Cybersecurity Regulatory Enforcement & Emerging Case Law Developments

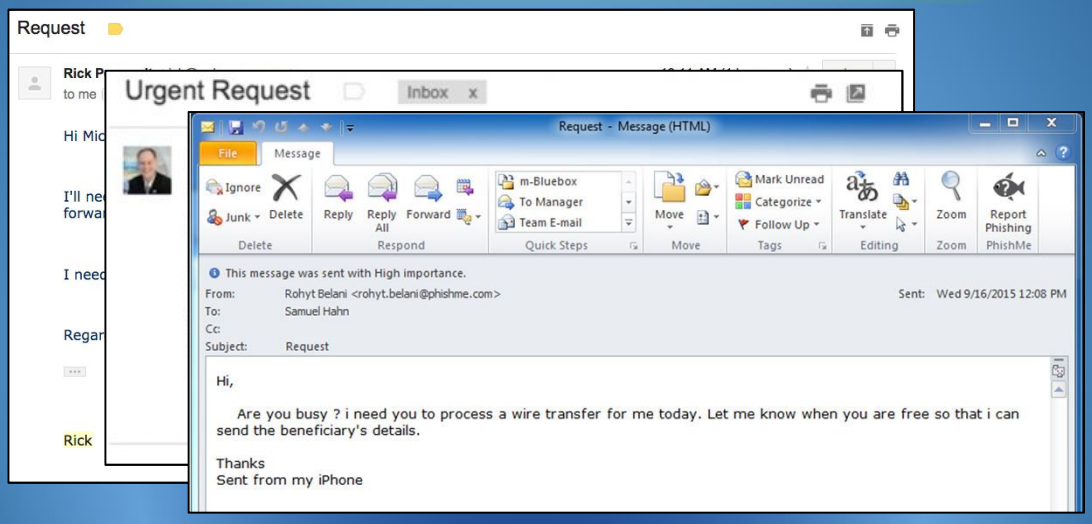
Presented by
Robert A. Stern (rstern@morrisonmahoney.com)
Daniel S. Marvin (dmarvin@morrisonmahoney.com)
August 21, 2017

MORRISON MAHONEY LLP

Payment Instruction Fraud/Social Engineering (Spoofing/Phishing)

- A legitimate looking email or communication (telephone) that is created to **dupe the recipient** into taking certain actions, **typically to wire funds** from insured's bank account **to a cyber-criminal's bank account**.
- **Spoof emails or phishing emails** commonly are intended to appear as legitimate emails that the recipient will recognize, **and therefore trust**, but actually are sent by someone else who masked their identity through the spoofed email to trick the recipient.

Phishing- CEO Fraud



Do Computer Fraud Policies Cover Payment Instruction Fraud

» The typical computer fraud policy language provides coverage when a computer is used to

- "fraudulently cause a transfer of property from inside [the insured's premises] to … a person outside those premises"

Note: Some policies require a **direct loss** to be **directly caused** by computer fraud

- the insured must suffer a **direct** loss of property that is **directly** caused by computer fraud, which, generally, is defined to include the use of any computer to "fraudulently cause a transfer of property from inside [the insured's premises] to … a person outside those premises."

Policy Wording Matters

- *Medidata Solutions, Inc. v. Federal Insurance Company*, CV-00907 (S.D.N.Y. July 21, 2017)
- *American Tooling Center vs. Travelers Casualty and Surety Company*, CV-12108-JCO (E.D. Mi., August 1, 2017)

Medidata Solutions (Facts)

- Medidata used Google Gmail platform
- Insured notified employees in finance dept. of possible acquisition by another company, with instructions to be prepared to assist on an urgent basis.
- Employee receives spoofed email purportedly from president of Medidata advising her to assist and devote fully attention to an attorney for the company. The spoofed email contained the president's correct, name, email address and picture.
- Follow up call on the same day as the email from the supposed attorney ("Michael Meyers") demanding an urgent wire transfer of $4.7 million.
- Employee requests confirming email from insured's president, which is promptly provided using the same means used in the first email.
- The wire transfer is executed with **the funds being routed to the thief.**

Medidata (Disclaimer of Coverage)

» Coverage disclaimed under the computer fraud provisions because there had been no "fraudulent entry of Data into Medidata's computer system" and there had been no "change in data elements."

Medidata (Holding)

» Spoofing/social engineering that directly results in the transfer of property can trigger computer fraud coverage.

Here, the court found the fraud was

"achieved by entry into Medidata's email system with

It was the spoofed email that directly caused the transfer and loss.

to achieve the email spoof."

American Tooling Center (Facts)

≫ Insured's requested copies of all outstanding invoices from vendor

1. Insured receives spoofed email from an imposter using an e-mail address made to look **indistinguishable from the actual vendor**
2. Instructions to wire the funds to a **new bank account**
3. Resulted in wiring of **$800,000 to the thief**

American Tooling Center (Disclaimer of Coverage)

≫ The loss was not a "direct loss" that was "directly caused by the use of a computer," as required by the policy, which provided:

1. The Company will pay the **Insured** for the **Insured's** direct loss of, or direct loss from damage to, **Money, Securities and Other Property** directly caused by **Computer Fraud**.
2. "Computer Fraud" is defined as:

   The use of any computer to fraudulently cause a transfer of **Money, Securities or Other Property** from inside the **Premises** or **Financial Institution Premises**:

   - ✓ to a person (other than a **Messenger**) outside the **Premises** or **Financial Institution Premises**; or
   - ✓ to a place outside the **Premises** or **Financial Institution Premises**

American Tooling Center (Holding)

- In ruling in favor of the insurer, the court held that Intervening facts after receipt of spoofed email, including the verification of production milestones, the authorization of the transfers and initiation of the transfers without verifying bank account information precluded a finding of "direct" loss "directly caused" by the use of any computer.
- Factors militating against computer fraud coverage:
  - No hacking, access or infiltration of the computer system to cause the loss.
  - The fraudulent emails did not directly cause the transfer of funds.
  - Transfers were authorized by the insured.
  - Intervening facts

Apache Corp. v. Great American Ins. Co., 662 Fed. Appx. 252 (5th Cir. 2016)

- Similar to ATC, the insured received email requests to make payments on legitimate invoices from a vendor to a scammer's bank account.
- Denial of coverage upheld because the court found the fraudulent emails did not constitute "the use of any computer to fraudulently cause a transfer." The Court stated:

> The email was part of the scheme; but, the email was merely incidental to the occurrence of the **authorized** transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would . . . convert the computer-fraud provision to one for general fraud.

Funds Transfer Fraud (Social Engineering Fraud)

Coverage protects against:

*….direct loss of Money or Securities sustained by an Organization resulting from **Funds Transfer Fraud** committed by a **Third Party.”***

*“**Funds Transfer Fraud**” is commonly defined as: “fraudulent electronic ... instructions ... purportedly issued by an Organization, and issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by such Organization at such institution, **without such Organization’s knowledge or consent**.”*

FTF/Social Engineering Schemes Covered?

- The majority of courts have concluded it is not covered because
  1. social engineering does not require what most courts consider to be unauthorized access to a computer system resulting in the unauthorized entry of data i.,e. **there is no hacking of the computer system**
  2. the transfers are executed with the insured’s knowledge and consent
     - (See Taylor & Lieberman v. Federal Insurance Co., 681 F. App’x 627 (9th Cir. 2017);
     - American Tooling Center, Inc. v. Travelers Casualty and Surety Co. of America, No. 16-cv-12108, 2017 WL 3263356 (E.D.Mich. Aug. 1, 2017);
     - Pestmaster Servs., Inc. v. Travelers Casualty & Surety Co. of America (requiring a transfer of funds to be without authorization to provide covererage for FTF);
     - Incomm Holdings, Inc. v. Great American Ins. Co., 2017 WL1021749 *10 (N.D. Ga. Mar. 16, 2017) (noting hacking of computer system causing the fraudulent transfer is required)

FTF/Social Engineering Schemes Covered?

- The majority of courts have concluded it is not covered because

3. Generally accept there is a distinction between when a hacker hacks an insured's computer system and the insured voluntary transfer funds.

Social Engineering Fraud Coverage

- Medidata far from resolves the issue of whether social engineering fraud that results in a voluntary transfer is covered under crime fraud policies.
- In the face of uncertainty as to coverage, the purchase by insureds of optional extensions, even with their sublimits, are still prudent.

Negotiating Broader Crime Fraud Policy Terms

When negotiating crime fraud coverage,
insureds should see if their insurer will agree to broaden the scope
of coverage by deleting any requirement that the loss arise
directly from computer fraud.

Derivative Lawsuits Under D & O Policies

- Typical allegations:
  - Breach of duty of loyalty due to failure to institute reasonable safeguards to mitigate the risk of a breach.
- Outcomes
  - Most cases have been dismissed because the plaintiffs have been unable to overcome procedural and substantive hurdles, such as the Business Judgment Rule. Motions to dismiss derivative lawsuits have been granted in cases brought against Home Depot (since settled), Target and Wyndham.
  - New lawsuits continue to be filed, including against Yahoo and Wendy's.

Article III Standing (Class Action Litigation)

- *Robins v. Spokeo*

  To have Article III Standing to sue in federal court, Plaintiff must demonstrate

  (i) an injury in fact that is

  (ii) concrete and particularized and

  (iii) actual or imminent, not conjectural or hypothetical.

Circuit Court Split Article III Standing

- Future risk of harm, including identity theft and fraudulent charges have been held by a number of circuit courts to be sufficient at the pleading stage to satisfy Article III standing if the complaint plausibly alleges there is a substantial risk of identity theft (or other harm) due to the defendant's negligence.
- Prevailing reasoning for finding concrete and particularized harm in data breach cases:

  "It is much less speculative – at the very least, it is plausible – to infer that [the hacker] has both the intent and ability to use that data for ill." ….. "Why else would hackers break into a … database and steal consumers' private information?

  Presumably, the purpose of the hack is, sooner or later to make fraudulent charges or assume those customers' identity." Chantal Attias et al. v. CareFirst Inc. et al

The Circuit Split on Standing

- Allegations of risk of future harm sufficient to satisfy Article III standing:
  - D.C. Circuit, Chantal Attias et al. v. CareFirst Inc. et al.,
  - Sixth Circuit; *Galaria v. Nationwide Mutual Insurance Company* (2016)
  - Seventh Circuit, *Remijas v. Neiman Marcus Grp*. (2015)
  - Third Circuit, *In Horizon Healthcare Services data breach litigation* (2017)
  - Ninth Circuit, *Krottner v. Starbucks Corp.* (2010)
  - Eleventh Circuit, *Resnick v. Avmed* (2012)
- Allegations of risk of future harm insufficient to satisfy Article III Standing
  - 4th Circuit, *Beck v. McDonald* (2017)

Federal Trade Commission (FTC)

The FTC

- Plays a leading role in the enforcement of U.S. privacy standards.
- Section 5 of the FTC Act gives it broad authority to regulate most companies, exempting certain types of financial institutions, airlines, telecommunications carriers, among others.
- Additionally, certain statutes give the FTC regulatory authority: COPPA, GLBA, TCFAPA, FCRA, etc.

FTC Act

- Unfairness Doctrine: The basic consumer protection statute enforced by the FTC is Section 5(a) of the FTC Act, commonly known as the "unfairness doctrine," which prohibits: "unfair or deceptive acts or practices in or affecting commerce."
- Unfair: An act or trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. Section 45(n).
- Deceptive: A deceptive act or practice is a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." (Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, Comm. On Energy & Commerce (Oct. 14, 1983)).

FTC Enforcement Actions

An FTC enforcement action usually begins with a claim that a company has committed an unfair or deceptive practice or has violated a specific consumer protection law under which it is granted enforcement authority.

FTC Enforcement Processes and Remedies

- The FTC can obtain injunctive relief and seek civil penalities and require government approved third-party monitoring of cybersecurity standards, policies, procedures and written information security programs be implemented to protect consumers' data.
- Consent decrees can include agreements to pay civil penalties and typically include mandatory third-party monitoring and data security compliance programs extending for a term of twenty years.

FTC Enforcement

- Prior to 2005, in evaluating whether to initiate a data security enforcement action against a business, the FTC relied on the deceptive practices prong of the unfairness doctrine, requiring businesses to have engaged in a deceptive act or misrepresentation.
  - Such misrepresentation typically centered on a business' false claims concerning the security measures it had implemented to safeguard and protect sensitive consumer data, rendering the privacy statements, to that extent, deceptive.

FTC Enforcement Actions

- ***In the Matter of BJ's Wholesale Club, Inc.* (2005)**
  - First time an FTC enforcement action was predicated on the unfairness prong, without any need to allege deception.
  - After hackers were able to infiltrate BJ's computer system and steal the names and credit card information of at least 40,000 customers, the FTC alleged that BJ's failed to institute reasonable measures to secure its customer's data.
- ***FTC v. Wyndham Worldwide Corp.* (2015)**
  - The FTC alleged that the hotelier's failure to protect its customers' data, resulted in three data breaches within two years.
  - Wyndham challenged the FTC's authority to maintain cybersecurity enforcement actions based on the unfairness prong, as opposed to any allegations that it affirmatively made a deceptive claim or misrepresentation.
  - The Third Circuit affirmed the FTC's authority to use the prohibition on unfair practices in section 5 of the FTC Act to challenge alleged data security failures.

FTC Enforcement Actions

- *Expansion of Enforcement Activities:* vulnerability of sensitive data, without unauthorized acquisition of data by third parties, is sufficient independent grounds for the FTC to exercise its enforcement authority.
  - *FTC v. D-Link Systems Corp. et al* (2017)
    - First FTC cybersecurity enforcement action in which an entity's alleged vulnerability to cyberattacks that left consumer data potentially susceptible to the unauthorized acquisition of their data by third parties could trigger liability, even though the data had not been hacked and there was no injury or damages sustained by consumers.
- Result: Just like a misrepresentation as to information security is no longer required under the unfairness doctrine, neither is actual injury or damages stemming from a cyber breach.

FTC Enforcement Actions

- *Uber Reaches Second Settlement with FTC:* For privacy violations relating to the collection of data of their customers and drivers:
  - Agrees to outside monitoring for 20-years
  - No civil payment
  - Had previously agreed to pay $20 million in connection with prior FTC enforcement action.

What This Means for Your Clients/Insureds

Companies must ensure they are implementing reasonable measures to protect their customer's data and following best practices as it applies to them and their respective industries to avoid triggering potential liability under Section 5(a) of the FTC Act—and resulting claims for coverage under applicable insurance policies.

U.S. Department of Health and Human Services (HHS): Office for Civil Rights (OCR)

- OCR is responsible for enforcing the HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164, Subparts A,C and E) to protect the privacy of health information.

HHS Authority

- HHS, pursuant to its authority under Health Insurance Portability and Accountability Act (HIPAA), promulgated regulations with regard to health privacy providing a **baseline** of privacy protection – **states can still provide more protection**.
  - **HIPAA Privacy Rule**
    - Establishes national standards for the protection of certain health information (Protected Health Information)
  - **HIPAA Security Rule**
    - "Operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that covered entities must put into place to secure 'electronic protected health information' (e-PHI)"

HHS Authority

- **The HITECH Act**
  - "Strengthens HIPAA regulations by mandating much higher penalties for violations, made many more organizations directly subject to HHS enforcement and required HHS to conduct audits of HIPAA compliance"
  - Breach Notification Rule requires individuals to be notified if their PHI is involved in a data security breach- the first such requirement in federal law.

Scope and Applicability of HIPAA: Covered Entities

A Covered Entity is one of the following:

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
This includes providers such as: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies ...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.	This includes: • Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Scope and Applicability of HIPAA: Business Associates

- HITECH makes HIPAA applicable to **business associates** (including personal health record vendors and subcontractors), requiring them to (i) comply with certain HIPAA Privacy and Security Rules, (ii) rendering them directly liable for violations and (iii) subjecting them to HIPAA and HHS enforcement.
  - BAs are subject to the same civil and criminal penalties under HIPAA as covered entities.

HIPAA Enforcement

- Conduct/initiate compliance reviews/investigations
- Issuance of fines– that have ranged between $50,000 up to millions of dollars.
- Enter into resolution agreements
- Require Corrective Action Plans, mandating implementation of compliant policies and procedures to ensure compliance with the Breach Notification Rule and annual employee training.

HHS Enforcement: lack of cybersecurity policies, risk analysis and access controls

- Breach of ePHI occurred on a shared data network between NY Presbyterian Hospital and Columbia University due to application developed by a physician.
  - HHS found that NY Presbyterian failed to have sufficient cybersecurity procedures, network monitoring and controls in place to protect patient databases.
    - **NY Presbyterian agreed to pay $3.3 million.**
  - HHS found Columbia University to have failed to conduct a proper risk analysis.
    - **Columbia agreed to pay $1.5 million.**

OCR Investigation Can Lead to Discovery of Multiple Violations

- In QCA Health Plan, Inc., an encrypted laptop computer containing the ePHI of 148 individuals was stolen from a workforce member's car.
  - In addition to finding that the loss of ePHI was a HIPAA violation, OCR also found other violations including failure to implement policies and procedures, conduct risk assessments, failure to implement physical safeguards for workstations, and failure to restrict access to only authorized users.
  - **QCA settled for $250,000.**

OCR Investigation Can Lead to Discovery of Multiple Violations

- In Adult & Pediatric Dermatology, a stolen unencrypted thumb drive led to OCR identifying additional HIPAA violations, including lack of policies and inadequate training, in addition to the improper loss of patient data on the thumb drive.

Federal Communications Commission (FCC)

- Responsible for implementing and enforcing communications law and regulations.
- Television, radio and phone companies are subject to FCC regulation.
- The FCC regulates all interstate communications, such as wire, satellite and cable, and international communications originating or terminating in the United States.
- No general privacy authority, but certain Communications Act provisions expressly grant FCC authority over particular areas of consumer privacy.

FCC Regulation

- Telecommunications Act of 1996
  - Section 222: governs the privacy of customer information provided to and obtained by telecommunication carriers.
  - The act imposed new restrictions on the access, use and disclosure of customer proprietary network information (CPNI) or information collected by telecommunications carriers related to their subscribers.

FCC Enforcement Actions

- ***In the Matter TerraCom, Inc. and YourTel America, Inc. (2015):***
  - TerraCom and YourTel entered into a consent decree with the FCC after failing to protect stored customer data on online servers without password protection or encryption, that lead to the data breach.
  - **$3.5 million civil penalty**
  - The companies must appoint a compliance officer and develop a compliance plan, implement an information security program, and other measures.
- ***In the Matter of AT&T Servs., Inc.* (2015)**
  - AT&T international call center employees stole the personal information of AT&T customers.
  - **$25 million fine** for failing to reasonably secure and protect customer data.
  - AT&T ordered to appoint a compliance officer, develop and implement a compliance plan that included a risk assessment, review and training, and provide notice to affected customers.

FCC Enforcement Actions

- ***In the Matter of Cellco P'ship (2016):***
  - Verizon Wireless added "supercookies" without notification or consent into customer's mobile internet traffic
  - **$1.35 million fine** and the adoption of a three-year compliance plan.
  - Verizon agreed to notify consumers about tracking practices
  - Verizon must get consumer consent to share "supercookie" information with third-parties

What This Means for Your Clients/Insureds

For companies that fall under FCC regulation,
the enforcement actions demonstrate that not having appropriate information security programs or failing to protect customer information can result in hefty penalties.

Questions

MORRISON MAHONEY LLP