Data Breach! Now what?

John Lande
Dickinson, Mackaman, Tyler, & Hagen, P.C.

DICKINSONLAW
ITA 2018

Agenda

- Cybersecurity threats
- Cybersecurity liability
- Cybersecurity insurance issues
- Mitigating cybersecurity risks

DICKINSONLAW
ITA 2018

Cybersecurity Threats

DICKINSONLAW
ITA 2018

Two Kinds of Attacks

- Social engineering
  - Using public or non-public information to trick organizations into providing confidential information or sending money
- Hacking
  - Unauthorized access to organization's computer network and devices

DICKINSONLAW
ITA 2018

Social Engineering

DICKINSONLAW
ITA 2018

Examples

- Principle Solutions Group v. Ironshore:
  - $1.717 million wired to fraudsters
- Medidata v. Federal Insurance:
  - $4.7 million wired to fraudsters
- Maxum Indemnity v. Long Beach Escrow:
  - $250,000 wired to fraudsters
- Apache Corp. v. Great Am. Insurance:
  - $2.4 million in AP sent to fraudsters

DICKINSONLAW
ITA 2018

PSG v. Ironshore Indemnity

- PSG: wealth management company
- 9:10 am: controller received fraudster email
- 10:15 am: "lawyer" called controller
- "Lawyer" claimed director authorized wire transfer

DICKINSONLAW
ITA 2018

PSG v. Ironshore Indemnity

- "Lawyer" emailed wire instructions
- Controller forwarded email to bank
- Bank required online submission
- Controller prepares wire via online system
- Fraud prevention unit at the bank contacts controller
- Controller calls "lawyer" to confirm authority
- Bank released $1.7 million

DICKINSONLAW
ITA 2018

How did this happen?

- Fraudster's fault?
- Controller's fault?
- Managing director's fault?
- Bank's fault?

DICKINSONLAW
ITA 2018

Preventing PSG v. Ironshore

- "Lawyer" sent an email with wire instructions
- Controller forwarded email to bank
- Bank required online submission
- Controller prepares wire via online system
- Fraud prevention unit at the bank contacted controller
- Controller called "lawyer" to confirm authority
- Bank released $1.7 million

DICKINSONLAW
ITA 2018

Preventing PSG v. Ironshore

- Segregate duties
- Controller can't wire money if the controller doesn't have the sole authority
- Threshold for approval: Controller has authority for wires below a certain amount

DICKINSONLAW
ITA 2018

Email Spoofing

- jlande@dickinsonlaw.com
- jlande@dickensonlaw.com
- ilande@dickinsonlaw.com
- jlande@dickinson.com

DICKINSONLAW
ITA 2018

Medidata v. Federal Insurance

- Medidata executives informed accounting department that there would be M & A activity on short notice
- Medidata routinely did business via email
- Accounting department received a series of emails claiming to be from a Medidata executive
- "Executive" told employees that a lawyer would be contacting them with wire instructions

DICKINSONLAW
ITA 2018

Medidata v. Federal Insurance

- "Attorney" called accounting department and asked for a wire transfer
- Employee informed "attorney" that authorization would need to come from particular executives
- Fraudsters sent email on behalf of authorized signatories confirming wire
- Employees authorized the wire
- Wired $4.7 million to China
- Second request for $4.8 million caused suspicion

DICKINSONLAW
ITA 2018

Preventing Medidata

- Medidata executives informed accounting department that there would be M & A activity on short notice
- Medidata routinely did business via email
- Accounting department received a series of emails claiming to be from a Medidata executive
- "Executive" told employees that a lawyer would be contacting them with wire instructions

DICKINSONLAW
ITA 2018

Preventing Medidata

- "Attorney" called AP department and asked for a wire transfer
- Employee informed "attorney" that authorization would need to come from particular executives
- Fraudsters sent email on behalf of authorized signatories confirming wire
- Employees authorized the wire
- Wired $4.7 million to China
- Second request for $4.8 million caused suspicion

DICKINSONLAW
ITA 2018

Fraud Nuts & Bolts

- Fraudsters altered the "from" address on the "envelope" that transmits the email
- Difficult to detect

DICKINSONLAW
ITA 2018

Preventing Medidata

- Executives told employees that transactions might occur on short notice
- Employees disclosed key individuals who could authorize transactions

DICKINSONLAW
ITA 2018

Tips

- Verify identity of person making request through some other means
- Be wary of urgent requests
- Limit authority to make significant transfers
- Setup procedures for when you are unavailable to verify authenticity of requests

DICKINSONLAW
ITA 2018

Hacking

DICKINSONLAW
ITA 2018

State Bank of Bellingham

- Bank's computer for initiating wire transfers was compromised
- Hackers were able to transfer $940,000 from bank to accounts located in Poland
- After reversing some of the transactions the bank lost $485,000

DICKINSONLAW
ITA 2018

How did the hackers get in?

- Failed to implement automatic security updates;
- Clicked on a spam link that downloaded multiple pieces of malware;
- The malware—Zeus—allowed hackers to obtain all passwords and usernames;
- Bank employees left secure token in computer;
- Antivirus software detected the Zeus virus; bank employees failed to remove the virus;
- History of spam email messages being opened;
- Computer was accessible by any employee because the computer was not password protected.

DICKINSONLAW
ITA 2018

Hybrid Attacks

DICKINSONLAW
ITA 2018

Outlook Rules

- Phishing email to gain access
- Hackers install rules to re-route email
- Fraudsters send/receive emails on behalf of the user

DICKINSONLAW
ITA 2018

Tips

- Utilize anti-malware/anti-virus software
- Implement security updates as they are released or shortly thereafter
- Be wary of emails, particularly emails that “urgent” or seem to good to be true

DICKINSONLAW
ITA 2018

Liability Rules

DICKINSONLAW
ITA 2018

What is the source of the loss?

- Cases involving money almost always involve wiring money or sending it via ACH
- Personally identifiable information and other data exfiltration

DICKINSONLAW
ITA 2018

No Consumer Protection

- Regulation E: Generally provides for reimbursement of funds for ***unauthorized*** transfers
- Limited to consumer accounts held directly or indirectly by a financial institution and established primarily for personal or household purposes
- Excludes accounts held under bona fide trust agreement
- Does not apply to remittance transfers

DICKINSONLAW
ITA 2018

Accounts Not Covered by Reg E

- Brokerage accounts
- IRAs
- Trust accounts
- Business accounts

DICKINSONLAW
ITA 2018

Authorization

- Consumers may not be protected if they authorize the transfer
- Bank did what it was supposed to do
- May not have recourse against the bank

DICKINSONLAW
ITA 2018

Relationship of UCC and Reg E

- UCC "does not apply to a funds transfer any part of which is governed by the Electronic Fund Transfer Act of 1978, 15 U.S.C. § 1693 et seq."
- Key: is the transfer from an account established primarily for personal or household purposes, **not** whether bank is liable

DICKINSONLAW
ITA 2018

UCC: Legal Framework

- Governs non-EFTA and remittance transfers
- Default: Banks are liable for loss
- Banks can shift liability to account holders
- Bank and account holder agree to verify the authenticity of payment orders using a commercially reasonable security procedure
- The bank follows the procedure in good faith

DICKINSONLAW
ITA 2018

Keys for Liability

- Commercially reasonable security procedure
- Acceptance of payment order in good faith
- Agreement on that procedure

DICKINSONLAW
ITA 2018

What does that mean for account holders?

- Do they initiate wire or ACH transfers?
- How does the bank verify authenticity of payment requests?
- Account holder may be liable if tricked into transferring money or gets hacked

DICKINSONLAW
ITA 2018