PROGRAM MATERIALS
Program #2991
September 18, 2019

Data Breaches – Preparing and Responding to Breaches in An Evolving Legal Landscape

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

IfrahLaw
Hands-on Counsel, Gloves-off Litigation

ifrahlaw.com

Data Breaches – Preparing and Responding to Breaches in An Evolving Legal Landscape

Michelle W. Cohen, Esq.

Certified Information Privacy Professional – U.S.

Ifrah, PLLC

Why It Matters

- Data breaches and identity theft are a daily occurrence. Increased public awareness and the demand for greater responsibility and accountability for custodians of personal data has followed.
- At least 4 billion records, including credit card numbers, home addresses, phone numbers, and other highly sensitive information, have been exposed through data breaches in 2019.
- Per Experian, 31% of data breach victims later have their identity stolen.
- Facebook, Google, Amazon and Apple have all experienced data breaches.

STATISTICS

Data Breach Statistics: *What is the Threat Level?*

- A cyberattack occurs every 39 seconds (University of Maryland)
- 1,244 data breaches, exposing 446.5 million records, in the U.S. in 2018 (Statista)
- Cyberattacks are one of the top three risks to global stability (World Economic Forum)
- As of 2015, 25 percent of global data required security but was not protected (Statista)

Data Breach Statistics: *What are the Costs?*

- Average cost of a data breach → $3.86 million (IBM)
- Lost business cost after a breach → $4.2 million (IBM)
- Average cost of a mega breach of 1 million+ records → $40 million (IBM)
- Average cost of mega breach of 50 million+ records → $350 million (IBM)
- Follow-on issues:
  - Brand and reputation
  - On the regulatory radar
  - Class actions

HEADLINERS

Recently Announced Data Breaches - 2019

- Poshmark – August 1, 2019 – 50 million users affected
- Capital One – July 29, 2019 – 100 million users affected
- Los Angeles County Department of Health Services – July 10, 2019 – 14,600 patients
- Labcorp – June 4, 2019 – 7.7 million users affected
- Quest Diagnostics – June 3, 2019 – 11.9 million users affected
- First American – May 25, 2019 – 885 million users affected

Headline Data Breaches

Capital One

- Incident
  - July 29, 2019: data breach announced; 106 million individuals affected
- Legal Ramifications
  - July 30, 2019: class action complaint filed in U.S. District Court for the District of Columbia (*Zosiak v. Capitol One Financial Corporation, et al.,* Case No.1:19-cv-02265)
    → *It does not take long for class action suit to follow a data breach announcement*.
  - Forthcoming?: FTC enforcement likely

Headline Data Breaches

Facebook

- Incidents
  - April 2019: 540 million records affected
  - September 2018: 50 million user accounts affected
  - March 2018: FB discloses that 87 million +/- users exposed in Cambridge Analytica scandal
- Legal Ramifications, *inter alia* …
  - Multiple federal investigations
  - Multiple consumer actions still pending
  - FTC settlement for $5 billion
  - SEC settlement for $100 million
  - Congressional investigations

Headline Data Breaches

Equifax

- Incident
  - September 2017: data breach announced; 147 million individuals affected
- Legal Ramifications
  - FTC
    - $575 million+ settlement
    - Free credit monitoring and identify theft services
  - Class action: company is pledging up to $2 billion for consumers impacted by the breach

LEGAL LANDSCAPE

The Legal Landscape: Overview

- What laws govern?
- How is data breach defined?
- What must a company do to protect against a data breach?
- What are a company's obligations in the event of a breach (to notify/mitigate/remediate)?
- What is the legal exposure for a data breach?

The Legal Landscape: Federal Level

- Status
  - No general federal law covering data breaches (or data security or privacy, for that matter)
  - Instead, there are
    - Several federal laws addressing specific industries or individual groups
      - » E.g., Gramm-Leach-Bliley Act for financial institutions
      - » E.g., Health Insurance Portability and Accountability Act ("HIPPA") and Health Information Technology for Economic and Clinical Health Act ("HITECH") for healthcare industry
    - Patchwork of state laws with varying security and notice obligations
- Implications
  - The circumstances of a data breach will trigger different notice and reporting obligations based upon whether any federal laws are implicated and what states are involved
  - **Any company dealing with a nationwide data breach must address compliance obligations for all 50 states**

The Legal Landscape: Federal Level

- Nuances from the patchwork of laws
  - What entities must comply?
  - What are the data protection standards?
  - What data must be protected?
  - What is considered a breach? (access to or unauthorized use of?)
  - What measures must a company undertake in the event of a breach?
  - Who must be notified of a breach (Individuals? Regulators?) and when?
  - What information must a notice contain?
  - What remediation must the entity offer to impacted individuals?
  - What are the legal ramifications? (Can individuals sue? Is there personal liability exposure?)

The Legal Landscape: Federal Level

Gramm-Leach-Bliley Act

- Overview: federal law that applies to financial institutions (NOTE: the definition of "financial institutions" is quite broad)
- Data security obligations: financial institutions must develop, implement and maintain administrative, technical and physical safeguards to protect the security, integrity and confidentiality of "nonpublic personal information"
- Data breach definition: unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer
- Notification requirements: if, upon analysis, conclude that "misuse of its information about a customer has occurred or is reasonably possible," should notify customer as soon as possible (risk-of-harm analysis)
- Liability: no private cause of action but officers and directors can be fined up to $10,000 for each violation, and criminal penalties include imprisonment for up to five years, a fine, or both
- NOTE: Proposed changes to regulations forthcoming (comment period ended in August)

The Legal Landscape: Federal Level

Health Insurance Portability and Accountability Act ("HIPPA") and Health Information Technology for Economic and Clinical Health Act ("HITECH")

- Overview: federal laws applying to health plans, health care clearinghouses, health care providers and their business associates
- Data security obligations: entities must ensure the confidentiality, integrity and availability of electronic personal health information and to protect against reasonably anticipated potential breaches
- Data breach definition: the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information"
- Notification requirements: entities must provide notice to individuals, Health and Human Services, and major print or broadcast media for breaches that impact more than 500 residents in a state
- Liability: no private right of action but HHS and state attorneys general can file civil actions for damages and injunctions

The Legal Landscape: Federal Level

Legislative Developments

- House and Senate Commerce and Judiciary Committees have held hearings on topics related to consumer data privacy
- Senator Ron Wyden (D-OR) released a draft *Consumer Data Protection Act*, which would expand the FTC's regulatory and enforcement powers to, among other things, establish minimum national data privacy and cybersecurity standards
- Senator Brian Schatz (D-HI) released the draft *Data Care Act*, which would require online providers to establish practices to reasonably secure personal data, require those providers to promptly inform users of data breaches that involve sensitive information, and would enhance the FTC's regulatory and enforcement powers

Presenter to read NY Code

This code is required for all attorneys wishing to receive CLE credit in the state of NY and taking the program 'on-demand' at Celesq AttorneysEd Center either online or via CD

Please notate it carefully

The presenter will only be able to read the code twice and will not be able to repeat it or email it to you.

Thank you!

The Legal Landscape: State Level

Overview

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted breach notification laws
- These laws typically address
  - Who must comply with the law (e.g., businesses, data brokers, government entities)
  - What is "personal information" under their law (e.g., name, SSN, drivers license, account numbers, etc.)
  - What constitutes a breach (e.g., unauthorized acquisition of data)
  - Notification requirements (e.g., timing or method of notice, who must be notified)
  - Exemptions (e.g., for encrypted information)
- In 2019, at least 21 states have considered measures that would amend existing security breach laws
- Illinois, Maryland, Massachusetts, New Jersey, New York, Oregon, Texas, and Washington recently amended their breach notification laws to expand their definitions of personal information and/or to include new reporting requirements

The Legal Landscape: State Level

Overview (cont'd)

- Trends in state legislation this year, according to the National Conference of State Legislatures, include:
  - Expanding the definition of "personal information" (e.g., to include biometric information, email address with password, passport number, etc.).
  - Setting or shortening the timeframe for notification.
  - Mandating breach notice to the state attorney general.
  - Providing for free credit freezes or identity theft protection for victims of data breaches.

The Legal Landscape: State Level: California

California Consumer Privacy Act (CCPA)

- Effective date: January 1, 2020
- Who is impacted: entities that,
  - do business in California,
  - collect (or have collected) personal information of California residents,
  - determine the purpose and means of processing of personal information, and
  - meet one or more of the following criteria:
    - annual gross revenues in excess of $25 million, adjusted for inflation;
    - annually buy, receive for a commercial purpose, sell or share the personal information of 50,000 or more consumers, households or devices; or
    - derive 50 percent or more of annual revenues from selling consumers' personal information
- Data security obligations: [under existing CA law] entities have a duty to implement and maintain reasonable security practices and procedures appropriate to the risk
- Data breach definition: an unauthorized acquisition of unencrypted personal information

The Legal Landscape: State Level: California

CCPA (cont'd)

- Notification requirements:
  - California residents have a right to be notified
  - When a company notifies 500+ California residents, a copy of the notification must be sent to the attorney general
  - Insurers and related entities must provide insurance commissioner with any information submitted to the attorney general
- Liability:
  - Consumer private right of action for certain data breaches involving data protection failures
    - Statutory damages range from $100 to $750 per consumer per incident
    - Courts may impose injunctive or declaratory relief
    - NOTE: entities have a 30-day period to cure violations
  - The attorney general may bring action for civil penalties of $2,500 per violation, or up to $7,500 per violation if intentional
    - NOTE: entities have a 30-day period to cure violations
- NOTE: Pending legislation of interest:
  - AB 1035: Would require entities to disclose a security breach within 72 hours following discovery or notification

The Legal Landscape: State Level: New York

New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act

- Effective date: March 2020
- Who is impacted: *any entity with private information about New York residents*

- Data security obligations: requires businesses to have "reasonable safeguards" for breach prevention
- Data breach definition:
  - The SHIELD Act expands the definition of a breach from unauthorized *acquisition of* private information to unauthorized *access to* private information
  - In determining whether unauthorized access has occurred, the SHIELD Act explains that businesses may consider "indications that the information was viewed, communicated with, used or altered"

The Legal Landscape: State Level: New York

SHIELD Act (cont'd)

- Notification requirements:
  - Risk-of-harm analysis: must notify individuals if determine that misuse or financial harm is likely to occur
  - No need to notify individuals if already notified under different breach notification regulation (e.g., GLBA, HIPPA)
  - Must maintain record of risk-of-harm analysis and determination; if the incident involves more than 500 New York residents, must submit risk-of-harm determination in writing to the attorney general within ten days after making determination
- Liability:
  - No private right of action
  - Statute of limitations for NYAG to bring action increased to three years under SHIELD
- Pending legislation of interest:
  - AB 1387: would impose a five-day time limit during which to disclose a breach

The Legal Landscape: State Level: Developments

- **Illinois** (SB 1624):
  - Amendment to the Personal Information Protection Act.
  - Effective January 1, 2020.
  - Requires businesses to notify the Attorney General of breaches involving at least 500 Illinois residents.
  - The Attorney General will be permitted to publish information concerning breaches.
- **Maryland** (HB 1154):
  - Amendment to the Personal Information Protection Act
  - Effective October 1, 2019.
  - The amended law: (1) expands the scope of businesses covered by the law to include businesses that own, license *or maintain* personal information of Maryland residents; (2) prohibits a business responsible for a breach from charging the applicable data owner or licensee for information needed for notification; and (3) prohibits business from using information "relative to the breach" for purposes other than providing notification regarding the breach, protecting or securing applicable personal information, and providing notification to certain information security organization to alert and avert future breaches.

The Legal Landscape: State Level: Developments

- **Massachusetts** (HB 4806):
  - Effective April 11, 2019.
  - The amendments require businesses to offer complimentary credit monitoring for 18 months if a breach involves a resident's Social Security number.
  - Breach notifications are to be provided on a rolling basis to avoid delay; and, if the exposed data is owned by a third party, then notice must identify that third party.
  - Businesses must inform state regulators as to whether they maintain "a written information security program."
- **New Jersey** (S. 52):
  - Effective September 1, 2019.
  - The amendments expand the definition of "personal information" to include.
  - If a breach occurs, businesses are required to notify affected New Jersey residents through written or electronic notice, directing them to promptly change their log-in credentials associated with that business, and any other accounts in which they use the same username or email address, password, or security questions/answers.
  - NOTE: If a resident's email account is the subject of the security breach, the business cannot provide electronic notice to that email.
  - Pending legislation of interest: AB 1360: would require certain notifications and free credit reports for customers following a breach.

The Legal Landscape: State Level: Developments

- **Oregon** (SB 684):
  - Effective January 1, 2020.
  - The Consumer Information Protection Act expands the definition of "personal information."
  - The law extends certain data breach notification requirements to vendors. Vendors must now notify any contracted "covered entity" within 10-days of discovering a breach of security, as well as the attorney general, if the breach involves more than 250 consumers or if the number of individuals effected is unknown. Notification to the attorney general is not required by vendors if the covered entity has already notified the attorney general.
- **Texas** (HB 4390):
  - Effective January 1, 2020.
  - Amendments to the Texas Identity Theft Enforcement and Protection Act law require businesses to send breach notifications (1) to affected individuals without "unreasonable delay," but no later than 60-days after identifying such breach, and (2) to the attorney general within 60-days of identifying the breach, provided that the breach effects at least 250 Texas residents.
  - The law establishes a Texas Privacy Protection Advisory Council consisting of 15 appointed members who are "to study data privacy laws in [the] state, other states, and relevant foreign jurisdictions."

The Legal Landscape: State Level: Developments

- **Washington** (HB 1071):
  - Effective March 1, 2020.
  - The law expands the definition of "personal information"
  - Businesses may send breach notifications by email, unless the breach involves the credentials associated with that email account.
  - If the breach effects more than 500 residents, then the entity must provide notice to the attorney general,
  - Entities must provide updated notice to the attorney general if any information required to be provided is unknown at the time the notice is filed.
  - The law reduces the prior 45-day notification timeline to 30-days.

GDPR

- "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. GDPR Article 4(12)
- Reporting personal data breaches
  - Containment
  - Assessment
    - What personal data impacted
      - "Sensitive or "special categories"?
    - Who impacted
    - Location of impacted individuals
  - Notifying regulators (timing, means, language)
    - If the breach is likely to result in a "risk to the rights and freedoms of natural persons"
    - Must report within 72 hours of becoming aware of incident
    - May need to have report translated
    - Need to identify how to file notice, which varies among authorities
    - If no Lead Supervisory Authority, notify every Supervisory Authority impacted
  - Notifying data subjects
    - If the breach is likely to result in a "high risk to the rights and freedoms of natural persons"
    - Notice in "clear and plain language" and local language
    - Contact details of DPO
    - Likely consequences and measures to be taken to mitigate breach
    - Direct communication if possible

CASE LAW

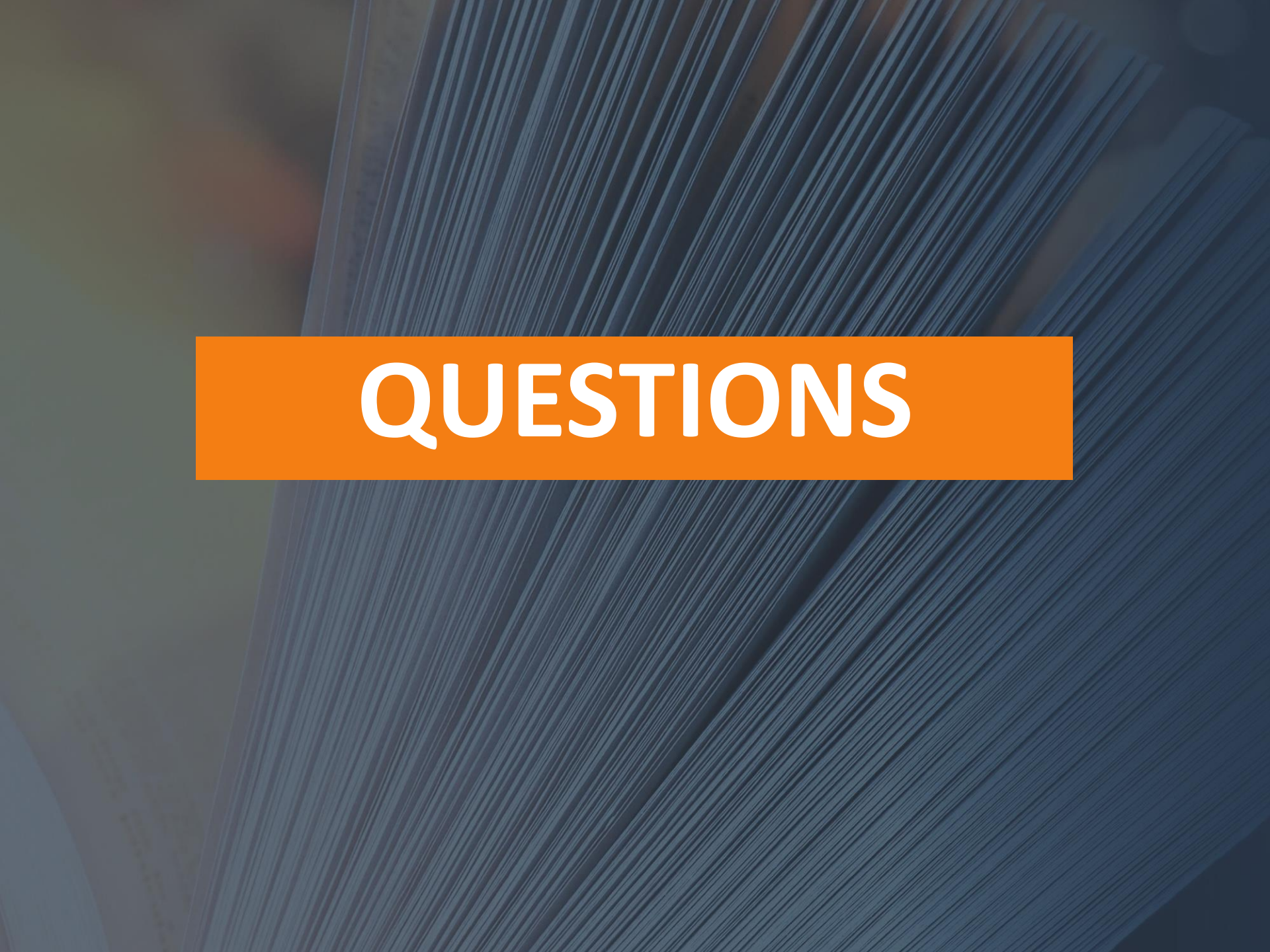
Court Split for Private Rights of Action

- Supreme Court: *Spokeo, Inc. v. Robins*
  - an injury must be both "concrete" *and* "particularized" to create standing
  - the "concreteness" element requires that an injury "actually exist"
- Sixth, Seventh, Ninth, and D.C. Circuits
  - a plaintiff can establish Article III standing at the pleading stage by alleging risk of future identity theft
  - NOTE: that doesn't mean they will survive a motion to dismiss for failure to state a claim where there is no alleged injury in fact: On remand, the D.C. District Court threw out most of the claims in the case on the defendants renewed motion to dismiss for failure to state a claim: "while plaintiffs' alleged injuries may be enough to establish standing at the pleading stage of the case, they are largely insufficient to satisfy the 'actual damages' element of nine of their state-law causes of action." *Attias v. CareFirst, Inc.*, No. 15-cv-00882(CRC), 2019 WL 367984 (D.D.C. Jan. 30, 2019)
- Second, Third, Fourth, and Eighth Circuits
  - a plaintiff cannot allege merely the risk of some future harm
  - allegations of injury that these courts have rejected:
    - including the increased risk of identity theft,
    - time spent monitoring or guarding against potential fraud,
    - diminished value of plaintiffs' personal information, and
    - not receiving the benefit of the bargain

RECOMMENDATIONS

Have a Plan

- Plan on a breach
  - A bad actor
  - A negligent employee
- Train employees
  - Data security
  - Data hygiene
  - Breach response
- Have a team in place
  - IT/IS, human resources, communications, legal, outside counsel
- Be able to
  - Contain the loss and fix the vulnerabilities
  - Assess the damage
  - Investigate, interview, work with forensics
- Have a communication plan for
  - Employees, customers, investors, business partners
- Have a notification plan for
  - Impacted individuals, authorities


QUESTIONS

Michelle W. Cohen

As Practice Group Leader for Ifrah Law's Data Protection and Cyber Security Group, Michelle Cohen assists clients with a wide range of issues, including data breaches and associated liabilities, litigation defense and counseling relating to consumer privacy issues, including the Telephone Consumer Protection Act, and federal and state agency investigations and enforcement actions, including the Federal Trade Commission, Federal Communications Commission, and state attorneys general. Michelle writes and speaks frequently on emerging topics in privacy, consumer protection, and the Internet. Michelle has extensive experience in arbitrations, mediation, and civil litigation. She has been a Certified Information Privacy Professional – U.S. for over ten years. Her *pro bono* activities include serving as Vice President-Legal & Secretary for the national non-profit the National Woman's Party at the Belmont-Paul Women's Equality National Monument.

Michelle's has been named by the National Law Journal as a Top Rated Lawyer for 2017 and 2018, a Top Rated Litigator for 2016, and a Cablefax Top Rated Lawyer for 2017 and 2018.

Michelle W. Cohen
Member
Ifrah PLLC
Telephone: 202.524.4144
Email: michelle@ifrahlaw.com