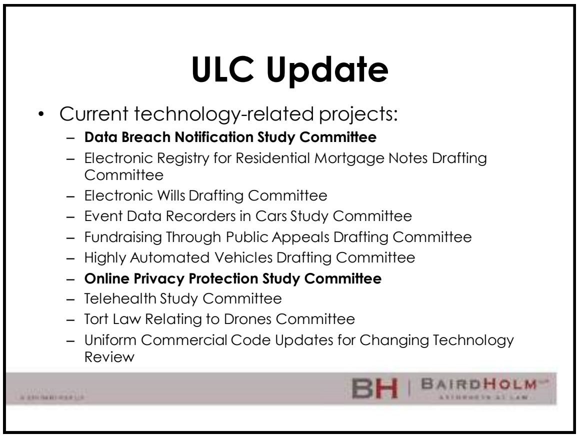
ULC Update

- ULC established 1892
  - Non-partisan, well-conceived and well-drafted legislation that brings clarity and stability to critical areas of state statutory law
- Well-known Acts:
  - Uniform Commercial Code (UCC)
  - Uniform Probate Code (UPC)
  - Uniform Electronic Transactions Act (UETA)
- Process:
  - Study→Draft→Full Conference Debate→Uniform Act
  - Introduce in state legislatures



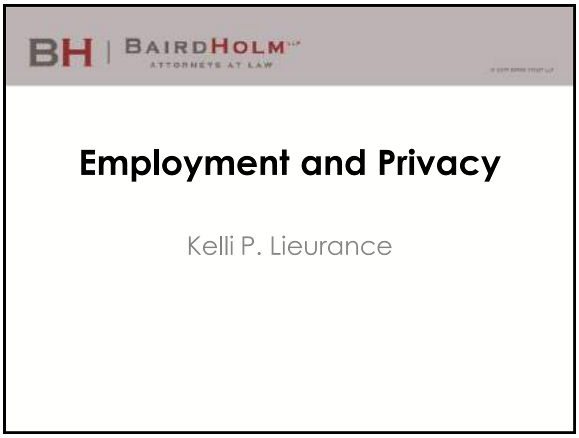
ULC Update

- Current technology-related projects:
  - Data Breach Notification Study Committee
  - Electronic Registry for Residential Mortgage Notes Drafting Committee
  - Electronic Wills Drafting Committee
  - Event Data Recorders in Cars Study Committee
  - Fundraising Through Public Appeals Drafting Committee
  - Highly Automated Vehicles Drafting Committee
  - Online Privacy Protection Study Committee
  - Telehealth Study Committee
  - Tort Law Relating to Drones Committee
  - Uniform Commercial Code Updates for Changing Technology Review



ULC Update

- Current technology-related projects:
  - **Data Breach Notification Study Committee**
  - Electronic Registry for Residential Mortgage Notes Drafting Committee
  - Electronic Wills Drafting Committee
  - Event Data Recorders in Cars Study Committee
  - Fundraising Through Public Appeals Drafting Committee
  - Highly Automated Vehicles Drafting Committee
  - **Online Privacy Protection Study Committee**
  - Telehealth Study Committee
  - Tort Law Relating to Drones Committee
  - Uniform Commercial Code Updates for Changing Technology Review



Employment and Privacy

Kelli P. Lieurance

Right to Privacy

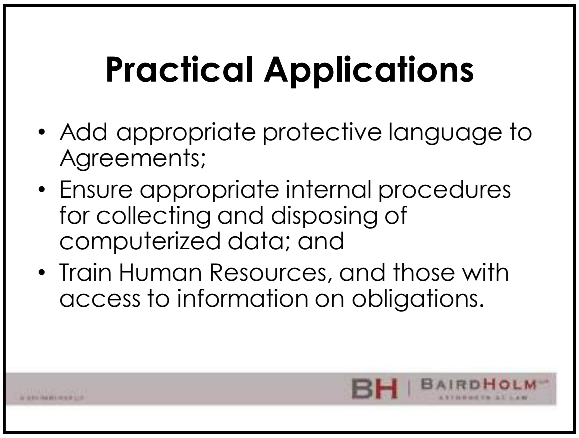
- At work, generally?
- In personal devices?
- In social media posts?
- In your personal information?

Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006

- Effective July 19, 2018
- Applies to anyone conducting business in Nebraska that "owns, licenses, or maintains computerized data that includes personal information about a resident of Nebraska."

Practical Applications

- Analyze which third party vendors have access to employee personal information:
  - Payroll providers;
  - Banks (direct deposit information);
  - Benefits brokers; and
  - IT consultants.



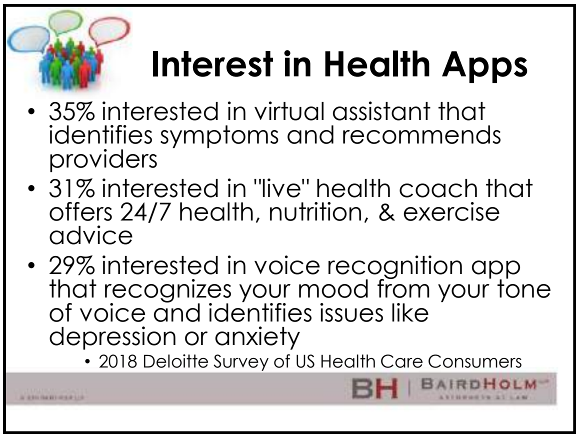
Practical Applications

- Add appropriate protective language to Agreements;
- Ensure appropriate internal procedures for collecting and disposing of computerized data; and
- Train Human Resources, and those with access to information on obligations.

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

Privacy, HIPAA, Health Apps, and the Apple Watch

Kimberly A. Lammers



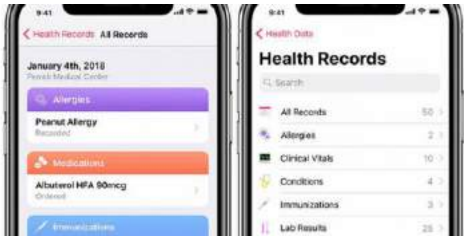
Interest in Health Apps

- 35% interested in virtual assistant that identifies symptoms and recommends providers
- 31% interested in "live" health coach that offers 24/7 health, nutrition, & exercise advice
- 29% interested in voice recognition app that recognizes your mood from your tone of voice and identifies issues like depression or anxiety
  - 2018 Deloitte Survey of US Health Care Consumers

Sharing of Information

- 60% willing to share personal health data (from wearables) with their physicians to improve their health
- 53% would share information with emergency services if experiencing emergency situation
- 39% willing to contribute blinded information to health care researchers
  - 2018 Deloitte Survey of US Health Care Consumers

Health Records Interface



9:41

Health Records All Records

January 4th, 2018

Penrab Medical Center

Allergies

Peanut Allergy

Recorded

Medications

Albuterol HFA 90mcg

Ordered

Immunizations

9:41

Health Data

Health Records

Search

All Records	50
Allergies	2
Clinical Vitals	10
Conditions	4
Immunizations	3
Lab Results	25

HIPAA

- Applies to covered entities (business associates) and governs how they gather and use information
- Does not protect all health care information
  - Health apps and wearables are a gap

Does HIPAA Apply to Apple?

- "Apple is providing a user the ability to request and download their health records utilizing a direct, encrypted connection between the user's iPhone and the APIs provided by the health system or clinic."

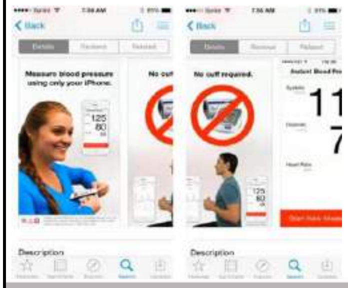
Short Answer: No

- "As part of this feature, Apple is not creating, receiving, maintaining, or transmitting protected health information for or on behalf of a covered entity or business associate."
- Apple is not a covered entity
- HIPAA does not apply to the information once it leaves the EMR

FDA Regulation of Medical Devices

- Issued clearance letters for EKG and irregular heart rhythm functions as Class II devices
- De novo approval for EKG feature – first direct-to-consumer EKG wearable
- FDA specified not intended to replace traditional methods of diagnosis nor to provide diagnosis

FTC & Deceptive Claims



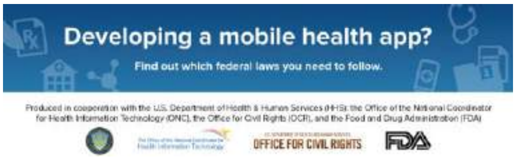
- Instant Blood Pressure App
- Priced at $3.99-$4.99
- Settlement with Aura Labs for misleading consumers

FTC's Complaint

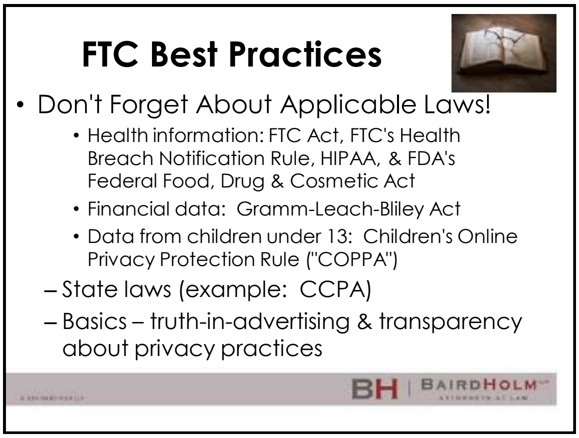
- FTC alleged that studies demonstrated "**clinically and statistically significant deviations"** between measurements from app v. traditional blood pressure cuff
- Positive endorsers of app were relatives of co-owner and Aura CEO/President ("ARCHIE1986")

FTC Best Practices – Mobile Health App Developers

- Focus on data collection, access, & security
- Mobile Health Apps Interactive Tool

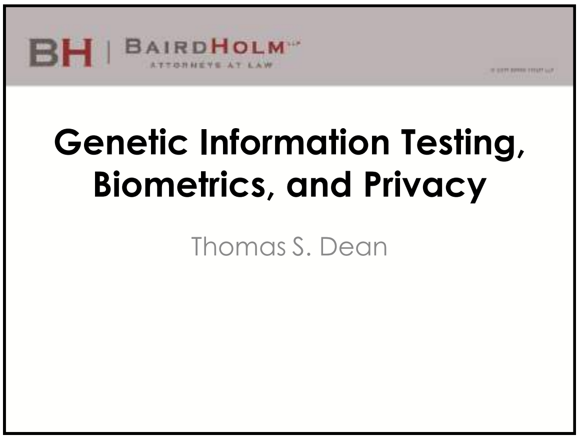

Developing a mobile health app?
Find out which federal laws you need to follow.
OFFICE FOR CIVIL RIGHTS
FDA

Produced in cooperation with the U.S. Department of Health & Human Services (HHS): the Office of the National Coordinator for Health Information Technology (ONC), the Office for Civil Rights (OCR), and the Food and Drug Administration (FDA)



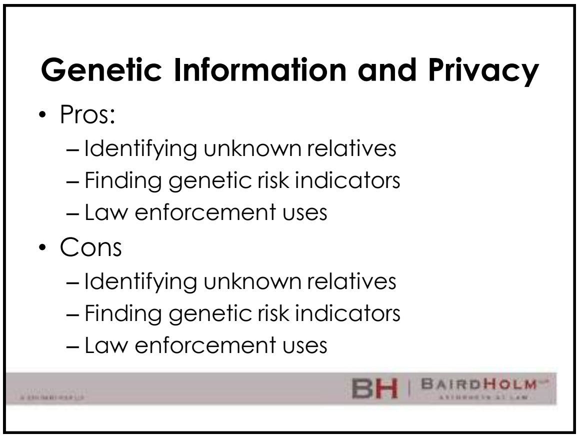
FTC Best Practices

- Don't Forget About Applicable Laws!
  - Health information: FTC Act, FTC's Health Breach Notification Rule, HIPAA, & FDA's Federal Food, Drug & Cosmetic Act
  - Financial data: Gramm-Leach-Bliley Act
  - Data from children under 13: Children's Online Privacy Protection Rule ("COPPA")
  - State laws (example: CCPA)
  - Basics – truth-in-advertising & transparency about privacy practices



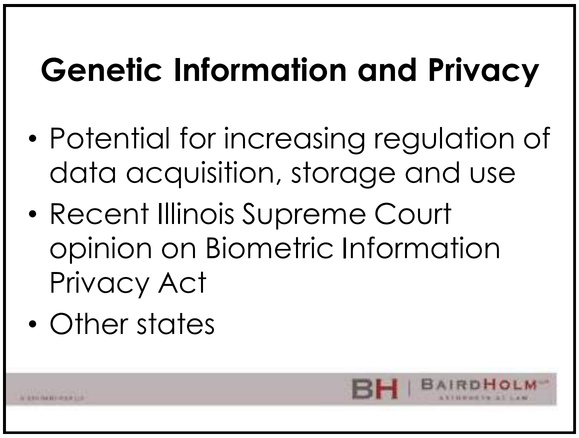
Genetic Information Testing, Biometrics, and Privacy

Thomas S. Dean



Genetic Information and Privacy

- Pros:
  - Identifying unknown relatives
  - Finding genetic risk indicators
  - Law enforcement uses
- Cons
  - Identifying unknown relatives
  - Finding genetic risk indicators
  - Law enforcement uses



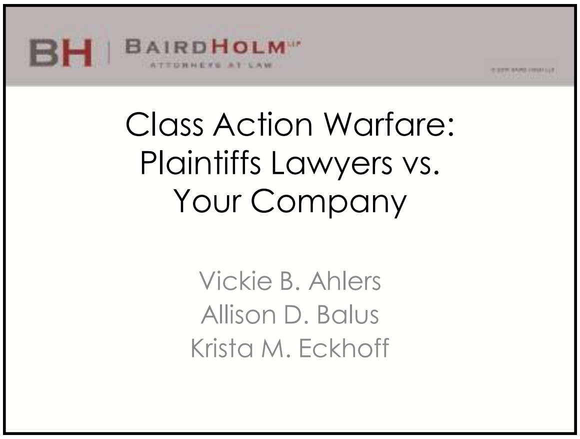
Genetic Information and Privacy

- Potential for increasing regulation of data acquisition, storage and use
- Recent Illinois Supreme Court opinion on Biometric Information Privacy Act
- Other states

Questions?

Class Action Warfare: Plaintiffs Lawyers vs. Your Company

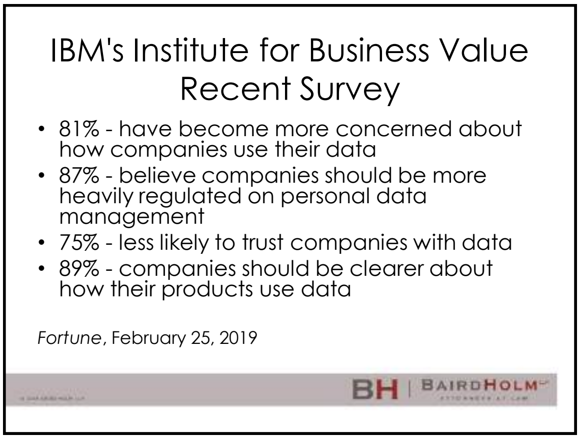
Vickie B. Ahlers, Krista M. Eckhoff and Allison D. Balus



BH | BAIRDHOLM LLP
ATTORNEYS AT LAW

Class Action Warfare: Plaintiffs Lawyers vs. Your Company

Vickie B. Ahlers
Allison D. Balus
Krista M. Eckhoff

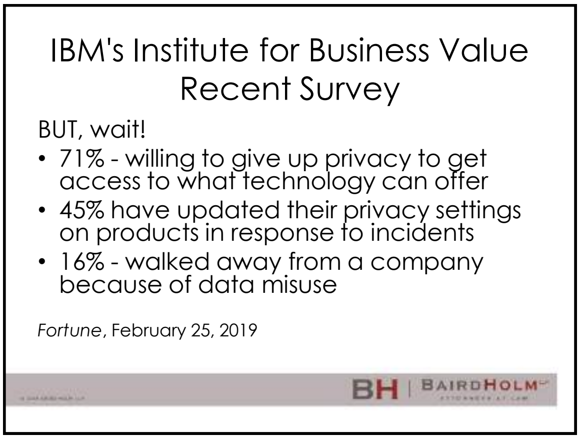


IBM's Institute for Business Value Recent Survey

- 81% - have become more concerned about how companies use their data
- 87% - believe companies should be more heavily regulated on personal data management
- 75% - less likely to trust companies with data
- 89% - companies should be clearer about how their products use data

Fortune, February 25, 2019

BH | BAIRDHOLM LLP
ATTORNEYS AT LAW



IBM's Institute for Business Value Recent Survey

BUT, wait!

- 71% - willing to give up privacy to get access to what technology can offer
- 45% have updated their privacy settings on products in response to incidents
- 16% - walked away from a company because of data misuse

Fortune, February 25, 2019

BH | BAIRDHOLM LLP
ATTORNEYS AT LAW

Who's behind some of the big lawsuits?

Big Tech vs. Big Privacy Lawsuits

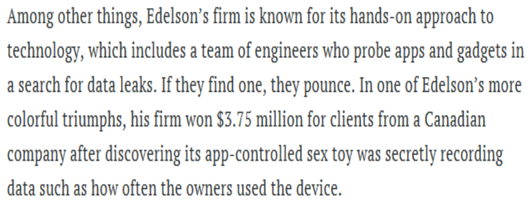
Fortune Magazine, Feb. 23, 2019

By JEFF JOHN ROBERTS February 23, 2019

Jay Edelson grew up poor among rich kids outside Boston. He seethes at the recollection of other boys smashing their $200 tennis rackets he could not afford, and of his parents scolding him for trying to spend the $10 he had earned raking leaves.

"Aggressive legal tactics"

Fortune Magazine, Feb 23, 2019



Among other things, Edelson's firm is known for its hands-on approach to technology, which includes a team of engineers who probe apps and gadgets in a search for data leaks. If they find one, they pounce. In one of Edelson's more colorful triumphs, his firm won $3.75 million for clients from a Canadian company after discovering its app-controlled sex toy was secretly recording data such as how often the owners used the device.

IoT Hacks May Bring Frenzy of Litigation

The rush to market for connected, embedded, and smart devices has already left security in the rear view mirror. And despite the Mirai attacks of 2016 and other countless Internet of things-related vulnerabilities and security research, little has been accomplished in keeping these devices from becoming an easy port of entry or pivot point for attacks targeting enterprises.

Now to make matters more complicated, here come the lawyers.

A Feeding Frenzy

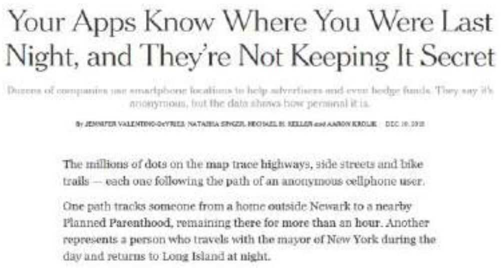
"Somewhere, there is a conclave of plaintiffs' lawyers wringing their hands waiting to file suits related to IoT hacks, according to Ijay Palansky, a trial lawyer in Washington, D.C. for the law firm Armstrong Teasdale, who said during the Black Hat security conference in Las Vegas that an inflection point is at hand for plaintiffs' lawyers. 'All conditions are ripe for a wave of these lawsuits,' Palansky said, likening it to a feeding frenzy."

Who is IJay Palansky?

- Lead lawyer for *plaintiffs* in the 220,000 member federal class action against Jeep (hackers allowed to take over Jeep's steering and breaking)
- BUT - built his career on *defending* class actions and defending companies (perhaps some in the defense bar are swirling too?)
- IJay also spent several years as a professional high-stakes poker player
  - A member of the two-man "human" team that played the world's leading artificial intelligence poker computer in the "Man vs. Machine" exhibition at the World Series of Poker in 2008.

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

New York Times, Dec. 10, 2018



Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret

Dozens of companies use smartphone locations to help advertisers and even hedge funds. They say it's anonymous, but the data shows how personal it is.

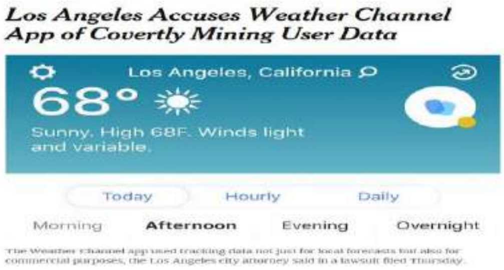
By JENNIFER VALENTINO-DeVRIES, NATASHA SINGER, MICHAEL H. KELLER and AARON KROLIK | DEC. 10, 2018

The millions of dots on the map trace highways, side streets and bike trails — each one following the path of an anonymous cellphone user.

One path tracks someone from a home outside Newark to a nearby Planned Parenthood, remaining there for more than an hour. Another represents a person who travels with the mayor of New York during the day and returns to Long Island at night.

BH | BAIRDHOLM LLP ATTORNEYS AT LAW

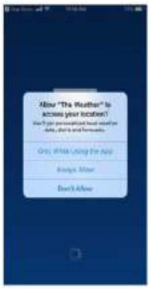
New York Times, January 3, 2019



Los Angeles Accuses Weather Channel App of Covertly Mining User Data

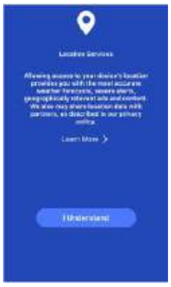
The Weather Channel app used tracking data not just for local forecasts but also for commercial purposes, the Los Angeles city attorney said in a lawsuit filed Thursday.

BH | BAIRDHOLM LLP ATTORNEYS AT LAW



Allow "The Weather" to access your location?

You'll get personalized local weather data, alerts and forecasts.



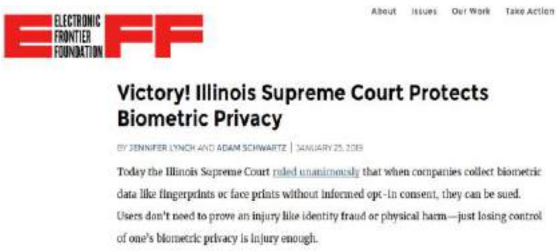
Location Services

Allowing access to your device's location provides you with the most accurate weather forecasts, severe alerts, geographically relevant ads and content. We also may share location data with partners, as described in our privacy policy.

Common Themes

- Negligence
- Negligence *per se*
- Invasion of privacy/breach of confidence
- Unjust enrichment
- Breach of Contract
  - Privacy policies/other documents formed contract
- Breach of Implied Contract
- Violation of federal statute (if private cause of action, e.g., Fair Credit Reporting Act)
- Violation of state statute
  - State consumer protection statute/unfair trade practices
  - ***State biometric information privacy statute***

Illinois Biometrics Battle

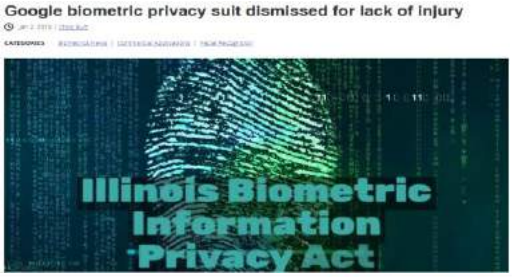


Victory! Illinois Supreme Court Protects Biometric Privacy

BY JENNIFER LYNCH AND ADAM SCHWARTZ | JANUARY 25, 2019

Today the Illinois Supreme Court ruled unanimously that when companies collect biometric data like fingerprints or face prints without informed opt-in consent, they can be sued. Users don't need to prove an injury like identity fraud or physical harm—just losing control of one's biometric privacy is injury enough.

But Feds Say No Standing



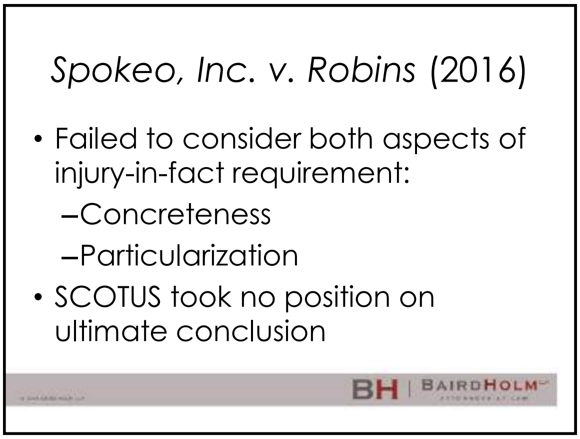
Google biometric privacy suit dismissed for lack of injury

CATEGORIES

Plaintiffs' biggest hurdle in data breach class actions: standing

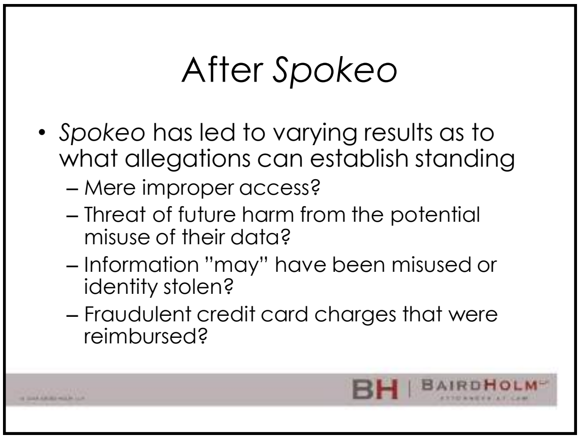
Spokeo, Inc. v. Robins (2016)

- FCRA case, pled as a class action, involving inaccurate info
- Trial court dismissed, finding plaintiff had not properly pled injury in fact—a required element of standing
- 9th Circuit reversed
- SCOTUS vacated and remanded



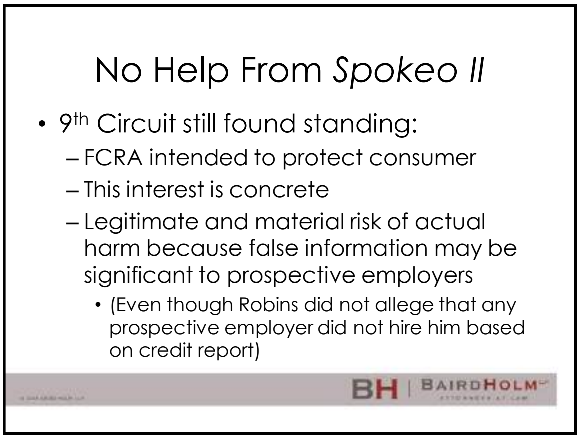
Spokeo, Inc. v. Robins (2016)

- Failed to consider both aspects of injury-in-fact requirement:
  - Concreteness
  - Particularization
- SCOTUS took no position on ultimate conclusion



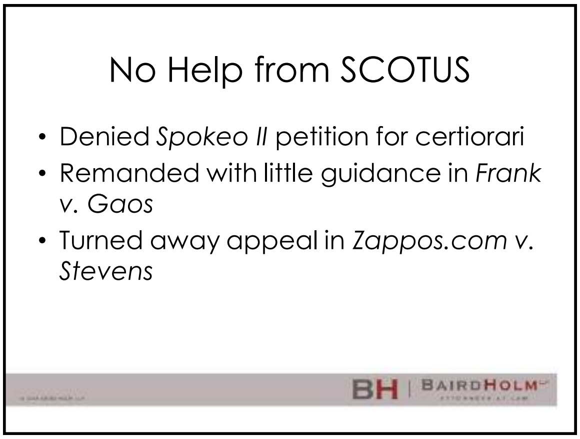
After *Spokeo*

- *Spokeo* has led to varying results as to what allegations can establish standing
  - Mere improper access?
  - Threat of future harm from the potential misuse of their data?
  - Information "may" have been misused or identity stolen?
  - Fraudulent credit card charges that were reimbursed?



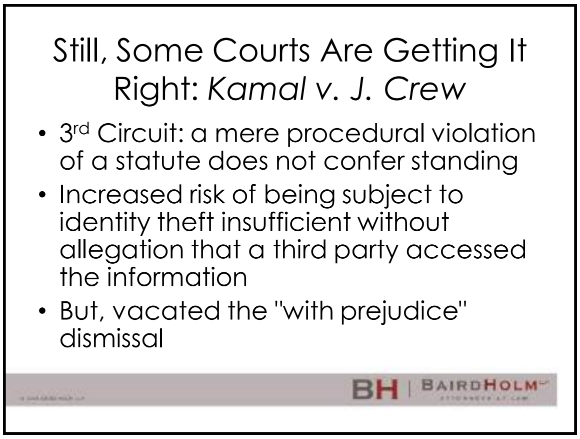
No Help From *Spokeo II*

- 9th Circuit still found standing:
  - FCRA intended to protect consumer
  - This interest is concrete
  - Legitimate and material risk of actual harm because false information may be significant to prospective employers
    - (Even though Robins did not allege that any prospective employer did not hire him based on credit report)



No Help from SCOTUS

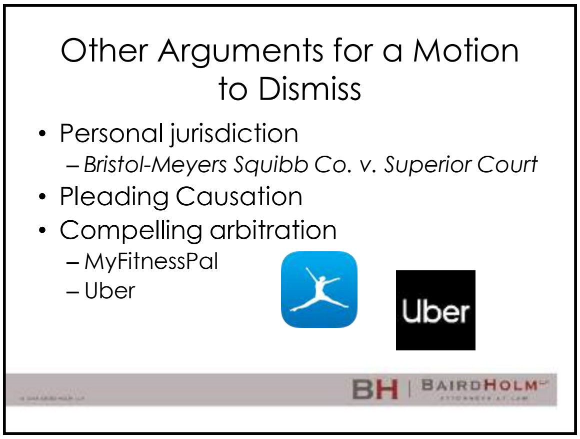
- Denied *Spokeo II* petition for certiorari
- Remanded with little guidance in *Frank v. Gaos*
- Turned away appeal in *Zappos.com v. Stevens*



Still, Some Courts Are Getting It Right: *Kamal v. J. Crew*

- 3rd Circuit: a mere procedural violation of a statute does not confer standing
- Increased risk of being subject to identity theft insufficient without allegation that a third party accessed the information
- But, vacated the "with prejudice" dismissal

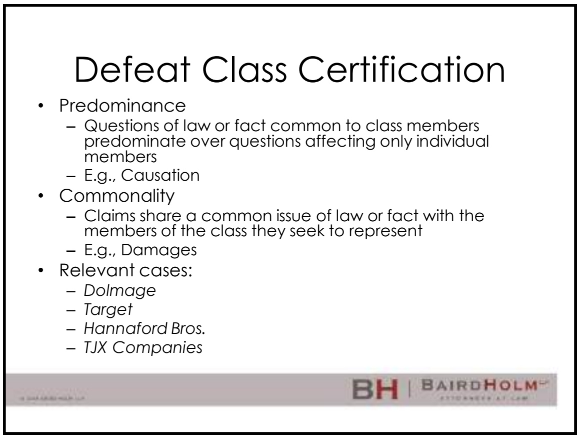
The Court found standing…now what?



Other Arguments for a Motion to Dismiss

- Personal jurisdiction
  - *Bristol-Meyers Squibb Co. v. Superior Court*
- Pleading Causation
- Compelling arbitration
  - MyFitnessPal
  - Uber

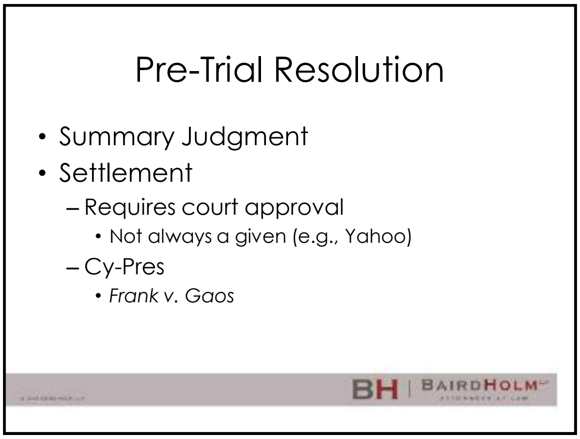
Uber
BH | BAIRDHOLM



Defeat Class Certification

- Predominance
  - Questions of law or fact common to class members predominate over questions affecting only individual members
  - E.g., Causation
- Commonality
  - Claims share a common issue of law or fact with the members of the class they seek to represent
  - E.g., Damages
- Relevant cases:
  - *Dolmage*
  - *Target*
  - *Hannaford Bros.*
  - *TJX Companies*

BH | BAIRDHOLM



Pre-Trial Resolution

- Summary Judgment
- Settlement
  - Requires court approval
    - Not always a given (e.g., Yahoo)
  - Cy-Pres
    - *Frank v. Gaos*

BH | BAIRDHOLM

Questions?

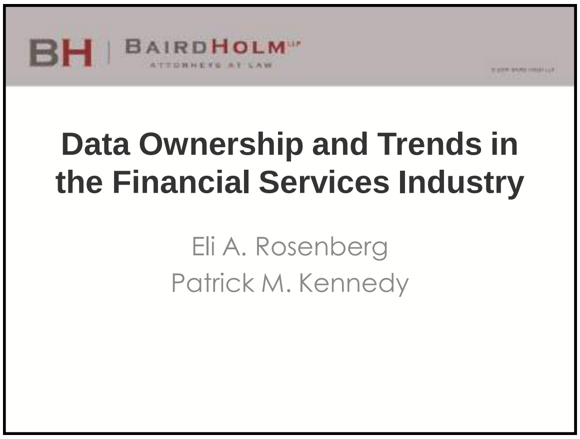
Vickie B. Ahlers
vahlers@bairdholm.com
(402) 636 – 8230

Allison D. Balus
abalus@bairdholm.com
(402) 636 – 8254

Krista M. Eckhoff
keckhoff@bairdholm.com
(402) 636 – 8287

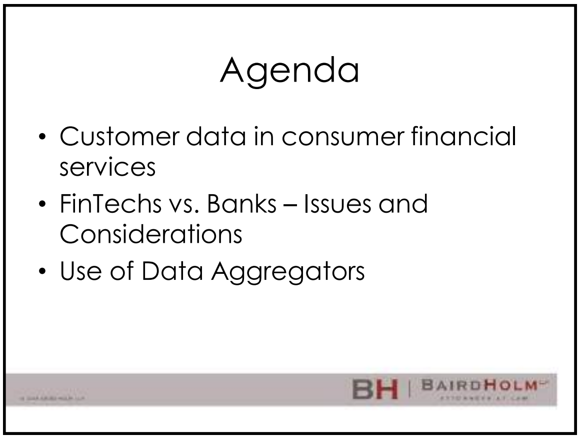
Data Ownership and Trends in the Financial Services Industry

Eli A. Rosenberg and Patrick M. Kennedy



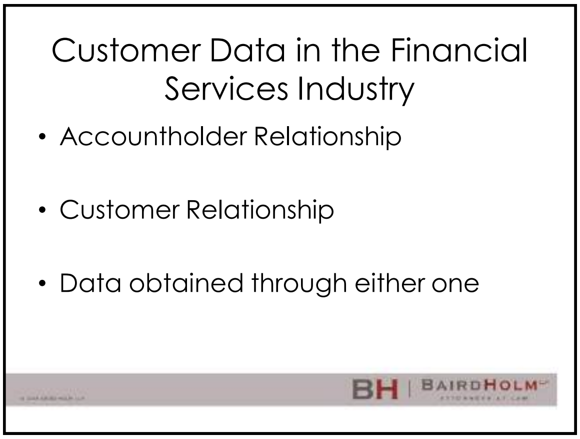
Data Ownership and Trends in the Financial Services Industry

Eli A. Rosenberg
Patrick M. Kennedy



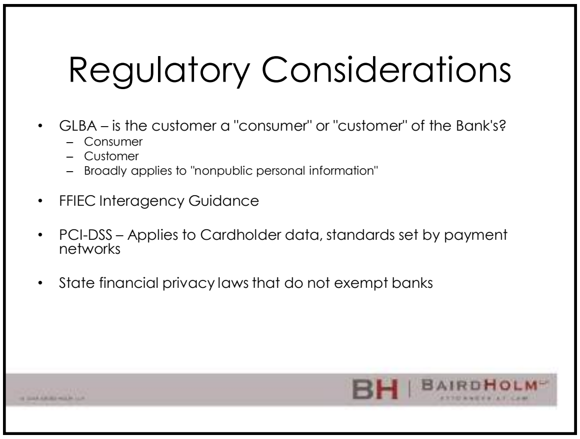
Agenda

- Customer data in consumer financial services
- FinTechs vs. Banks – Issues and Considerations
- Use of Data Aggregators



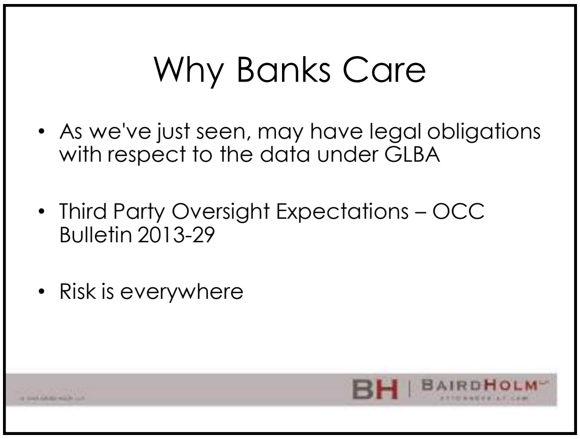
Customer Data in the Financial Services Industry

- Accountholder Relationship
- Customer Relationship
- Data obtained through either one



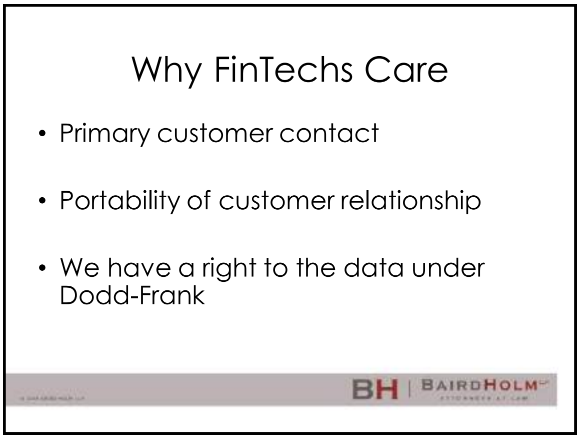
Regulatory Considerations

- GLBA – is the customer a "consumer" or "customer" of the Bank's?
  - Consumer
  - Customer
  - Broadly applies to "nonpublic personal information"
- FFIEC Interagency Guidance
- PCI-DSS – Applies to Cardholder data, standards set by payment networks
- State financial privacy laws that do not exempt banks



Why Banks Care

- As we've just seen, may have legal obligations with respect to the data under GLBA
- Third Party Oversight Expectations – OCC Bulletin 2013-29
- Risk is everywhere



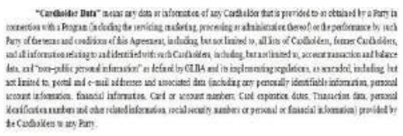
Why FinTechs Care

- Primary customer contact
- Portability of customer relationship
- We have a right to the data under Dodd-Frank

General Bank Position

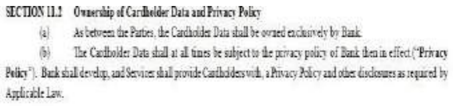
- Customer data is owned "exclusively" by Bank and the bank has all rights and interest with respect to sharing, use, disclosure of data
- Subject to the Bank's privacy policy
- FinTech – and any service provider of FinTech – only uses data as necessary to perform services
- Bank may convey joint ownership in "select data", but only if customer has not opted-out of sharing that data

Sample Contract Language



"Cardholder Data" means any data or information of any Cardholder that is provided to or obtained by a Party in connection with a Program (including the servicing, marketing, processing or administration thereof) or the performance by such Party of the terms and conditions of this Agreement, including, but not limited to, all lists of Cardholders, former Cardholders, and all information relating to and identified with such Cardholders, including, but not limited to, account transaction and balance data, and "non-public personal information" as defined by GLBA and its implementing regulations, as amended, including, but not limited to, postal and e-mail addresses and associated data (including any personally identifiable information, personal account information, financial information, Card or account numbers, Card expiration dates, Transaction data, personal identification numbers and other related information, social security numbers or personal or financial information) provided by the Cardholders to any Party.

Sample Contract Language

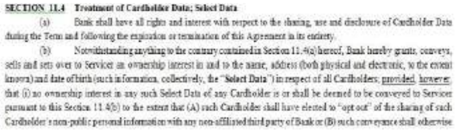


SECTION 11.2 Ownership of Cardholder Data and Privacy Policy

(a) As between the Parties, the Cardholder Data shall be owned exclusively by Bank.

(b) The Cardholder Data shall at all times be subject to the privacy policy of Bank then in effect ("Privacy Policy"). Bank shall develop, and Servicer shall provide Cardholders with, a Privacy Policy and other disclosures as required by Applicable Law.

Sample Contract Language



SECTION 11.4 Treatment of Cardholder Data; Select Data

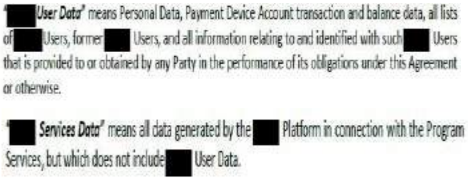
(a) Bank shall have all rights and interest with respect to the sharing, use and disclosure of Cardholder Data during the Term and following the expiration or termination of this Agreement in its entirety.

(b) Notwithstanding anything to the contrary contained in Section 11.4(a) hereof, Bank hereby grants, conveys, sells and sets over to Servicer an ownership interest in and to the name, address (both physical and electronic, to the extent known) and date of birth (such information, collectively, the "**Select Data**") in respect of all Cardholders; provided, however, that (i) no ownership interest in any such Select Data of any Cardholder is or shall be deemed to be conveyed to Servicer pursuant to this Section 11.4(b) to the extent that (A) such Cardholder shall have elected to "opt out" of the sharing of such Cardholder's non-public personal information with any non-affiliated third party of Bank or (B) such conveyance shall otherwise

New FinTech Position

- Two kinds of data
  - Program Data
  - FinTech Data
- Bank controls Program Data
- FinTech controls FinTech Data
- But –
  - Bank can only use/share Program Data to perform under agreement
  - FinTech can use / share Program Data to perform under agreement **and** use / share FinTech Data for any purpose (in accordance with the **FinTech's** privacy policy)

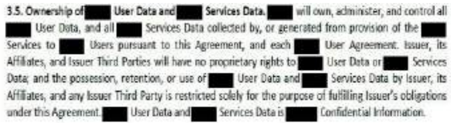
Sample Contract Language



"[redacted] *User Data*" means Personal Data, Payment Device Account transaction and balance data, all lists of [redacted] Users, former [redacted] Users, and all information relating to and identified with such [redacted] Users that is provided to or obtained by any Party in the performance of its obligations under this Agreement or otherwise.

"[redacted] *Services Data*" means all data generated by the [redacted] Platform in connection with the Program Services, but which does not include [redacted] User Data.

Sample Contract Langauge

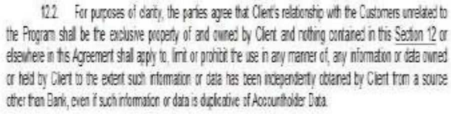


3.5. Ownership of [redacted] User Data and [redacted] Services Data. [redacted] will own, administer, and control all [redacted] User Data, and all [redacted] Services Data collected by, or generated from provision of the [redacted] Services to [redacted] Users pursuant to this Agreement, and each [redacted] User Agreement. Issuer, its Affiliates, and Issuer Third Parties will have no proprietary rights to [redacted] User Data or [redacted] Services Data; and the possession, retention, or use of [redacted] User Data and [redacted] Services Data by Issuer, its Affiliates, and any Issuer Third Party is restricted solely for the purpose of fulfilling Issuer's obligations under this Agreement. [redacted] User Data and [redacted] Services Data is [redacted] Confidential Information.

Compromise Position

- Three kinds of data
  - Bank Data
  - FinTech Data
  - Joint Data
- Bank owns its data, FinTech owns its data, Joint or "overlapping data" owned by both parties

Sample Contract Language

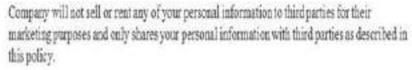


12.2. For purposes of clarity, the parties agree that Client's relationship with the Customers unrelated to the Program shall be the exclusive property of and owned by Client and nothing contained in this Section 12 or elsewhere in this Agreement shall apply to, limit or prohibit the use in any manner of, any information or data owned or held by Client to the extent such information or data has been independently obtained by Client from a source other than Bank, even if such information or data is duplicative of Accountholder Data.

Issue – Who's Privacy Policy Controls?

- From the customers perspective, they may only see one service provider
- But, information they provide may be subject to two differing privacy policies
- What happens in the event of a conflict between the two policies?

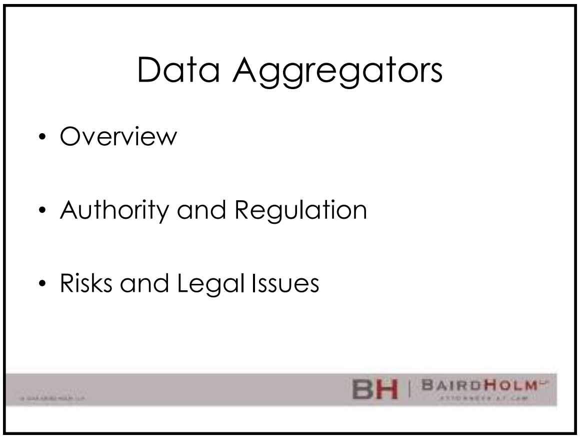
FinTech Privacy Policy



Company will not sell or rent any of your personal information to third parties for their marketing purposes and only shares your personal information with third parties as described in this policy.

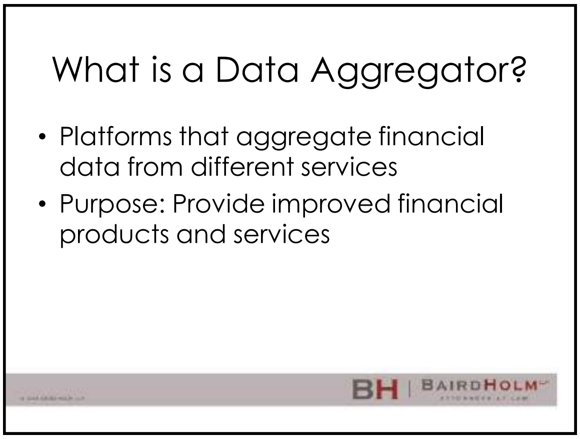
Bank Privacy Policy

- Bank will share information for –
  - Bank affiliate to market to you
  - Bank "non-affiliates" to market to you
- Non-affiliates we share with can include companies, such as direct marketing companies, insurance companies, non-profit organizations and mortgage companies



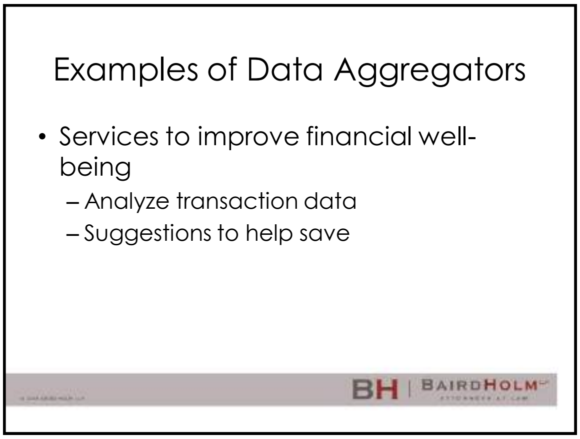
Data Aggregators

- Overview
- Authority and Regulation
- Risks and Legal Issues



What is a Data Aggregator?

- Platforms that aggregate financial data from different services
- Purpose: Provide improved financial products and services



Examples of Data Aggregators

- Services to improve financial well-being
  - Analyze transaction data
  - Suggestions to help save

Examples of Data Aggregators

- Eligibility determinations
  - Credit
  - Leasing

- Query: Is a data aggregator a consumer reporting agency?

Regulation of Data Aggregators

- No settled law
  - FCRA: FTC, CFPB
  - Dodd-Frank/UDAAP: FTC, CFPB
- CFPB Principles of Data Aggregation
- Dept. of Treasury July 2018 Report
- Private regulation

CFPB Principles of Data Aggregation

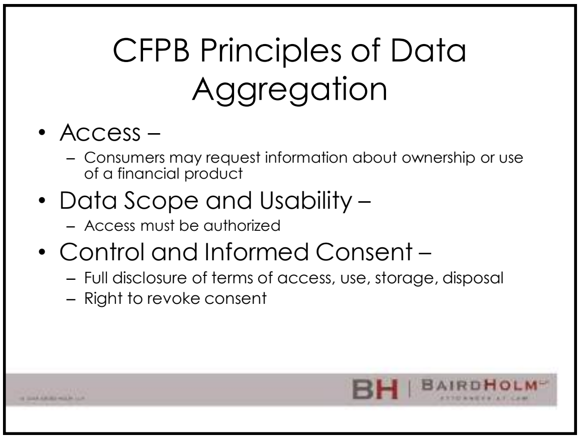
cfpb Consumer Financial Protection Bureau

1700 G Street N.W., Washington, D.C. 20552

October 18, 2017

Consumer Protection Principles:
Consumer-Authorized Financial Data Sharing and Aggregation

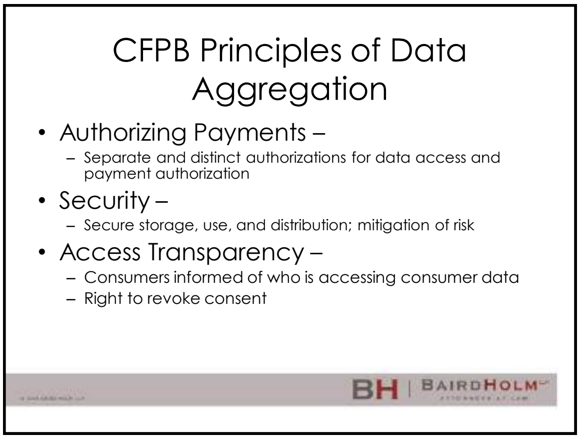
- Issued October 2017
  - Affirmed by Mulvaney CFPB
- Consumer protection focus
  - Questionable effect



CFPB Principles of Data Aggregation

- Access –
  - Consumers may request information about ownership or use of a financial product
- Data Scope and Usability –
  - Access must be authorized
- Control and Informed Consent –
  - Full disclosure of terms of access, use, storage, disposal
  - Right to revoke consent

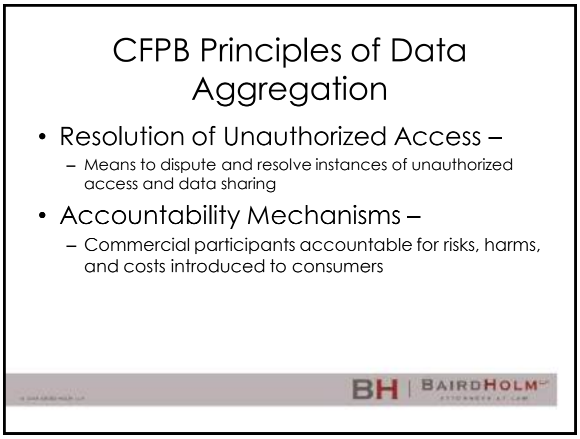
BH | BAIRDHOLM



CFPB Principles of Data Aggregation

- Authorizing Payments –
  - Separate and distinct authorizations for data access and payment authorization
- Security –
  - Secure storage, use, and distribution; mitigation of risk
- Access Transparency –
  - Consumers informed of who is accessing consumer data
  - Right to revoke consent

BH | BAIRDHOLM



CFPB Principles of Data Aggregation

- Resolution of Unauthorized Access –
  - Means to dispute and resolve instances of unauthorized access and data sharing
- Accountability Mechanisms –
  - Commercial participants accountable for risks, harms, and costs introduced to consumers

BH | BAIRDHOLM

Treasury Report

U.S. DEPARTMENT OF THE TREASURY

A Financial System
That Creates Economic Opportunities

**Nonbank Financials, Fintech,
and Innovation**

JULY 2018

BH | BAIRDHOLM LLP
ATTORNEYS AT LAW

Risks and Legal Issues

- FCRA
- UDAAP
- Privacy concerns

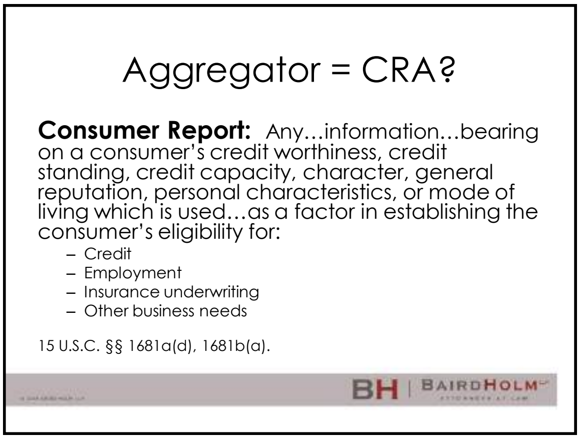
BH | BAIRDHOLM LLP
ATTORNEYS AT LAW

Aggregator = CRA?

Consumer Reporting Agency: Any person which…for fees…regularly engages…in the practice of assembling or evaluating consumer credit information…for the purpose of furnishing **consumer reports** to third parties

15 U.S.C. § 1681a(f).

BH | BAIRDHOLM LLP
ATTORNEYS AT LAW

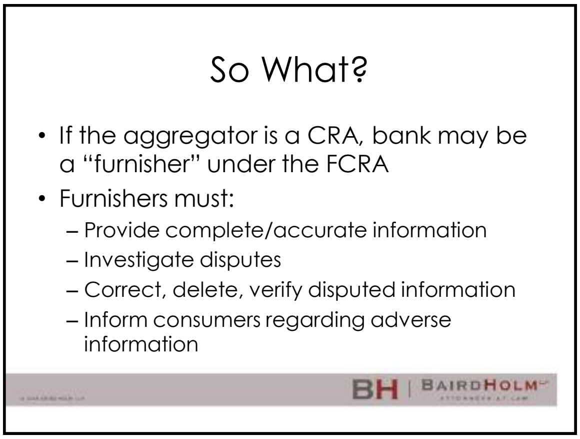


Aggregator = CRA?

Consumer Report: Any…information…bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used…as a factor in establishing the consumer's eligibility for:

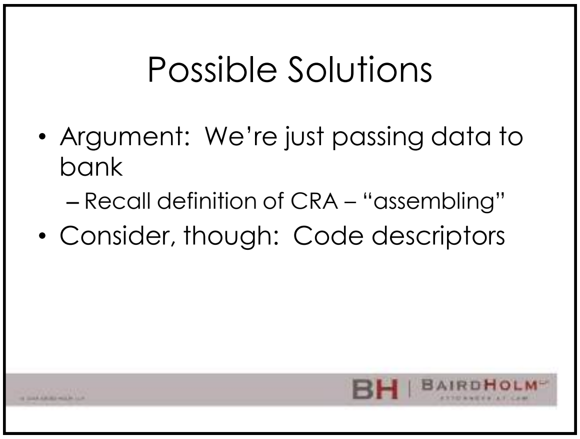
- Credit
- Employment
- Insurance underwriting
- Other business needs

15 U.S.C. §§ 1681a(d), 1681b(a).



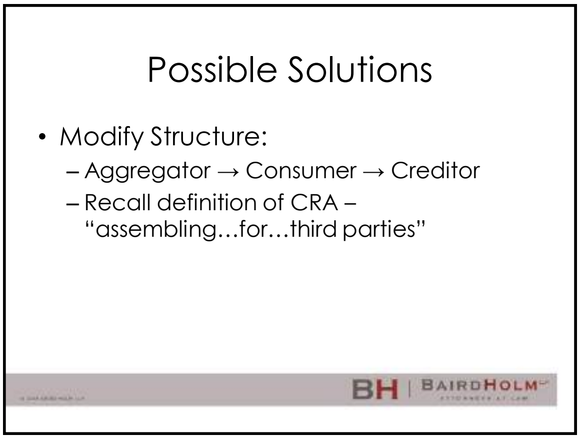
So What?

- If the aggregator is a CRA, bank may be a "furnisher" under the FCRA
- Furnishers must:
  - Provide complete/accurate information
  - Investigate disputes
  - Correct, delete, verify disputed information
  - Inform consumers regarding adverse information



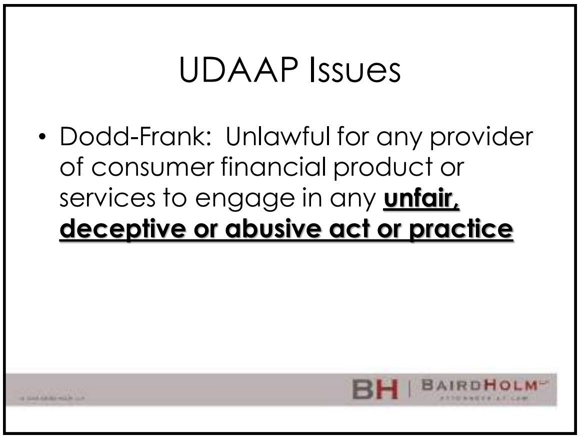
Possible Solutions

- Argument: We're just passing data to bank
  - Recall definition of CRA – "assembling"
- Consider, though: Code descriptors



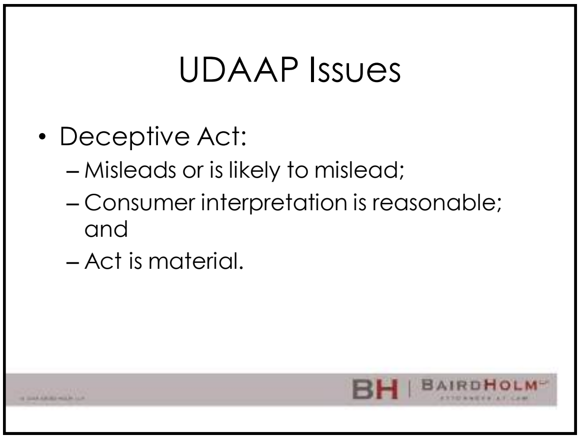
Possible Solutions

- Modify Structure:
  - Aggregator → Consumer → Creditor
  - Recall definition of CRA – “assembling…for…third parties”



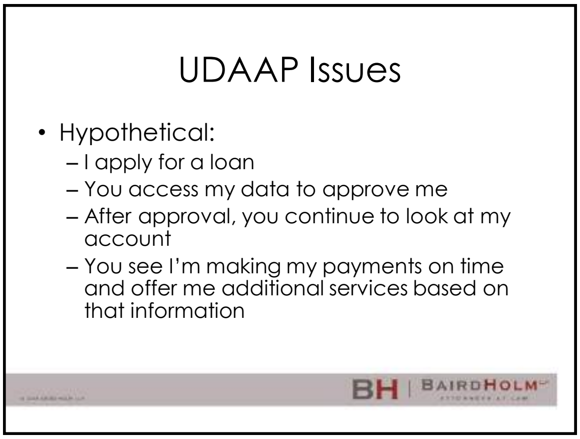
UDAAP Issues

- Dodd-Frank: Unlawful for any provider of consumer financial product or services to engage in any **unfair, deceptive or abusive act or practice**



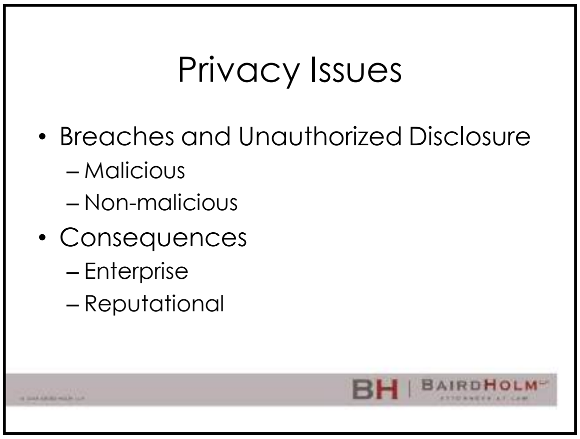
UDAAP Issues

- Deceptive Act:
  - Misleads or is likely to mislead;
  - Consumer interpretation is reasonable; and
  - Act is material.



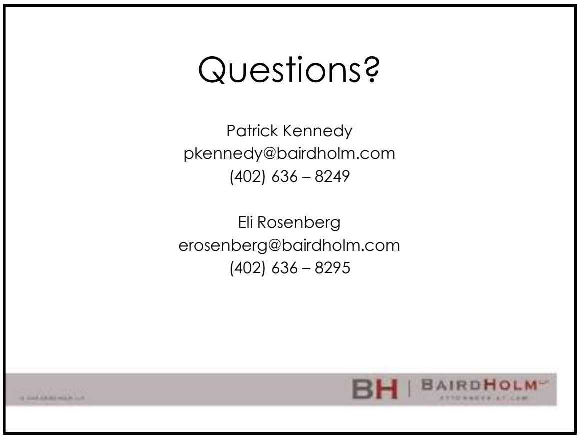
UDAAP Issues

- Hypothetical:
  - I apply for a loan
  - You access my data to approve me
  - After approval, you continue to look at my account
  - You see I'm making my payments on time and offer me additional services based on that information



Privacy Issues

- Breaches and Unauthorized Disclosure
  - Malicious
  - Non-malicious
- Consequences
  - Enterprise
  - Reputational



Questions?

Patrick Kennedy
pkennedy@bairdholm.com
(402) 636 – 8249

Eli Rosenberg
erosenberg@bairdholm.com
(402) 636 – 8295