HSE INSTITUTE

INFORM. CONNECT. SHARE.

Two (and a Half) Weeks In: Ongoing Data Protection Concerns During the COVID-19 Pandemic

Webinar – April 1, 2020

F. Paul Greene, CIPP/US
Daniel J. Altieri
fgreene@hselaw.com
daltieri@hselaw.com

Overview

1. Regulatory Developments
2. Managing Data Protection Requirements in a State of Change
3. Incident Response Considerations
4. Developing Threats

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Regulatory Developments

- **New York**
  - No general amnesty or loosening of data protection requirements in recent Executive Orders
  - SHIELD Act effective as of 3/21/2020
    - Violation of SHIELD Act is an unfair/deceptive business practice, subject to fine
    - Administered by NY AG's office
    - Requests have been made to AG to put off enforcement of SHIELD Act
      - » No response yet
    - But – AG's office dealing with complaints concerning non-essential businesses continuing operation, price gouging

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Regulatory Developments

- **New York**
  - Fines under N.Y. Gen. Bus. Law § 899-aa (data breach notification requirement) can only be levied by a court
  - The same is true under N.Y. Gen. Bus. Law § 899-bb (adequate safeguards, written information security program requirement)
  - But N.Y. courts are closed and no filings are being accepted for non-essential matters
  - Two SHIELD Act traps
    - Compliant Regulated Entity
    - Small Business Carve Out?

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Regulatory Developments

- **The remaining 49 states**
  - No change in data breach reporting deadlines
    - Range from 30 days (FL) to "in the most expedient time possible and without unreasonable delay consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore the integrity of the system"
    - Other state AGs similarly busy with COVID-19 matters
    - But, for example, MA still publishing data breach report summaries: https://www.mass.gov/doc/data-breach-report-2020/download

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Regulatory Developments

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

COMMONWEALTH OF MASSACHUSETTS
Office of Consumer Affairs and Business Regulation
501 Boylston Street, Suite 5100, Boston, MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

MIKE KENNEALY
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

EDWARD A. PALLESCHI
UNDERSECRETARY

Data Breach Notification Report

Assigned Breach Number	Date Reported To OCA	Organization Name	Breach Type Description	Breach Occur at the Reporting Entity?	MA Residents Affected	SSNBreached	Account Number Breached	Drivers Licenses Breached	Credit Debit Numbers Breached	Provided Credit Monitoring	Data Encrypted	Mobile Device Lost Stolen
16653	3/18/2020	Robert Silman Associates Structural Engineers, D.P.C.	Electronic	Yes	1				Yes	Yes		
16654	3/18/2020	Banfi Products Corporation	Electronic	Yes	39	Yes		Yes		Yes		
16655	3/18/2020	The Village Bank	Electronic		2				Yes			
16652	3/19/2020	Firstmark Services	Electronic	Yes	1		Yes					
16661	3/19/2020	National Grid	Electronic	Yes	1	Yes		Yes		Yes		
16662	3/20/2020	Cirtec Medical Corporation	Electronic	Yes	583	Yes		Yes		Yes		
16663	3/20/2020	Discover Financial Services	Electronic		40				Yes			
16664	3/20/2020	General Electric Company	Electronic		487	Yes	Yes	Yes		Yes		
16665	3/20/2020	Savers Bank	Electronic		1				Yes			
16666	3/20/2020	Mutual One Bank	Electronic		1				Yes			
16667	3/20/2020	Adams Community Bank	Electronic		1				Yes			
16668	3/20/2020	Discover Financial Services	Electronic		9				Yes			
16669	3/20/2020	Family Ford, Inc. (d/b/a Family Ford of Enfield, Inc.)	Paper	Yes	218	Yes		Yes		Yes		
16659	3/20/2020	Steele County	Electronic	Yes	2			Yes				
16660	3/20/2020	Censeo Consulting Group Inc	Electronic	Yes	4	Yes				Yes		

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Regulatory Developments

- **HIPAA (February Guidance)**
  - Providers obligated to continue to implement reasonable safeguards to protect patient information against intentional and unintentional uses, and to continue to utilize administrative, physical, and technical safeguards to protect ePHI
  - Covered entities reminded that public health authorities (such as CDC or local designees) may be notified of infected patients to ensure public safety and to attempt to control disease
  - Minimum Necessary rule still applies. In the event of disclosure to public health authority, covered entities may rely on representations from the authority that what is being requested is the minimum necessary

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Regulatory Developments

- **HIPAA (March Guidance)**
  - On March 17, 2020, the Office of Civil Rights at HHS indicated that it would exercise enforcement discretion and allow covered entities to communicate with patients for telehealth services using previously non-compliant means of remote communication
    - Pre-COVID-19: Covered entities could use only HIPAA compliant communications, such as Skype for Business, Zoom for Healthcare, Updox.
    - COVID-19: Covered entities may now use non-public platforms, such as FaceTime, Skype, and Google Hangouts to provide telehealth services.
    - Public-facing platforms may not be used, such as TikTok, Facebook Live, and Twitch.

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Regulatory Developments

- **FERPA**
  - DOE has issued guidance to the effect that all applicable FERPA rules and exceptions remain in place
  - https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20and%20Coronavirus%20Frequently%20Asked%20Questions.pdf
  - Certain COVID-19 information can be shared, but subject to health and safety exception and then only to an "appropriate person"
    - The media is generally not an appropriate person
    - "rational basis" test

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Regulatory Developments

- **CCPA**
  - Industry advocates have requested a delay of enforcement until January 2, 2021
  - Consumer advocates have opposed
  - CA AG has indicated no general delay in enforcement
    - But, as a practical matter, enforcement resources may be limited
  - Private right of action looms
    - *Ring* case, filed in February, alleges private causes of action arising from failure to notify and failure to secure

HSE INSTITUTE
INFORM. CONNECT. SHARE.

- **Transparency**
  - Truthful and accurate data processing disclosures required under CA, NV law, and under FTC Act
    - Generally required in the court of public opinion
    - Assess changes to data processing activities and whether you need flexibility in your disclosures
    - "in emergency situations, **[Company]** may share your personal information with other categories of third parties to allow **[Company]** to continue providing services to you, and/or maintain its operations"
    - Any substantive change in processing or sharing should be prospective only

HSE INSTITUTE
INFORM. CONNECT. SHARE.

- **Security**
  - Here too, you're actions should correspond to your disclosures
  - Avoid absolutes
  - Consider flexibility
  - "In this time of crisis, security risks have only increased. At **[Company]**, we take these threats seriously, and are taking steps to address them. Despite our best efforts, however, we may not be able to counter every threat we face, but we will always do our best to protect your information."
  - Educate, educate, educate
  - Empower reporting of security concerns

HSE INSTITUTE
INFORM. CONNECT. SHARE.

- **Privacy**
  - You may not be prohibited from sharing COVID-19 and coronavirus information concerning your employees, but you may want to refrain from doing so
  - "Don't be creepy" – don't use information your customers or employees would consider to be private without disclosing the use beforehand
    - Geolocation
    - Sale, sharing, data co-ops
    - Other inferences, propensity scores

HSE INSTITUTE
INFORM. CONNECT. SHARE.

- **Risk**
  - Now is certainly not the time to engage in a full blown Risk Assessment, unless you are able
  - It is also not the time to assume that your last Risk Assessment still applies or was even adequate
  - Risk Assessments must be updated "as needed to continue provision of reasonable and appropriate protection of [e]PHI" under HIPAA, for example
  - Under the SHIELD Act, you must "identif[y] reasonably foreseeable internal and external risks," and then "assess" those risks in eight separate arenas
  - Consider a Risk Assessment refresh in light of COVID-19-related changes, internally and externally

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Incident Response Considerations

- **The role of insurance**
  - Password protect your policy, or at least keep it safe
  - Review your policy, and have it available remotely (or locally, in a secure fashion) for those that decide whether to make a claim
  - Err on the side of notice, unless your broker tells you otherwise
  - Know whom you will be talking to, when you provide notice
  - Review your existing relationships – are they covered?
  - Understand your retention levels and sublimits
  - Do you have any post-incident remediation coverage?

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Incident Response Considerations

- **Communications – IR Team**
  - How well is your remote meeting platform working?
  - Do you have a separate, secure line for IR communications?
  - Who has access to those credentials? Can they be changed?
  - Back up communication platform if e-mail goes down or is compromised?
  - Back up telephone lines?
  - Apply the attorney-client privilege at the first indication of a potentially material or reportable “breach”
  - Be aware of group chats and “reply to all”
  - Be aware of limited role of IT infrastructure companies, other support vendors, in IR process – they can be fatal to privilege

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Incident Response Considerations

- **Communications - External**
  - Do you have a crisis communication plan? Does it cover cyber?
  - How will you harmonize any cyber-related messaging with COVID-19 messaging
  - Do you already work with a PR firm? Do they have experience in cyber? Will your carrier pay for their services?
  - Be aware of the internal to external communication pathway
  - The good news:
    - cyber-related disruptions may not be as noticeable
    - cyber incidents may not make the news as easily as before

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Incident Response Considerations

- **Ransomware**
  - Ransomware as a Service
    - Usually involves longer periods of persistence
    - Can bring with it more detailed reconnaissance into your organization
      - Roles/responsibilities
      - Home and cell numbers, personal e-mail addresses
      - Insurance limits
      - Pending deals
    - If they can't sell the compromise, they will detonate the ransomware payload on the way out

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Incident Response Considerations

- **Ransomware**
  - Can come with the threat to publish exfiltrated information
    - "dirty" financial information
    - sensitive personal information
  - Is your IR team ready to handle a very active attacker in this vein?
    - Internal messaging is key
    - Working with law enforcement can limit effect of attacker posts
    - What will you say when Krebs or Bleepingcomputer requests a statement?

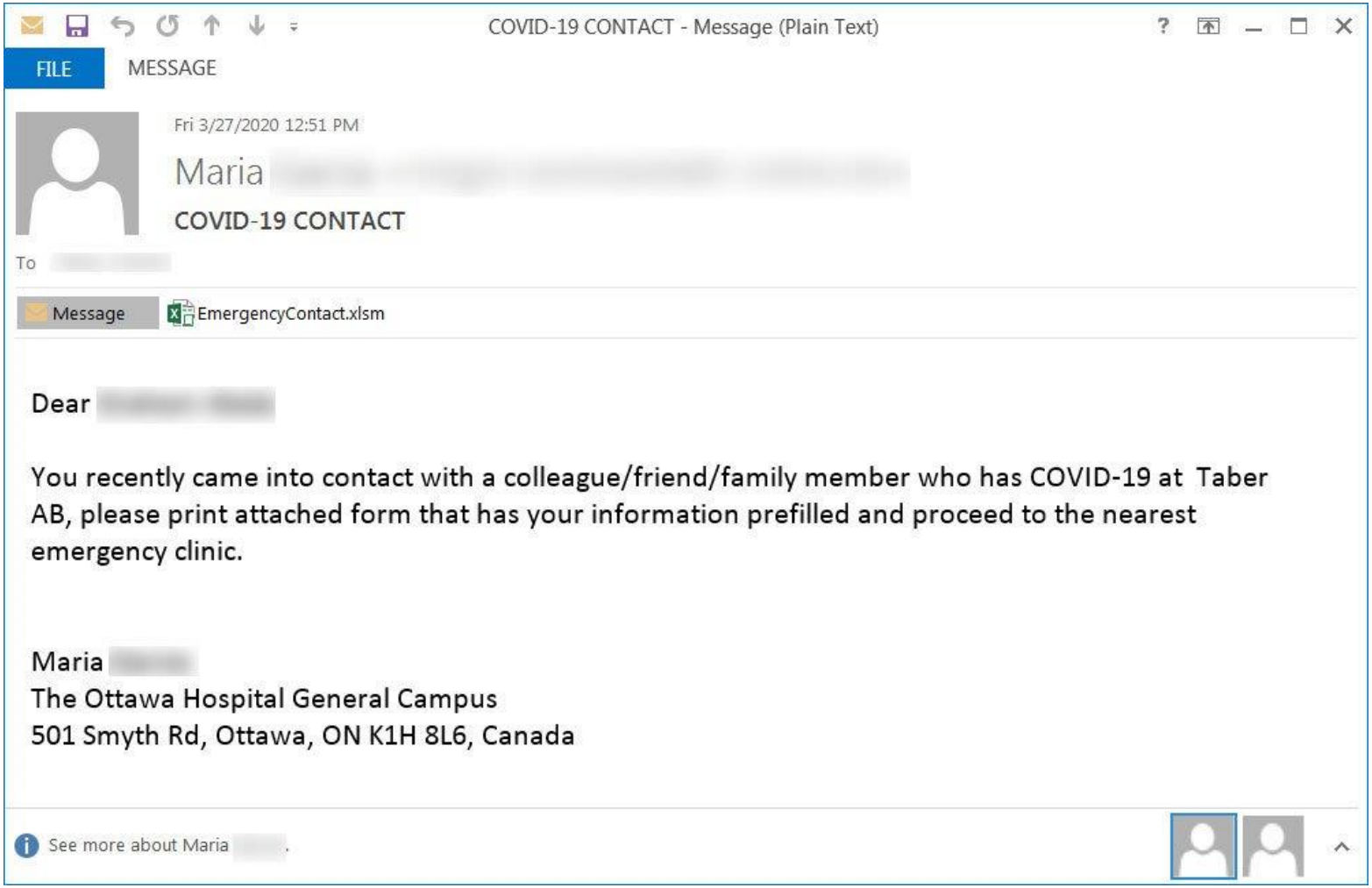
HSE INSTITUTE
INFORM. CONNECT. SHARE.

Developing Threats

- **COVID-19 Related Attacks**
  - CDC Alerts
  - Health advisories
  - Stimulus checks, CARES Act
  - Workplace policy updates, *e.g.*, Communicable Disease Management Policy
  - Some organizations are filtering COVID and coronavirus related e-mails, but that may not work for everyone
  - Won't work against fake ads, other malvertising

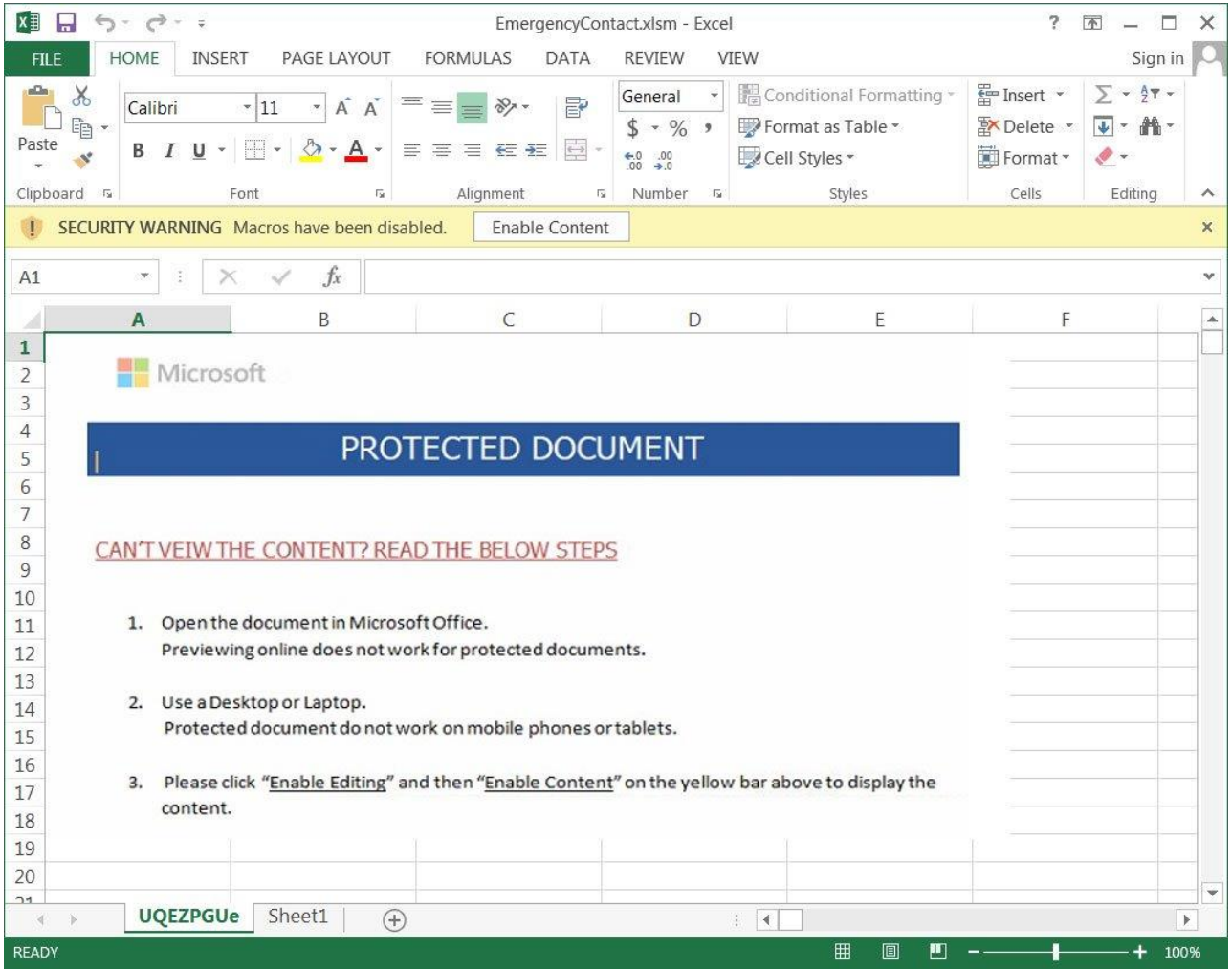
HSE INSTITUTE
INFORM. CONNECT. SHARE.

Developing Threats



HSE INSTITUTE
INFORM. CONNECT. SHARE.

Developing Threats



HSE INSTITUTE
INFORM. CONNECT. SHARE.

Developing Threats

- **Attacks directed at remote work environment**
  - 0365 compromises
  - Help desk impersonations
  - Credential scraping, keylogging
  - Coronavirus app exploits
  - Sextortion demands
  - Drive by ransomware attacks

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Developing Threats

- **Attacks directed at remote work environment**
  - Zoombombing
  - Bogus Zoom domain names

HSE INSTITUTE
INFORM. CONNECT. SHARE.

How to Manage COVID-19 Risk

- Be sure employees are ready for the challenge. Focus on low-hanging fruit:
  - A simple email reminder to be on the lookout for phishing scams will go a long way
  - Especially now, consider email banner identifying external emails to help highlight spoofing senders
  - Wire transfer controls – implement voice confirmation, at a minimum
- To the extent possible, have employees work from employer-owned (not personal) devices
  - Otherwise, consider patching and endpoint protection gaps

HSE INSTITUTE
INFORM. CONNECT. SHARE.

How to Manage COVID-19 Risk

- Patch and scan! Don't stop your good work when it's needed most
- Now is the time to make sure everyone is on the same page (literally)
  - What policies have been invoked because of the crisis? What policies matter more now?
- MFA implementation
  - If not currently using, consider whether remote work has led to a change in access rights, such that risk has increased
  - Review administrative rights: are they necessary for every user that has them?

HSE INSTITUTE
INFORM. CONNECT. SHARE.

What's next?

- **Who knows?**
  - It is almost certain that new security risks and exploits will arise, tailored to the new threats we face
  - A new privacy scandal will almost certainly occur
    - The NY AG is already making inquiries of Zoom for its privacy and security practices
  - The full regulatory response has yet to be felt
    - State actions have yet to catch up with the new risks we face
    - Regulations move much more quickly than legislation
    - Executive orders/federal guidance can change the rules
    - Essential business v. essential workforce conundrum has yet to be solved

HSE INSTITUTE
INFORM. CONNECT. SHARE.

Questions

- Communication strategies for end users that would not add to an already high anxiety situation?
- How do I find an appropriate forensic vendor under my insurance policy?
- Is it a breach when a file with PII is sent to the wrong employee?
- Who do I call in law enforcement when I have a security breach?

HSE INSTITUTE
INFORM. CONNECT. SHARE.

HSE INSTITUTE

INFORM. CONNECT. SHARE.

F. Paul Greene

585-348-0938 (m), 585-231-1435 (o)

800-232-3021

fgreene@hselaw.com

daltieri@hselaw.com

incidentresponse@hselaw.com

HSE

Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

hselaw.com

This presentation is provided as a service to clients and friends of Harter Secrest & Emery LLP. It is intended for general information purposes only and should not be considered as legal advice. The contents are neither an exhaustive discussion nor do they purport to cover all developments in the area. The reader should consult with legal counsel to determine how applicable laws relate to specific situations. Attorney Advertising. Prior results do not guarantee a similar outcome.