CYBERSECURITY LAW

CRENSHAW, WARE & MARTIN, PLC

This presentation is for educational purposes only. It is not legal advice for any particular situation. Laws change all the time. Always verify that information is accurate and up to date before you rely on it.

DISCLAIMER

CRENSHAW, WARE & MARTIN, PLC

Agenda

01 Professional Responsibility

02 Virginia Statue

03 Case Law

04 Business Risk

05 Risk Mitigation

CRENSHAW, WARE & MARTIN, PLC

Cybersecurity Is Not Just an IT Issue...

CRENSHAW, WARE & MARTIN, PLC

01 Professional Responsibility

CRENSHAW, WARE & MARTIN, PLC

The attorney–client privilege is one of the oldest recognized privileges for confidential communications.

CWM
CRENSHAW, WARE & MARTIN, PLC

We have enshrined the privilege into -

ABA Model Rule of Professional Responsibility 1.6 - “a lawyer shall not reveal information related to the representation of a client …”

CWM
CRENSHAW, WARE & MARTIN, PLC

For lawyers, a data breach equals a breach of confidentiality.

CWM
CRENSHAW, WARE & MARTIN, PLC

Virginia Rule of Professional Conduct 1.6

Confidentiality of Information

(a) A lawyer shall not reveal information protected by the attorney-client privilege …which would be embarrassing or would be likely to be detrimental to the client …

(d) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information protected under this Rule

CRENSHAW, WARE & MARTIN, PLC

Comment 20 to Virginia Rule of Professional Responsibility 1.6

- Take reasonable action.
- Employ reasonable methods to protect client data.

CWM
CRENSHAW, WARE & MARTIN, PLC

The 3 Reasonable Steps

1. Adopt a security framework
2. Develop cybersecurity plans and policies
3. Insure against remaining threats

CWM
CRENSHAW, WARE & MARTIN, PLC

Virginia Rule of Professional Conduct 5.1

- **Responsibilities Of Partners And Supervisory Lawyers**
- **A partner in a law firm, or a lawyer who individually or together with other lawyers possesses managerial authority, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.**

CRENSHAW, WARE & MARTIN, PLC

Virginia Rule of Professional Conduct 5.3

Responsibilities Regarding Non-lawyer Assistants

With respect to a non-lawyer employed or retained by or associated with a lawyer:

(a) a partner or a lawyer who individually or together with other lawyers possesses managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;

CRENSHAW, WARE & MARTIN, PLC

Comment to Rule 1.1 ABA Model Rule & Virginia Rule of Professional Responsibility

Maintaining Competence

[8] / [6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, …

CRENSHAW, WARE & MARTIN, PLC

02 Virginia Statue

CRENSHAW, WARE & MARTIN, PLC

What is a Data Breach?

CRENSHAW, WARE & MARTIN, PLC

Data Breach / Incident *(General Definition)*

A data breach is an incident in which sensitive, protected or confidential data has been viewed, stolen or used by an unauthorized individual. They may involve:

- **Personal Health Information (PHI)**
- **Personally Identifiable Information (PII)**
- **Trade secrets or intellectual property**

CRENSHAW, WARE & MARTIN, PLC

Data Breach *(Legal Definition)*

- § 18.2-186.6 - Breach of Personal Information notification
- "[T]he unauthorized access and acquisition of unencrypted and un-redacted computerized data that compromises the security or confidentiality of personal information…"
- Does not include lawful uses of information

CRENSHAW, WARE & MARTIN, PLC

Personal Information in Virginia

First Name or **First Initial** AND **Last Name** in conjunction with one of the following:

- Social Security Number
- Drivers License Number or State ID Card Number
- Financial Account Number in combination with the accompanying security code, access code or password for the account

CRENSHAW, WARE & MARTIN, PLC

CRENSHAW, WARE & MARTIN, PLC

If you have:

- Personal Health Information (PHI)
- Personally Identifiable Information (PII)
- Intellectual Property

YOU are a target

03 Recent Case Law

CRENSHAW, WARE & MARTIN, PLC


NBEO
NATIONAL BOARD OF EXAMINERS IN OPTOMETRY®

Issue:

- Did the Plaintiff's have standing?

Holding:

- Yes

Standing Rule:

- Injury in fact
- Causal connection between injury and defendant's conduct
- Injury is redressable by a favorable judicial decision


DOMINION®
NATIONAL

Facts:

- From August 2010 – April 2019 Hackers accessed Dominion National customer's PI.
- Dominion informed customers that they detected the intrusion with the help of Mandiant.
- In 2016,Dominion Hired Mandiant to "investigate, prevent and remediate data breaches" prior to the discovery of the breach.
- In 2018, Mandiant and BakerHostetler executed a SOW for "computer incident response support, digital forensic support, threat actor support …
- Post breach discovery, Mandiant entered another SOW with BakerHostetler for the benefit of the defendant that incorporated the 2016 and 2018 SOW and listed a virtually identical scope of work

DOMINION® NATIONAL

Facts:

- Mandiant concluded its investigation on May 17, 2019.
- Dominion's crisis communications stated that:
  - They were investigating the incident with the assistance of Mandiant.
  - Instructed clients to tell their customers that Dominion engaged Mandiant to assist with the investigation.
- Dominion used information from the Manidient report in communications with the Indiana Attorney General's Office

Issue 1

- Is the Mandiant Data Breach Investigation Report Discoverable?

Holding:

- Yes

General Attorney Client Privilege Rule:

- A party may not ordinarily discover documents that are prepared in anticipation of litigation

Reasoning:

- The report was primarily created for non-litigation business purposes.
- Dominion engaged Mandiant prior to 2019.
- The SOW was the same.
- The 2019 addition of “under the direction of counsel” was to shield the report from disclosure and not alter the business purpose of the work.
- Defendants publicized Mandiant’s work as a customer management strategy (non-litigation purpose)

Reasoning:

- **Premera Case** (Discoverable) – Prior agreement with same scope of work that shifted to counsel post breach.
- **Target Case** (Not Discoverable) - two-track investigation. One report for Target and one report for counsel investigating the breach.
- **Experian Case** (Not Discoverable) – No continuous relationship with Mandiant. Mandiant was engaged by counsel. Full report was withheld from defendant. Customers never told of Mandiant's involvement.

Takeaways:

- A security scope of work should be different than an incident response scope of work.
- Consider using different data forensic companies for security and incident response.
- Counsel should engage data forensics services for incident response (scope of work, payment, etc.).
- Consider a two-track investigation.
- Don’t turn over the full report (oral briefing, letter from counsel).
- Don’t publicize your privileged investigative efforts.


Capital One

Facts:

- 29 July 2019 Capital One announce it has experienced a data breach of its AWS cloud environment
- Capital One stored tons of consumer PII in the cloud (100 million US records and 6 million in Canada)
- Capital One and Amazon were aware that the AWS cloud servers were susceptible to exploitation due to the misconfiguration of a firewall and Capital Ones broad access permissions
- Capital One did 2 things
    1. Kept storing all of the customer PII in the cloud
    2. Encrypted all of the data

Facts:

- However, the data was still vulnerable if a hacker was able to obtain an authorized users (employee) credentials.
- In March and April of 2019 a former AWS employee gained access to the Capital One cloud by exploiting the firewall vulnerability
- Due to her credentials, she moved freely through the cloud environment
- The hacker
  - Downloaded 1.75 terabytes of data
  - Probed the system 5 times between March and May
  - Posted instructions on how to hack Capital One online
  - Bragged online about all the “secure data” she found on AWS

Plaintiffs (nationwide class) Allegations:

- PII exposure mitigation damages
- Diminution in the value of their PII
- Increased risk of identity theft or other fraud
- Did not receive the benefit of their barging with Capital One
- Actual identity theft
- Negligence
- Negligence per se
- Unjust enrichment
- Breach of Confidence
- Breach of Implied Contract
- Breach of Contract
- Claims under the Virginia data breach notification statute

Issue # 1

- Does the economic loss rule bar the plaintiffs claims?

Holding:

- No

General Economic Loss Rule:

- Plaintiff cannot recovery pure economic losses under tort negligence theories

Reasoning (Voluntary Duty Doctrine)

- Plaintiff must prove that a party took an affirmative course of action and:
  - Failed to exercise reasonable care;
  - Undertook a duty owed to a third party; or
  - The harm was a result of either parties reliance upon the defendant's undertaking
- Capital One
  - Undertook the duty to protect its customers PII
  - Capital One was aware of the vulnerabilities and failed to exercise reasonable care
- Therefore a duty exists and the negligence claims are not bared by the Economic Loss Rule

Issue # 2

- Can the Plaintiffs recover for actual fraud or the imminent risk of fraud?

Holding:

- Yes

General Rules:

- A plaintiff's allegations of actual losses are sufficient to survive a 12 (b)(6)
- Plaintiff must show causation is a probability rather than a possibility

Reasoning

- Allegations of actual monetary losses/harms are sufficient
  - Unauthorized charges
  - Theft of financial information
  - Mitigation cost
- Possibility over probability
  - Hacker acquired data
  - Posted how to get more
  - Plaintiffs suffered actual PII misuse
  - Therefore the inference is that the hacker shared info with others and linking the harm suffered to the data breach, and
  - Additional injuries are likely imminent

Issue # 3

- Can the Plaintiffs recover for lost value of PII?

Holding:

- No

Reasoning:

- Plaintiffs didn't allege how their data became less valuable
- No allegations that data was rejected or less valuable

Issue # 4

- Can the Plaintiffs recover for loss of the benefit of the bargain?

Holding:

- No

Reasoning:

- Virginia courts have yet to recognize BoB in data breach cases
- Plaintiff's didn't cite any authority
- BoB is primarily a contract and not a tort doctrine

Issue # 5

- Can the Plaintiffs recover under theories of negligence per se (Section of the FTC Act and GBLA)?

Holding:

- No

General Rule:

- Plaintiff must show (1) Defendant violated a statute enacted for public safety, (2) he belongs to the class the statute benefits, (3) the statute was designed to protect from the harm suffered, and (4) the statutory violation was the proximate cause of the injury

Reasoning

- FTC Act was intended to prevent unfair and deceptive trade practices
- The GLBA was designed to encourage financial institutions to respect the privacy of customers and to protect customer PII
- Neither act is expressly aimed at protecting public safety under Virginia definition of the same
- Statutes aimed at fraud protection and other dishonest conduct impact the public, but are not the type of regulations to support a negligence per se claim

Issue # 6

- Can the Plaintiffs recover under theories of breach of confidence?

Holding:

- No

General Rule:

- Virginia has not recognized a breach of confidence tort in a banker and customer context
- There is no common law cause of action for a breach of confidentially under Virginia law

Issue # 7

- Can the Plaintiffs recover for breach of contract?

Holding:

- Yes

General Rule:

- A breach occurs if a party without legal excuse fails to perform an obligation in a timely manner, repudiates a contract, or exceeds a contractual use term, or otherwise is not in compliance with an obligation placed on it by … the agreement.

Reasoning

- The cardholder agreement does not contain all of the contractual obligations
- The cardholder agreement incorporates the terms of the privacy policy into the agreement
- The same consideration that makes the cardholder agreement enforceable makes the privacy notice requirements enforceable
- Both parties assent to the relationship based on the totality of the agreement and policy
- The privacy policy contains a promise to maintain the security of customer information
- This includes promises to comply with federal law and recognized security standards

Issue # 8

- Can the Plaintiffs recover for unjust enrichment?
- What is the scope of the contractual relationship between the parties?

Holding:

- Yes/Maybe

General Rule:

- Plaintiff must (1) receive a benefit and (2) unjustly retain the benefit at the expense of another
- No recovery if an express contract covers the conduct at issue

Reasoning

- Amazon
  - No express contract between the parties
  - Defendant accepts the benefit of the data a Plaintiff's expense by not implementing adequate safeguards
- Capital One
  - There is a contract between the parties
  - There is a dispute regarding the scope of the contract re: data security
  - If the contract does not cover data security, they have plead a claim for unjust enrichment for the same reasons as Amazon

Issue # 9

- Can the Plaintiffs recover for breach of an implied contract?

Holding:

- Yes/Maybe

General Rule:

- No recovery if an express contract covers the conduct at issue

Reasoning

- **There is a Cardholder Agreement**
- **There is a Privacy Notice that governs the security of PII**
- **There is also a dispute regarding if the protection of PII is within the scope of the contract**
- **If the contract does not cover data security, the court will treat the implied contract claim as an alternative claim**

Issue # 10

- Can the Plaintiffs bring claims for breach under VA's Data Breach Notification Law?

Holding:

- Yes

General Rule:

- If PI is accessed and acquired, the custodian of the data must make timely notification to those affected

Reasoning

- The statute allows a citizen to recover direct economic damages
- Plaintiffs adequately plead that PI was compromised
- Issue of notice is not ripe (factual issue)
- Mitigation expenses are traceable to the data breach
- Amazon as a third-party data vendor also falls within the scope of these allegations as well.

Takeaways

- A court may find that you undertook a duty to protect data.
- Lawyers have a duty of confidentiality and you have to take reasonable measures to protect client data.
- One might be liable for fraud if the harm can be linked to the data breach.
- No claims for loss value of PII, BoB, negligence *per se*
- Possible liability for breach of contract and unjust enrichment

03 Business Risk

CRENSHAW, WARE & MARTIN, PLC

Hackers

Hackers do not discriminate. It does not matter if your organization is

BIG or small

CRENSHAW, WARE & MARTIN, PLC

Risk Management & Business Resiliency

Risk & Challenges

- Downtime
- Customer security requirements
- Teleworking
- Customer & employee data
- Employees
- Vendors
- Supply chain disruption
- Internet of things
- Intellectual property

CRENSHAW, WARE & MARTIN, PLC

Business Risk & Resiliency

The following statistics were reported in victim complaints to the IC3 between June 2016 and July 2019:

Domestic and international incidents: **166,349**

Domestic and international exposed dollar loss: **$26,201,775,589**

CWM
CRENSHAW, WARE & MARTIN, PLC

Business Risk & Resiliency

The following BEC/EAC statistics were reported in victim complaints to the IC3 between October 2013 and July 2019:

Total U.S. Victims	69,384
Total U.S. Exposed Dollar Loss:	$10,135,319,091
Total non-U.S. Victims	3,624
Total non-U.S. Exposed Dollar Loss:	$1,053,331,166

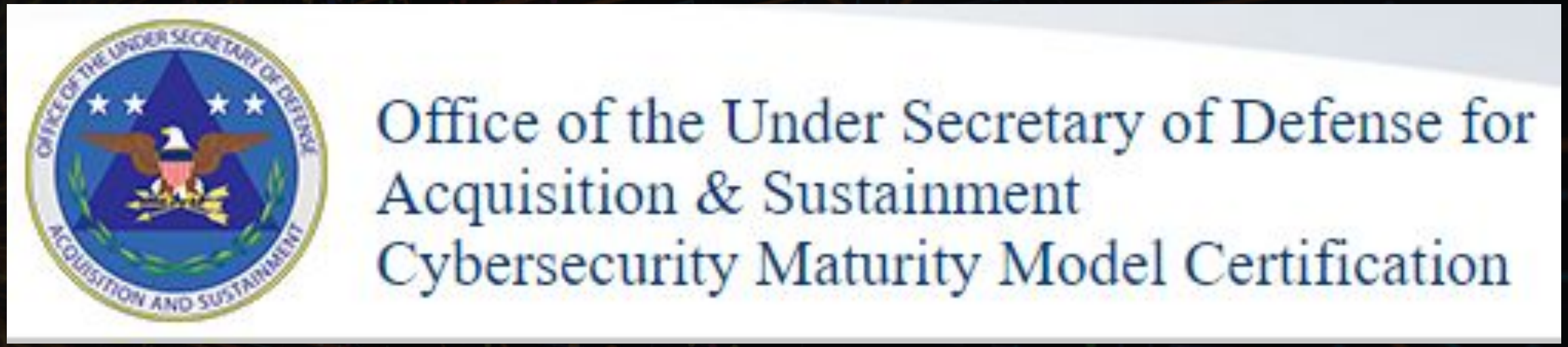
CWM
CRENSHAW, WARE & MARTIN, PLC

Business Risk & Resiliency

- Data Breach
- Ransomware

CRENSHAW, WARE & MARTIN, PLC

Business Risk & Resiliency



CRENSHAW, WARE & MARTIN, PLC

05 Risk Mitigation

CRENSHAW, WARE & MARTIN, PLC

Business Risk & Resiliency Solutions

- Incident Response Planning
- Employee Policies
- Training
- System Security Plans
- Insurance

CWM
CRENSHAW, WARE & MARTIN, PLC

Teleworking Data Security

- Update devices and applications (auto update)
- Avoid unsecure wireless access to company data
- Secure & segregate work devices if possible
- Provide security software
- Continue to enforce password policies
- Continue to enforce data storage policies
- Report and avoid suspicious activity
- Provide remote security training
- Email usage and encryption

CRENSHAW, WARE & MARTIN, PLC

We are not just any other business.

We are lawyers!

Clients give us information because they need help and we have a history and reputation for keeping information confidential.

CWM
CRENSHAW, WARE & MARTIN, PLC

Darius Davenport

Attorney at Law
Data Breach Counsel
Cybersecurity and Data Privacy Practice

Crenshaw Ware & Martin, P.L.C.

150 W. Main Street | Suite 1500
Norfolk, VA 23510
(757) 623-3000
ddavenport@cwm-law.com
www.cwm.law.com

CRENSHAW, WARE & MARTIN, PLC

CRENSHAW, WARE & MARTIN, PLC