



Data Breach Response: *Discovery and Investigation*

September 10, 2020

**Chris Hart**

Partner, Co-Chair, Privacy & Data Security Practice

Foley Hoag LLP

617.832.1232

chart@foleyhoag.com

**Veronica Jennings**

Partner, Litigation Department

Foley Hoag LLP

202.261.7316

vjennings@foleyhoag.com

Agenda: Topics We Will Discuss Today

- 
- Data incidents and breaches
 - Pre-planning for an incident
 - The first 24 hours
 - Investigating breaches
 - Compliance considerations
 - Beyond the breach: liability and litigation
 - Takeaways

- Incidents v. Breaches
- When is an incident a breach?
- Why does the distinction matter?



Pre-Planning for an Incident



- Breach Response Plan
- Internal Reporting
- Outside vendors
 - Legal
 - Forensics
 - PR

The first 24 hours upon discovery of an incident are crucial:

- Business continuity
- Identification of incident
- Remediation
- Contacting stakeholders and vendors

- Document and evidence preservation
- Developing an investigation plan
- Investigations depend on root causes
 - Third/outside party
 - Insider threat
- Law enforcement involvement
- Internal v. external investigation
- Law & forensics





■ Individual Notifications

- Differ by jurisdiction
- Not immediate

■ Government Notifications

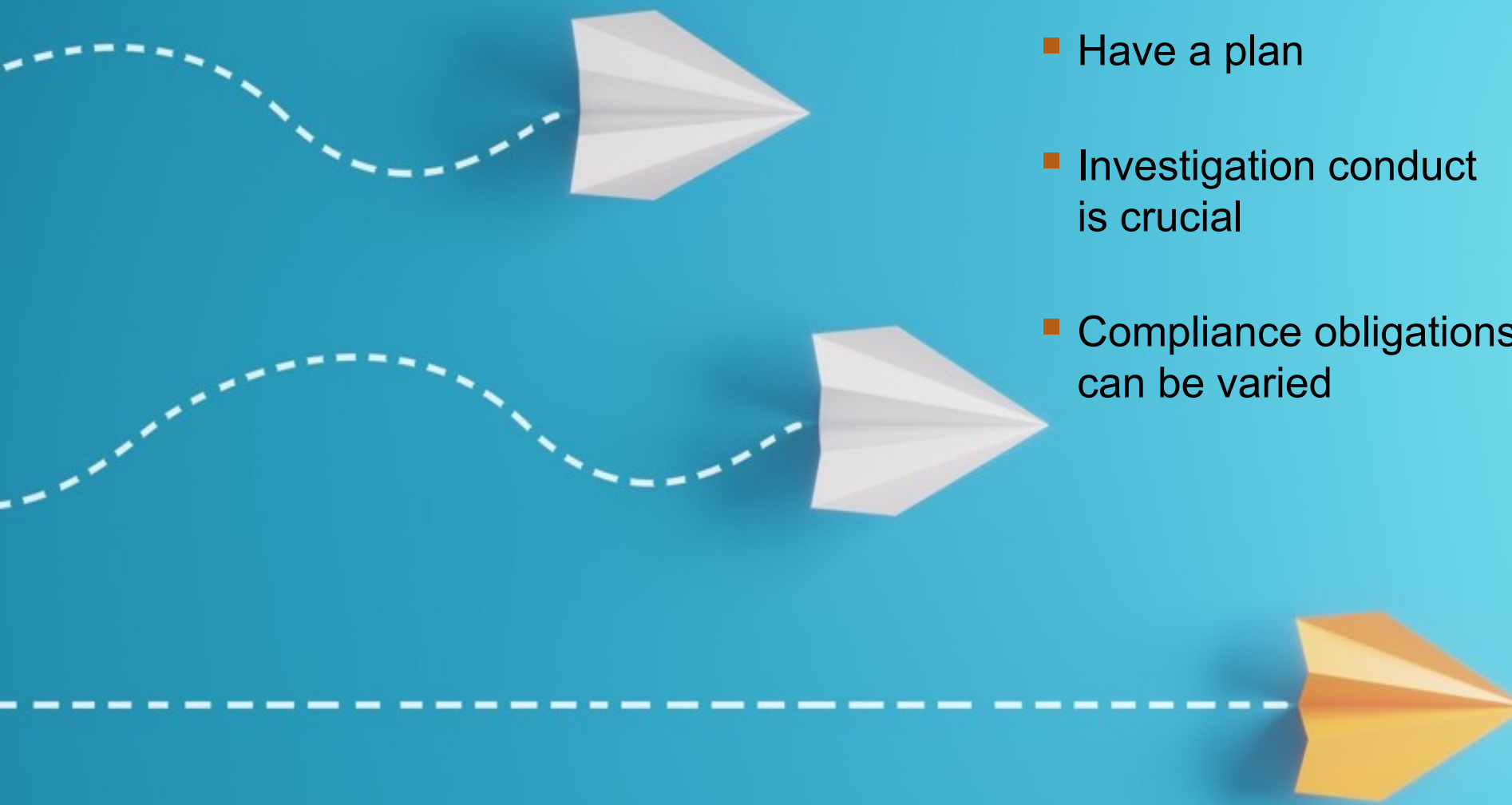
- Differ by jurisdiction
- Can be more immediate

■ Contractual Obligations

- Can differ greatly from regulatory requirements
- Not confined to personal information



- Insurance
- Government investigations
- Consumer litigation
- Counterparty litigation
- Criminal proceedings



- Have a plan
- Investigation conduct is crucial
- Compliance obligations can be varied
- Mitigate litigation risk but prepare for the worst



**FOLEY
HOAG LLP**

CYBERSECURITY INCIDENT RESPONSE TEAM

When your data security is compromised you need to act quickly: to resolve the breach, investigate what happened, make required notifications, consider contacting law enforcement and impacted individuals—all while maintaining continuity of your operations. Any compromise of your cybersecurity implicates a host of legal, technical, and personnel challenges. Foley Hoag can help you identify and address these issues.

Foley Hoag's Cybersecurity Incident Response Team includes lawyers from a number of the firm's practice areas—litigation, white collar criminal defense, and privacy and data security law. These lawyers have deep knowledge in the different substantive areas of law that cybersecurity issues can affect, such as finance and banking, securities, health care, and intellectual property. The Incident Response Team has worked extensively with federal and state law enforcement on cybersecurity issues

and has drafted breach response policies, trained personnel, assisted companies through data breaches (including compliance with the wide array of laws and regulations), and handled litigation stemming from data breaches. Our lawyers also have a network of contacts in related fields, including crisis management, computer forensics, and customer and public relations.

Whether you experience a data breach, need help with litigation resulting from a data breach, or want to plan your company's breach prevention and response strategy, **Foley Hoag's Cybersecurity Incident Response Team is ready to assist you.**



COLIN ZICK
617.832.1275
czick@foleyhoag.com



CHRISTOPHER HART
617.832.1232
chart@foleyhoag.com



VERONICA JENNINGS
202.261.7316
vjennings@foleyhoag.com



JEREMY MEISINGER
617.832.3029
jmeisinger@foleyhoag.com



RACHEL HUTCHINSON
617.832.3063
rhutchinson@foleyhoag.com



STEPHEN STICH
617.832.7157
sstich@foleyhoag.com

BOSTON | NEW YORK | PARIS | WASHINGTON, D.C.

FOLEYHOAG.COM

TEAM MEMBERS:

Colin Zick

Chris Hart

Veronica Jennings

Jeremy Meisinger

Rachel Hutchinson

Stephen Stich

SECURITY, PRIVACY AND THE LAW

LEGAL PERSPECTIVES ON THE EXPANDING UNIVERSE OF INFORMATION SECURITY & PRIVACY ISSUES

The Foley Hoag Security, Privacy and the Law Blog focuses on the security and privacy issues encountered by businesses that often require immediate and discreet solutions.

www.securityprivacyandthelaw.com

A Game of 'Cat and Mouse': Hacking Attacks on Hospitals for Patient Data Increase During Coronavirus Pandemic

Posted on [July 13th, 2020](#) by [Foley Hoag](#)

Colin Zick, co-chair of Foley Hoag's Healthcare and Privacy and Data Security Practice Groups, was recently quoted in USA Today about cyberattacks against health care providers. This is a particularly timely issue in the time of COVID-19. Click [here](#) to read the full article. [More](#)

 CATEGORIES: [Uncategorized](#)

   [Comments](#)  [Trackbacks](#)  [Tweet](#)  [Like 0](#)  [Share](#)

Watch Now: Maintaining Privacy and Data Security in the Remote Workplace

Posted on [June 24th, 2020](#) by [Foley Hoag](#)

The coronavirus pandemic has required a rapid and dramatic shift to remote work, raising important implications for workplace privacy and information security. Some of these concerns are new; others are the same concerns that employers have always held, now amplified by the increasingly blurred lines between work and home. All of these concerns will remain as the workplace travels from the office to the home and, in the near future,... [More](#)

 TAGS: [coronavirus](#), [remote work](#), [Covid-19](#), [data security](#), [information security](#), [privacy](#), [Privacy Policy](#)

CATEGORIES: [Uncategorized](#)

   [Comments](#)  [Trackbacks](#)  [Tweet](#)  [Like 0](#)  [Share](#)



THANK YOU.



FOLEY
HOAG LLP

Questions?