We welcome you to take a break. Please return at 2:20 p.m.

VORYS

Cybersecurity Overview, Recent Legal Developments, and Data Privacy Best Practices

Eric W. Richardson and Brent D. Craft

Vorys, Sater, Seymour and Pease LLP
513.723.4000| ewrichardson@vorys.com| bdcraft@vorys.com

VORYS

Topics

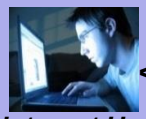
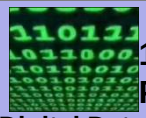
- Cybersecurity and data breach overview
  - Types of threats
  - Impact of breaches
- Timeline of a data breach
- Bad cybersecurity habits
- Data breach notification laws, consumer protection laws, and regulatory enforcement
- Legal ethics and cybersecurity

VORYS

The number of users and methods used to access cyberspace have grown exponentially…

Exponential Growth

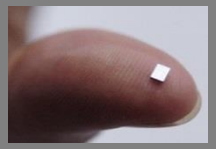
Growth in the developed world exploded over the last 30 years…

	1990	2023
 *Internet Users*	< 1 million	5 billion
 Cell Phones	11 million	5.22 billion
 Digital Data	100 Petabytes	Over 64 zettabytes
 Internet Hosts	300,000	Over 1 billion

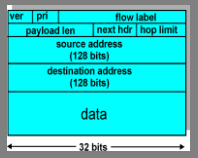
New Technologies

…and will accelerate as a result of new technologies and reduced prices…

$100 laptops



Miniaturized "Smart" Devices



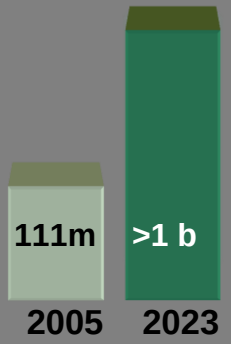
IP v6

Ubiquitous Wireless Networks

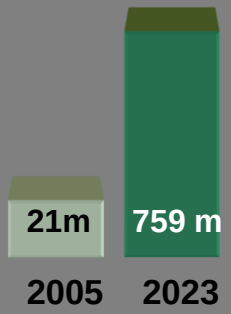
Global Adoption

…fueling the adoption of cyber capabilities in developing countries

Internet Users in China



Internet Users in India



VORYS

…which has transformed business models and driving economic growth

Massive Investment

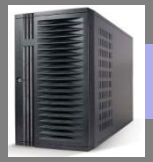
Industry / Gov't invest $4t in ICT goods and services every year…

$400b

Computers

$360b

Software

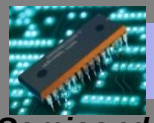


$60b

Servers

$100b

Network Equipment



$260b

Semiconductors

Mission Enablement

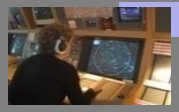
…These investments have transformed business models and military operations…

Finance:
$3.2t per day in foreign exchange

Health:
Electronic Health Records

Energy:
300k kilometers of lines carrying 3.8 b kilowatts per year

E-Commerce:
$200b in on-line sales



Air Transportation:
741 million passengers per year

Defense:
Network-Centric Operations

Growing Vulnerabilities

…while exposing substantial vulnerabilities and risks

Hackers steal 40 million credit card numbers

Hackers steal 8.3 million Health Records

Electricity grid in U.S. penetrated by spies

Hackers break into FAA Air Traffic Control Systems

VORYS

In this new environment, the threats are more diverse, increasing in frequency and magnitude of attacks

More Diverse

The threats have become more diverse and distributed…

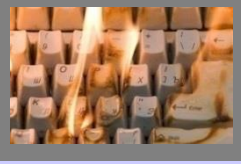
Capabilities

Foreign Intelligence Services

Cyber Criminals

Terrorists

Hactivists



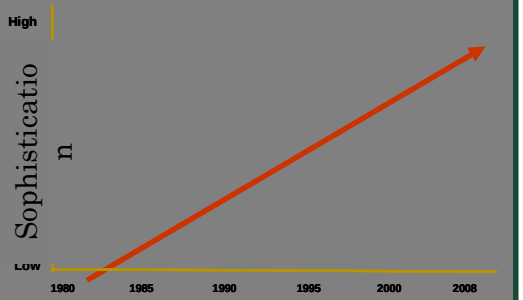
Hate Groups

Risks include both malign and benign threats

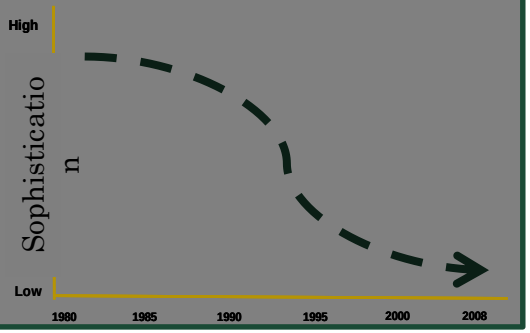
More Capable

… while growing in sophistication with lower barriers to entry

The sophistication of available tools is growing



While the sophistication required of actors is declining



Greater Impact

…increasing the frequency and impact of attacks (2022 statistics)

1,802 CONFIRMED BREACHES

422 million + PEOPLE IMPACTED

$4.35 million = Global Average Total Cost of Data Breach in 2022

$9.44 million = Average Cost of Data Breach in U.S.

VORYS

2022 Statistics

- **1,802** confirmed data breaches in 2022
- Impacted more than **422 million** people—a 40% increase form the prior year
  - Most affected areas include healthcare, financial services, education, manufacturing, professional services, and public administration
  - Healthcare breach most expensive—average total cost of a breach was $10.1 million in 2022
  - Financial second highest at $5.97 million

VORYS

2022 Statistics

- 83% of organizations experienced more than one data breach
- 60% of data breaches led to prices increases passed on to customers
- 19% of breaches resulted from a data compromise experienced by a vendor or business partner
- 45% of data breaches were cloud-based

VORYS

2022 Statistics

- **What were the primary causes of data breaches in 2022?**
  - 19% of breaches resulted from **compromised credentials**
  - 16% were caused by **phishing**
  - 15% involved **cloud misconfiguration**
  - 13% were rooted in vulnerabilities in **third-party software**
  - 11% were caused by **malicious insiders**

VORYS

2022 Statistics

- **Other causes of data breaches (less than 10%) included:**
  - Physical security compromises
  - System errors
  - Business email compromises
  - Accidental data loss / stolen devices
  - Social engineering

VORYS

2022 Statistics

- **Other 2022 data breach statistics:**
  - 96% of breaches were **financially motivated**
  - 43% of cyber attacks aimed at **small businesses** through:
    - Phishing/social engineering (57%)
    - Compromised/stolen devices (33%)
    - Credential theft (30%)
  - 11% of cybersecurity incidents were **ransomware attacks**

VORYS

2022 Statistics

- Global cyberattacks increased by 38% in 2022 as compared to 2021
- Global average cost of a data breach in 2022 = **$4.35 million**
- Cost of a data breach in the United States in 2022 = **$9.44 million**

VORYS

Cybersecurity Cost Drivers

- **Detection and Escalation:**
  - Activities that allow a company to detect and report the breach to appropriate personnel within a specified time period (e.g., forensic investigation activities, audit services, crisis team management, communications).
- **Notification Costs**:
  - Activities that allow the company to notify individuals who had data compromised in the breach (e.g., newsletters, telephone calls, emails).

VORYS

Cybersecurity Cost Drivers

- **Post-Data Breach Response**:
  - Processes that help affected individuals or customers communicate with the company and costs associated with redress and reparation with data subject regulators (e.g., legal expenditures, credit reporting, issuing new accounts).
- **Lost Business Cost:**
  - Activities associated with the cost of lost business, including customer churn, business disruption, and system downtime (e.g., cost of business disruption, cost of lost customers, reputational loss).

VORYS

Types of Threats

- Skimmers
- Hacking/malware
- Physical theft
- Insiders
- Carelessness
- Ransomware/ Denial-of-service attacks

VORYS

Skimmers and Shimmers

- Credit, ATM and debit card info
- Typically perpetrated by organized crime
- Low barrier to entry (can buy online)

VORYS

Skimmers and Shimmers

The real card reader slot.

The capture device

The side cut out is not visible when on the ATM.

VORYS

Skimmers and Shimmers

VORYS

Skimmers and Shimmers

VORYS

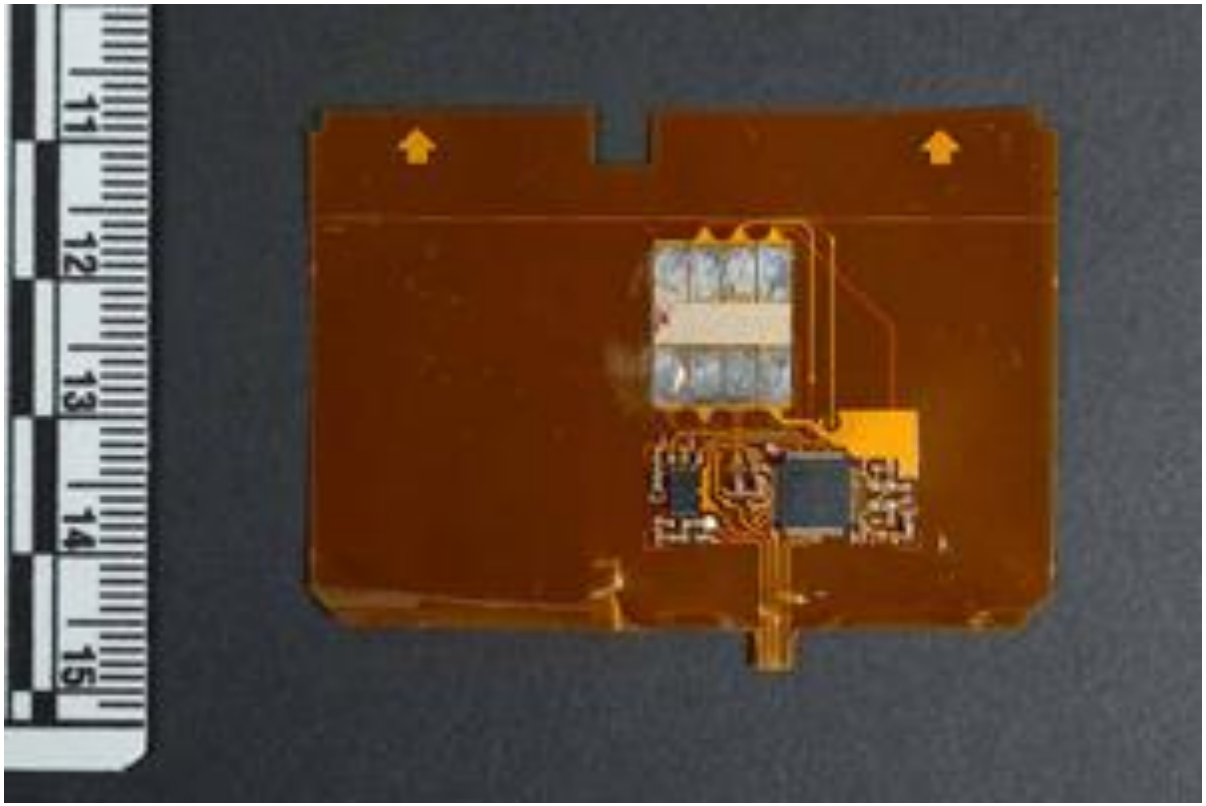
Skimmers (cont'd)

VORYS

Skimmers and Shimmers

VORYS

Skimmers and Shimmers



VORYS

Hacking / Malware

- Sony
  - More than 47,000 SSNs of current and former employees
  - Movies and emails
  - Hackers used malware, which allowed hackers to find other passwords

VORYS

Hacking / Malware—Vendors are Targets Too

- Target (110 million card records)
  - Hackers installed malware on HVAC vendor's system, found login credentials to Target's systems
- Home Depot (56 million card records)
  - Used vendor's user name and password to gain access to perimeter of Home Depot's network. Once inside, were able to gain elevated access and install malware on Home Depot's checkout systems.

VORYS

Physical Theft

- AvMed, Inc. (healthcare)
  - PII for more than 1.2 million customers compromised
  - Contained on two unencrypted laptops stolen from corporate office
- Starbucks
  - PII for more than 97,000 employees compromised after laptop stolen

VORYS

Physical Theft

- Office of Personnel Management
  - Personnel records of 22 million current and former federal employees compromised (includes records for employees with security clearances, including even fingerprints)
  - Undetected for 343 days
  - Used stolen credentials from a contractor to plant malware in the network

VORYS

Insiders—High Tech

- Vodafone (personal data of 2 million customers)
  - Insider likely assisted in installation of malware
- South Korea Credit Bureau (20 million records)
  - Employee stole information off of servers

VORYS

Insiders—High Tech

- *In re Countrywide Fin. Corp. Customer Data Sec. Breach Litig.*, Nos. 3:08-MD-01998, 1998, 2010 U.S. Dist. LEXIS 87409 (W.D. Ky. Aug. 20, 2010).
  - An employee of Countrywide copied customer data on a **flash drive** and sold the information as sales leads to other mortgage brokers.
  - The employee downloaded as many as 20,000 customer account records, including name, address, loan amounts and Social Security numbers **each week for 2 years.**

VORYS

Insiders—Low Tech

- Houston employee of U.S. Passport Agency took photos of passport applications to steal identities

- U.S. Passport Agency banned employees from bringing phones to work

VORYS

Carelessness

- Hacking Team (created spyware and malware programs for law enforcement and intelligence agencies)
  - Hacker gained access to engineer's PC while it was logged onto network using his password ("P4ssword")

- **<u>Most popular passwords as of 2022</u>**:

password	password1	12345	123456	1234567
12345678	123456789	guest	qwerty	a1b2c3
1234567890	1234567	111111	123123	abc123
iloveyou	1q2w3e4r	1zaq12wsx	dragon	sunshine
princess	letmein	654321	monkey	1qaz2wsx

VORYS

Ransomware / Denial of Service Attacks

- **Boston Children's Hospital ("BCH")**
  - **DoS attack:** cyber-attack that makes a machine or network resource unavailable by flooding the targeted system with additional traffic.
  - **Anonymous' DoS attack's impact on BCH:**
    - Inability to route prescriptions electronically to pharmacies
    - Email downtime for departments where email supports critical processes
    - Inability to access remotely hosted electronic health records
  - **Response:** Internal IT response; External retention of IT consultants to mitigate DDoS attack.

VORYS

Ransomware / Denial of Service Attacks

- **Hollywood Presbyterian Medical Center**
  - **Ransomware:** malicious software designed to block access to a computer system until a sum of money is paid.
  - Ransomware / malware locked access to files
  - Paid $17,000 in Bitcoins
- **ProtonMail** (encrypted email provider)
  - DDoS attack
  - Paid ransom and was attacked by new hackers

VORYS

Ransomware / Denial of Service Attacks

- **<u>Methodist Hospital (Henderson, KY)</u>**
  - Ransomware attack that limited KY hospital's use of its electronic web-based services
    - The attackers used "Locky" ransomware, which encrypts files on a computer/system and prevents their access/use.
  - Methodist declared an **"Internal State of Emergency"** that required the hospital to individually shut down and restart all computers to check for infection.
  - The attack, which lasted for nearly six days, required the hospital to **temporarily process everything on paper.**

VORYS

Timeline of a Breach

Eric W. Richardson and Brent D. Craft

Vorys, Sater, Seymour and Pease LLP
513.723.4000| ewrichardson@vorys.com| bdcraft@vorys.com

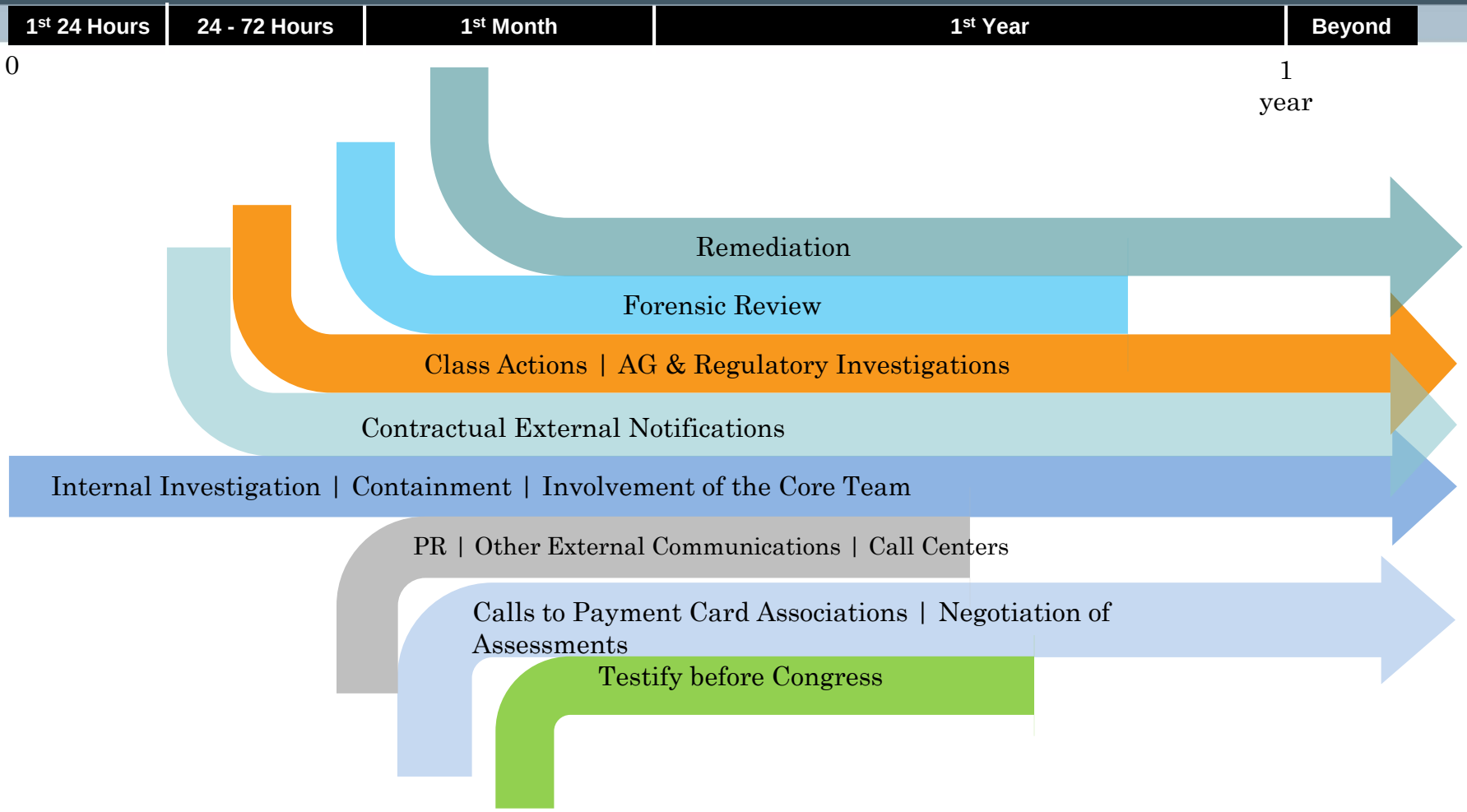
VORYS

Incident Happens – Immediate / Simultaneous Demands

- Customers
- Containment / Remediation
- Payment Card Brands
- News Media / Bloggers
- Forensic Investigators
- Major Shareholders
- Class Action Lawsuits
- Risk Management

VORYS

Coordinating Response



VORYS

The First 24 Hours

- Core Team determines if this is an Event or Incident
- Activate Your Workflow Processes
- Determine form and type of data, source of data, potential size

VORYS

The First 24 Hours

- **Start advising internally**
  - Members outside of Core Team and others who may be necessary
  - Advise appropriate Board Members
  - General Counsel has a special role
  - Communications
  - Information Owner (e.g. Marketing, HR)
- **Start internal investigation**

VORYS

The First 24-72 Hours

- Contact U.S. Secret Service
- Activate Forensic Investigator
- Consider contacting appropriate regulator(s)
- Make initial notifications to Payment Card Associations, credit card processor and acquiring bank
- Submit Standardized Initial Report to Payment Card Associations

VORYS

First Month – External Communications

- Statutory Notifications
- Press Releases
- FAQs across all media – Websites and Social Media Pages
- Risk Management – Insurance notices
- Daily meetings and calls with counsel to prepare for calls with regulators, plaintiffs' counsel and Payment Card Associations.

VORYS

First Month – Internal Communications

- Immediately before initial external communication:
  - Notify your employees and include “Help Line” number for questions
  - Consider notification to major shareholders
- Prepare scripting for customer calls to Call Center
- Prepare scripting for associate calls to Help Line

VORYS

First Month – Investigations/Lawsuits/Remediation

- FTC / CFPB Investigations or Insurance Commissioners Commence
  - Was there "reasonable" security?
  - What was the business purpose for collecting or retaining the data?
- Office of Civil Rights (Health and Human Services) if PHI involved
- Securities and Exchange Commission
- State AG Investigations Commence
- Class action lawsuits filed
- Remediation plans must be started

VORYS

First Year and Beyond: More to Come

- Review and finalize Forensic Reports (3-9 months)
  - Work with Investigator on results and wording
  - Finalize and implement remediation plan
  - Ongoing negotiations of assessments with Payment Card Associations (1-2 years)
  - Responding to document demands and inquiries from regulatory investigations; meetings and negotiations (1-2 years)
  - Addressing class actions

VORYS

Accuracy Matters

- Two main issues with inaccuracies in investigations:
  - Inaccuracies during the investigation
  - Inaccuracies in the resulting report

VORYS

Inaccuracies During the Investigation

- More and more companies are purchasing insurance policies that cover data breaches
- These policies are very specific and require detailed information about the claims.
- Coverage can hinge entirely upon the date of the breach and whether it can be linked to other breaches.
- Distinctions of timing can cost millions.

VORYS

Accuracy in Reporting Results of Investigations

The purpose of investigations is to gather the

FACTS

The goal of reporting the results of investigations is to share the

FACTS

Companies get in trouble when investigators deviate from the

FACTS

VORYS

Things to Avoid in Reporting Results of Investigations

1. Avoid Offering Opinions and Conclusions

- Different people can reach different opinions based on the same facts.
- At investigation stage, it is often too early to draw final conclusions.
- As time passes, your conclusions may change due to:
  - New documents
  - New testimony
  - Different context
- In other words, conclusions and opinions may be ***inaccurate***

VORYS

Things to Avoid in Reporting Results of Investigations

- If you must report your conclusions or opinions:
  - Avoid doing so in writing
  - Report conclusions orally
- If you must report your conclusions or opinions *in writing*, be careful to qualify them.
  - "As of right now…"
  - "Based on evidence currently available…"
  - "…but the investigation is still ongoing"

VORYS

Things to Avoid in Reporting Results of Investigations

2. Avoid Using Figures of Speech

- Metaphors, similes, and other figures of speech are very common; a part of our everyday life.
  - The 800 pound gorilla
  - The elephant in the room
  - The smoking gun
- They can emphasize points and highlight important details.
- They can also cause big problems down the road…

VORYS

Things to Avoid in Reporting Results of Investigations

- Litigants will interpret figures of speech differently
- Litigation can drag on for years—you can lose context.
- Examples:
  - "House of Cards"
  - "When the music stops"
  - "Churning"

VORYS

Accuracy Matters

- Major takeaways:
  - Be thorough in your investigation to ensure that accurate decisions can be made.
  - Be accurate in how you report the results of your investigation:
    - Avoid opinions and conclusions
    - Avoid unnecessary figures of speech
    - Stick to the ***facts***

VORYS

Bad Cybersecurity Habits

Eric W. Richardson, Jacob D. Mahle, J.B. Lind and Brent D. Craft

Vorys, Sater, Seymour and Pease LLP
513.723.4000| ewrichardson@vorys.com|
jdmahle@vorys.com | jblind@vorys.com | bdcraft@vorys.com

VORYS

Bad Cybersecurity Habits

- **<u>Technical / Access Control Bad Habits</u>**
  - Not regularly downloading and installing software updates, patches, firewalls, anti-virus
  - Not changing passwords to customer or other databases
  - Not segregating databases or networks
  - Not encrypting sensitive data
  - Not requiring multi-factor authentication

VORYS

Bad Cybersecurity Habits

- **<u>Technical/Access Control Bad Habits (cont'd)</u>**
  - Not implementing tiers of data access based on employee need
  - Not insulating sensitive data and network locations from public access points (e.g., wi-fi)
  - Not suspending inactive accounts after termination or lack of use

VORYS

Bad Cybersecurity Habits

- **<u>Data Retention Bad Habits</u>**
  - Unnecessarily maintaining customer and employee data and payment information
  - Not imposing data retention limits / policies (*e.g.*, no time limits on how long to retain certain types of data; keeping data beyond the reasonable time period)
  - Not disposing of information (hard copy and electronic) safely and securely

VORYS

Bad Cybersecurity Habits

- **<u>Breach Response Bad Habits</u>**
  - Not having an incident response plan or designated procedure to handle and decision breaches
  - Not having an internal procedure to ensure preservation of data in the event of a breach
  - Not having a forensic investigator or data security firm on retainer
  - Not having counsel involved early and throughout investigation, so as to maintain privilege

VORYS

Bad Cybersecurity Habits

- **<u>Breach Response Bad Habits (cont'd)</u>**
  - Not having statutory / regulatory notifications and press releases pre-drafted
  - Not identifying beforehand the governmental, private and other affected parties / stakeholders who must be notified in the event of a breach

VORYS

Bad Cybersecurity Habits

- **<u>Vendor / Third Party Bad Habits</u>**
  - Using vendor agreements that impose varying and sometimes conflicting requirements
  - Not requiring vendors to indemnify against breaches and other cyberliability
  - Not having cyberliability insurance that covers the likely risks

VORYS

Bad Cybersecurity Habits

- **<u>Other Bad Habits</u>**
  - Using inconsistent and/or vague language in and between policies
  - Not communicating consistently to customers—or having them agree to—your data policies and procedures, retention and security periods, data use, etc.

VORYS

Tips for Protection

- Review your workplace policies
  - Encrypt records, including in transport
  - Have a response plan
- Review your insurance policies
- Stay up-to-date in antivirus, anti-spyware software
- Backup files to protect against ransomware attacks

VORYS

Notification Laws and Emerging Legal Trends

Eric W. Richardson and Brent D. Craft

Vorys, Sater, Seymour and Pease LLP
513.723.4000| ewrichardson@vorys.com| bdcraft@vorys.com

VORYS

Federal Laws

- No comprehensive federal law governing cybersecurity for employee benefit service providers.
- Federal laws governing financial industry:
  - Fair Credit Reporting Act
  - Gramm-Leach-Bliley Act
  - Fair and Accurate Credit Transactions Act

VORYS

Section 5 of the FTC Act

Prohibits "**unfair or deceptive** acts or practices in or affecting commerce"	Enforcement through administrative enforcement actions or federal court

1) Unfair act or practice "causes or is likely to cause substantial injury to consumers;"

2) The injury "is not reasonably avoidable by consumers themselves;" and,

3) The injury is "not outweighed by countervailing benefits to consumers or competition."

VORYS

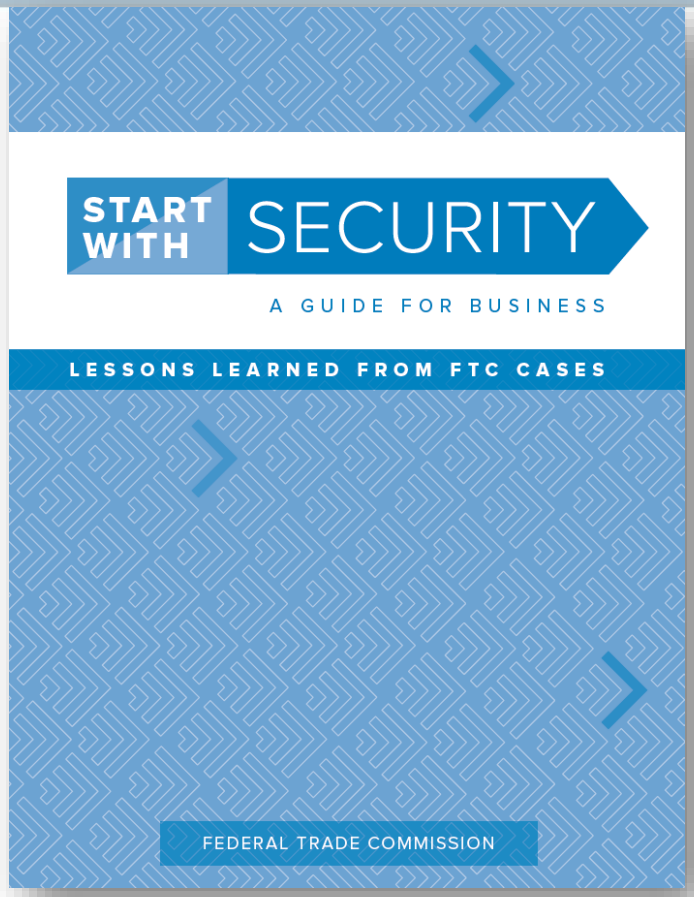
FTC's "Unfairness" Test in Data Security

- FTC does not require perfect data security
  - Recognizes no one-size-fits-all solution
- Whether a data security practice is unfair is determined through a cost-benefit analysis:
  - Probability and size of reasonably avoidable harms to consumers given a certain level of cybersecurity, ***VS.***
  - Cost to consumers if stronger cybersecurity implemented
- "Reasonableness"
  - Level of security may vary among size and complexity of the business and availability of tools.

VORYS

FTC's Data Security Guidance

- Lists lessons learned from prior enforcement actions.
- Targeted to businesses
- Identifies minimum data security expectations.



VORYS

FTC's Data Security Guidance (cont'd)

HIGHLIGHTS:

- Control access.
- Require secure passwords and authentication.
- Store sensitive personal information securely and protect it during transmission.
- Segment your network and monitor who's trying to get in and out.
- Secure remote access to your network.
- Make sure your service providers implement reasonable security measures.

VORYS

Revisions to Safeguards Rule

- **March 2019**: FTC announced proposed revisions to its Safeguards Rule
- **Safeguards Rule**: governs data security practices for financial institutions under the FTC's GLB Act jurisdiction
- Proposed revisions expand the scope of companies covered by the Rule **and** mandate that covered entities take certain specific steps to secure customers' information (e.g., encryption, multi-factor authentication)

VORYS

Notification Laws

- All 50 states plus the U.S. Territories have data breach notification laws
  - Alabama and South Dakota were the last 2 states to enact notification laws—Alabama's and South Dakota's laws became effective on June 1, 2018 and July 1, 2018, respectively.
  - U.S. Territories of Puerto Rico, Guam, and the U.S. Virgin Islands all have notification laws

VORYS

Notification Laws

- **<u>Notification laws typically consist of:</u>**
  - Definitions
    - "Breach" and "PII" definitions are very important, as these typically trigger requirements
  - Safe harbor
  - Notification requirements (timing, method)
  - Whether notification should be made to law enforcement, state AG, regulators
  - Enforcement/penalty provisions

VORYS

Ohio's Notification Law
O.R.C § 1349.19(A)(6), (A)(7)

- **Person**
  - [A]n individual, corporation, business trust, estate, trust, partnership, association, sole proprietorship, financial institution or other business entity if it conducts business in this state
- **Personal Information**
  - An **individual's first and last name or first initial and last name** in combination with any **one (1) or more of the following data elements**:
    - Social security number
    - Driver's license number or state ID card number
    - Account number or credit or debit card number, **in conjunction with** any required security code, access code, or password

VORYS

Ohio's Notification Law
O.R.C § 1349.19(A)(7)(b)

- Personal information **does not** include **publicly available information** that is lawfully made available to the general public from **federal, state or local government records** or distribution through **bona fide news media**
  - Newspapers, magazines, radio, television
  - Publications of charitable/nonprofit corporations or associations

VORYS

Ohio's Notification Law
O.R.C § 1349.19(A)(1)(a)

- **"Breach of the security of the system"**
  - **Unauthorized** access
  - **Computerized** data
  - Compromises the security or confidentiality of **personal information** owned or licensed by a **person**
  - Causes, reasonably is believed to have caused, or reasonably is believed will cause a **material risk of identity theft or fraud** to the person or property of a **resident of this state**

VORYS

Ohio's Notification Law
O.R.C § 1349.19(B)

- **When must a disclosure be made?**
  - Owner or licensee of computerized data containing **personal information** shall disclose any **breach of the security system** following discovery or notification of the breach to **any resident** whose data was, or reasonably believed to have been, **accessed and acquired by an unauthorized person** if the breach causes or reasonably is believed will cause a **material risk of identity theft or fraud**
- **Time for disclosure:**
  - Disclosure must be made in the **most expedient time possible** but **not later than 45 days** following discovery of the breach

VORYS

Ohio's Notification Law
O.R.C § 1349.191(E)

- Notification may be provided through:
  - Written notice;
  - Electronic notice (if primary communication with resident to whom disclosure must be made is by electronic means);
  - Telephone notice;
  - Substitute notice, if information holder demonstrates cost of notice exceeds $250,000 or class of affected persons exceeds 500,000
    - Email notice
    - Conspicuous posting of notice on business entity's website
    - Notification to major media outlets (if audience exceeds 75% of the population of the state)

VORYS

Ohio's Notification Law
O.R.C § 1349.191(E)(5)

- Substitute notice for business entities with ten (10) employees or fewer **and** cost of providing notice exceeds $10,000
  - Newspaper notice:
    - Circulation in the geographic area in which the business is located
    - Paid advertisement covers at least one-quarter of a page
    - Published in the newspaper at least once a week for three consecutive weeks
  - Conspicuous notice on business entity's website
  - Notification to major media outlets in the geographic area in which the business is located

VORYS

Ohio's Notification Law
O.R.C § 1349.191(C), (G)

- **Permissible Delay:**
  - Notification may be delayed if law enforcement agency determines notification will **impede criminal investigation**
- If circumstances require notification of **more than 1,000 persons at one time**:
  - Entity must also notify all consumer reporting agencies and credit bureaus

VORYS

Ohio's Notification Law
O.R.C § 1349.191(F)

- **Exemptions:**
  - Financial institutions, trust companies, or credit unions that are required by federal law to notify customers of an information security breach and are subject to examination by a regulatory agency for compliance with the applicable law (e.g., Gramm-Leach-Bliley Act (15 U.S.C. § 6801, *et seq.*); Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (12 C.F.R. Parts 30, 364, 568))
  - A covered entity as defined in 45 C.F.R. Part 160.103 (definition section of HHS Standards for Privacy of Individually Identifiable Health Information)
    - Includes health plan, health care clearinghouse, health care provider who transmits health information in electronic form

VORYS

Ohio's Notification Law
O.R.C § 1349.191(H), (I)

- **Ohio's Notification Law includes no provisions creating a private right of action for a violation**
- Any waiver of the law's requirements is contrary to public policy and void/unenforceable
- **<u>Enforcement:</u>**
  - Ohio AG may conduct an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of the law

VORYS

Kentucky's Notification Law
KRS § 365.732(1)(b)-(c)

- **Information Holder**
  - [A]ny person or business entity that conducts business in this state
- **Personally Identifiable Information**
  - An **individual's first and last name or first initial and last name** in combination with any **one (1) or more of the following data elements**:
    - Social security number
    - Driver's license number
    - Account number or credit or debit card number, **in conjunction with** any required security code, access code, or password

VORYS

Kentucky's Notification Law
KRS § 365.732(1)(a)

- **Breach**
  - **Unauthorized** acquisition
  - **Unencrypted** and **unredacted** data
  - Compromises the security, confidentiality, or integrity of **personally identifiable information** maintained by the **information holder**
  - Actually causes, or leads the information holder to reasonably believe has caused or will cause, **identity theft or fraud** against any **resident.**

VORYS

Kentucky's Notification Law
KRS § 365.732(2)

- **When must a disclosure be made?**
  - **Information holder** shall disclose any breach, following discovery or notification of the breach, to **any resident of Kentucky** whose **personal information** was, or is reasonably believed to have been, acquired by an **unauthorized person.**
- **Time for disclosure:**
  - Disclosure must be made in the **most expedient time possible** and **without unreasonable delay**

VORYS

Kentucky Notification Law
KRS § 365.732(5)

- Notification may be provided through:
  - Written notice;
  - Electronic notice (if consistent with requirements of 15 U.S.C. sec. 7001);
  - Substitute notice, if information holder demonstrates cost of notice exceeds $250,000 or class of affected persons exceeds 500,000
    - Email notice
    - Conspicuous posting of notice on information holder's website
    - Notification to major statewide media

VORYS

Kentucky Notification Law
KRS § 365.732(4), (7), (8)

- **Permissible Delay:**
  - Notification may be delayed if law enforcement agency determines notification will **impede criminal investigation**
- If circumstances require notification of **more than 1,000 persons at one time**:
  - Information holder must also notify all consumer reporting agencies and credit bureaus
- **Exemptions:**
  - Persons or entities subject to Title V of the Gramm-Leach-Bliley Act or HIPAA

VORYS

Notification Laws

- States starting to enact more stringent notification laws
- Requirements imposed in one state soon spread to other states—legislatures are seeking to expand protections to their residents' information
- **RULE OF THUMB:** Have your / your clients' policies and procedures comply with the strictest applicable state requirements

VORYS

Massachusetts Notification Law

- Amendments to Massachusetts Notification Law:
  - Expansion of information that must be reported
  - Imposition of new requirements on compromised entities
  - Additional clarification as to when entities are required to issue notice of a breach
- Changes took effect on April 11, 2019
- Represents trend toward more stringent notice requirements

VORYS

Massachusetts Notification Law

- Additional Requirements:
  - Entities that have experienced a data breach involving the personal information of Massachusetts residents must inform the Massachusetts AG and Office of Consumer Affairs and Business Regulation "whether the person or agency maintains a written information security program" (WISP).
  - New requirement provides regulators with mechanism to penalize entities who have failed to implement a compliant WISP.

VORYS

Massachusetts Notification Law

- Additional Requirements:
  - General requirement of 18 months of credit monitoring services must be provided when Social Security numbers are compromised
  - Breached credit reporting agencies must provide 42 months of free credit monitoring services when Social Security numbers are involved
  - Affected individuals cannot be required to waive their right to a private right of action as a condition to receive the credit monitoring services

VORYS

Massachusetts Notification Law

- Additional Requirements:
  - Companies must disclose to Massachusetts regulators the types of personal information compromised in the breach
  - Companies must inform affected residents that they have the right to place a security freeze on their credit reports at no charge
  - If a subsidiary is breached, the notification to affected residents must include the name of the parent or affiliated corporations

VORYS

Massachusetts Notification Law

- Additional Requirements:
  - Notice cannot be delayed on grounds that the total number of residents affected by the breach is not yet known
  - Companies must give notice "as soon as practicable and without unreasonable delay" once an entity "knows or has reason to know" of a breach of a resident's personal information

VORYS

New York Cybersecurity Regulation
23 NYCRR 500

- Official Title: "Cybersecurity Requirements for Financial Services Companies"
  - Effective date: March 1, 2017
- Sets forth cybersecurity requirements for banks, insurance companies, and other financial services institutions regulated by the NY Department of Financial Services
- Regulation was the **first of its kind** in the U.S.
- **Potential benchmark/model for states that follow in adopting cybersecurity regulations**

VORYS

New York Cybersecurity Regulation
23 NYCRR 500

- Requirements for Covered Entities:
  - A Cybersecurity program designed to protect consumers' private data
  - A written policy or policies that are approved by the board or a senior officer
  - A Chief Information Security Officer (CISO) to help protect data and systems, and to oversee and enforce cybersecurity policy.
  - Controls and plans in place to help ensure the safety and soundness of NY's financial services

VORYS

New York Cybersecurity Regulation
23 NYCRR 500

- Requirements for Covered Entities:
  - Annual penetration testing, bi-annual vulnerability assessments, audit trails, limiting system access, periodic review of access privileges, MFA or equivalent and encryption of data in transit and at rest.
  - 72 hour notice requirement of cybersecurity events; annual certification to DFS on compliance with regulation's requirements.

VORYS

New York Cybersecurity Regulation
23 NYCRR 500

- Cybersecurity Program Requirements:
  - Identify and assess **internal and external cybersecurity risks** that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems
  - Use **defensive infrastructure and policies and procedures** to protect the Information Systems and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts

VORYS

New York Cybersecurity Regulation
23 NYCRR 500

- Proposed Amendments to Regulation:
  - **Chief Information Security Officer (CISO) Authority & Responsibility.** Grant CISOs authority to manage cybersecurity risks appropriately, and require that the CISO report to the senior governing body
  - **Senior Governing Body.** The Board of Directors, or similar managerial body, must annually approve the written cybersecurity policy which must include policies regarding data retention, asset disposition, security awareness and training, breach notification, encryption requirements for nonpublic information, and vulnerability management.
  - **Vulnerability Management**. Develop written vulnerability management policies and procedures
  - **Multi-factor Authentication (MFA).** MFA implemented for remote access to all privileged accounts (admin or security accounts) or third-party applications (including cloud based) which host nonpublic information.

VORYS

New York Cybersecurity Regulation
23 NYCRR 500

- Proposed Amendments to Regulation:
  - **Data Inventory**. Maintain an asset inventory of all hardware and software, including their location and accessibility.
  - **Training and Monitoring.** Implement controls that protect against malicious code, and provide at least annual training with social engineering exercises to all employees.
  - **Third Party Event Notification.** The 72-hour notification requirement for cybersecurity events now requires entities to report events affecting them which occur at or within third-party service providers. Entities are required to provide, via NYDFS' website form, "any information requested regarding the investigation of the cybersecurity event," with an ongoing obligation to update and supplement the NYDFS form.
  - **Ransomware & Extortion Payment Reporting**. Covered entities must now report if they experience a cybersecurity event involving ransomware. If extortion payments are made in connection with the ransomware event, the entity must: (1) submit notice of payment within 24 hours; and (2) within 30 days of payment, provide a written description of the reasons payment was necessary, a description of alternatives considered.

VORYS

New York Cybersecurity Regulation
23 NYCRR 500

- Proposed Amendments to Regulation:
  - The comment period on the proposed amendments to NYDFS Reg. 500 concluded on January 9, 2023.
  - When adopted, most of the amendments to NYDFS Reg. 500 will become effective 180 days after adoption.
  - Expect states with comparable regulations that apply to licensed financial services companies (*e.g.*, insurance companies) to follow suit similar amendments.

VORYS

Ohio Data Protection Act

- **Ohio Data Protection Act**
  - Ohio Senate Bill 220, signed by Governor on August 3, 2018
  - Law went into effect on November 2, 2018
  - Act permits eligible organizations to rely on their conformance to certain cybersecurity standards/frameworks as an affirmative defense in data breach litigation
  - Provides organizations with legal incentive to implement cybersecurity programs and measures

VORYS

Ohio Data Protection Act

- To qualify for the affirmative defense, the organization must implement a written cybersecurity policy designed to:

  (1) protect the security and confidentiality of personal information;

  (2) protect against anticipated threats or hazards to the security or integrity of personal information; and

  (3) protect against unauthorized access to personal information that is likely to result in identity theft or fraud

VORYS

Ohio Data Protection Act

- The organization's cybersecurity program must also reasonably conform to one of the following standards/frameworks:
  - National Institute of Standards and Technology's (NIST) Cybersecurity Framework
  - NIST special publication 800-171, or 800-53 and 800-53a
  - Federal Risk and Authorization Management Program's Security Assessment Framework
  - Center for Internet Security's Critical Security Controls for Effective Cyber Defense
  - International Organization for Standardization (ISO)/International Electrotechnical Commission's (IEC) 27000 Family – Information Security Management Systems Standards

VORYS

Ohio Data Protection Act

- **Pluses:**
  - Provides potential defendants with some semblance of confidence if they meet the requirements of a qualifying standard / framework
  - Promotes uniformity of cybersecurity programs and practices
- **Minuses:**
  - Ohio-only law
  - Eligible standards are not necessarily uniform or static
  - If a company fails to meet an eligible standard / framework, does a presumption of liability attach?

VORYS

Ohio Data Protection Act

- Other states are following suit.
  - On September 23, 2020, the Indiana Attorney General announced intention to establish a rule that would create a safe harbor for businesses that have "reasonably designed, implemented and executed" data security plans pursuant to specified frameworks
  - The rule would recognize frameworks similar to those under the Ohio law: NIST Cybersecurity Framework, PCI-DSS, ISO 27000

VORYS

CA Consumer Privacy Act of 2018

- **California Consumer Privacy Act of 2018**
  - Imposes regulations on the collection, use, and disclosure of consumers' personal information
  - Enacted on June 28, 2018
  - Required Date of Compliance: January 1, 2020
  - Example of states implementing measures to protect the privacy rights of consumers, similar to the EU GDPR

VORYS

CA Consumer Privacy Act of 2018

- Broadly applies to "businesses"—any for profit legal entity (e.g., corporation, partnership, LLC) that does business in the State of California, that collects consumers' personal information, and that meets **one** of the following thresholds:
  - Has gross revenue in excess of $25,000,000;
  - Buys, receives, or sells for commercial purposes the personal information of 50,000 or more consumers, households, or devices; **or**
  - Derives 50 percent or more of its revenue from selling consumers' personal information

VORYS

CA Consumer Privacy Act of 2018

- Law creates new privacy rights for consumers:
  - The right for consumers to know what personal information is being collected
  - The right to know whether the personal information is being sold or disclosed
  - The right to prevent the sale of one's personal information
  - The right to access one's personal information; and
  - The right to enjoy equal service and price even if one exercises his or her privacy rights.

VORYS

CA Consumer Privacy Act of 2018

- Under the law, business must inform consumers of categories of information being collected and the purposes for which the information is collected
- Consumers can request that the business disclose:

1. The categories of the consumers' personal information collected
2. The sources of the collected information
3. The business purposes for the collection or sale of the information
4. The identities of third parties with whom the information has been shared
5. The specific pieces of personal information collected.

VORYS

CA Consumer Privacy Act of 2018

- The law creates a private right of action for consumers' claims based on the **unauthorized access** and **exfiltration**, **theft**, or **disclosure** of **unencrypted and nonredacted** personal information.
- Allows for statutory damages that are the greater of:

  (a) between $100 and $750 per consumer per incident; or

  (b) actual damages
- Also provides for administrative enforcement with penalties up to $2,500 ($7,500 if intentional) per violation.

VORYS

CA Consumer Privacy Act of 2018

- On September 25, 2020, the Governor of California signed into law multiple amendments to the CCPA:
  - PHI "de-identified" in accordance with the HIPAA Privacy rule is exempt from CCPA requirements
  - If a business sells or shares de-identified PHI, it must notify consumers in its privacy policy and disclose the method through which the information was de-identified

VORYS

CA Consumer Privacy Act of 2018

- CCPA Amendments, cont'd:
  - If a business sells or licenses de-identified PHI to a third party, it must have a contract with the third party which includes: (1) a statement that de-identified information being sold or licensed contains de-identified PHI; (2) a statement that the purchaser cannot re-identify, or attempt to re-identify, the de-identified information; and (3) a prohibition on the further sharing of the de-identified PHI unless the third-party is subject to the same use restrictions. (Effective Jan. 1, 2021)

VORYS

CA Consumer Privacy Act of 2018

- CCPA Amendments, cont'd:
  - Re-identification of de-identified information is prohibited unless it is for one of the following purposes: (1) a HIPAA regulated entity's treatment, payment, or health care operations; (2) public health activities or purposes set forth in HIPAA; (3) research; (4) compliance with legal requirements; or (5) performance of a contract that engages an entity to re-identify the information for testing, analysis, validation, or related statistical techniques.
  - PHI collected by a "covered entity" or a "business associate" under HIPAA is excepted from the CCPA.

VORYS

Legal Ethics and Cybersecurity

Eric W. Richardson and Brent D. Craft

Vorys, Sater, Seymour and Pease LLP
513.723.4000| ewrichardson@vorys.com| bdcraft@vorys.com

VORYS

Ethics and Cybersecurity

- The rapid pace at which new cybersecurity threats appear, the frequent passage and implementation of new cybersecurity statutes and regulations, and the short time frames in which clients and their attorneys must act in the event of a data breach implicate and highlight several ethical duties imposed by the Kentucky Rules of Professional Conduct.
  - Competence
  - Diligence
  - Communication
  - Confidentiality
  - Safekeeping of Client Property

VORYS

Law Firms

- Law firms are ethically required to ensure that their attorneys are observing and complying with these ethical requirements.
  - Rule 5.1(a)
    - A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, 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.

VORYS

Law Firms

- Rule 5.1 – Relevant Commentary
  - (2) Paragraph (a) requires lawyers with managerial authority within a firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the Rules of Professional Conduct. Such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised.

VORYS

Law Firms

- Cybersecurity Threats to Law Firms
  - Confidential Documents and Data
    - Law firms are holders hold huge volumes of privileged documents and private information
    - Physical sources (laptops, thumb drives) particularly vulnerable
    - Insider breaches are possible
  - Ransomware
    - Disabling of a firm's document management or billing systems
      - Official-looking email or attachment
      - Downloads covert program that takes over the lawyer's machine, disabling the system and holding the files and data hostage

VORYS

Law Firms

- Cybersecurity Threats to Law Firms (cont'd)
  - User Error / Carelessness
    - Misdirected emails; failing to encrypt emails
    - Mistaken clicking on email or website links
      - Downloading malicious software
      - Phishing attacks – providing login / password / confidential information

VORYS

Law Firms

- Cybersecurity Threats to Law Firms (cont'd)
  - Cybersurveillance
    - Downloading malicious surveillance software via phishing scheme
      - Users baited with a phishing email.
      - User asked to log in to seemingly official website.
      - With login information, hacker can access confidential
        - email databases
        - contracts
        - private and personal information
        - financial records
        - attorney-client privileged information

VORYS

Law Firms

- Cybersecurity Threats to Law Firms (cont'd)
  - Hacktivism
    - Infiltration/exfiltration not typically not financially motivated (think WikiLeaks)
    - **Panama Papers**
      - 11 million documents leaked from Panamanian law firm Mossack Fonseca in 2015
      - Revealed financial documentation and breached attorney-client privilege for over 200,000 offshore entities
      - Privacy of financial dealings and records was a paramount concern for many wealthy clients of the firm

VORYS

Ethics Rules: Competence

- **Rule 1.1 - Competence**
  - A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
  - Relevant Commentary:
    - **Thoroughness and Preparation** (5) Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners.
    - **Maintaining Competence** (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, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

VORYS

Ethics Rules: Competence

- Competence and Cybersecurity
  - Data breaches can happen to clients of any size and type
  - A lawyer should have sufficient knowledge of cybersecurity and data breach laws and regulations so that he or she can competently advise the client in the event of a breach
  - Cybersecurity and data breach laws are frequently evolving—"keep[ing] abreast of changes in the law and its practice" is essential

VORYS

Ethics Rules: Diligence

- **Rule 1.3 – Diligence**
  - A lawyer shall act with reasonable diligence and promptness in representing a client.
  - Relevant Commentary:
    - (3) Perhaps no professional shortcoming is more widely resented than procrastination. A client's interests often can be adversely affected by the passage of time or the change of conditions … Even when the client's interests are not affected in substance, however, unreasonable delay can cause a client needless anxiety and undermine confidence in the lawyer's trustworthiness.

VORYS

Ethics Rules: Diligence

- Diligence and Data Breaches
  - Whenever a data breach occurs, time is of the essence
  - Unreasonable delay in assessing and responding to a data breach can irreparably damage a client's business and ability to defend in resulting litigation
  - Notifications laws require an entity that has experienced a data breach to move quickly
    - In some cases a breached organization must provide notices within 72 hours (*See* KRS § 61.931-34)

VORYS

Ethics Rules: Communication

- **<u>Rule 1.4 - Communication</u>**
  - (a)(3) A lawyer shall keep the client reasonably informed about the status of the matter
  - (a)(4) A lawyer shall promptly comply with reasonable requests for information
  - (b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation
  - Relevant Commentary:
    - (3) [P]aragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.
    - (5) The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so.

VORYS

Ethics Rules: Communication

- Communication
  - A lawyer's ability to adequately communicate the status of a data breach with a client depends on the lawyer's familiarity with relevant law and existing threats
  - A lawyers' familiarity with cybersecurity laws and threats allows attorneys to communicate with a client by:
    - Properly identifying a breach
    - Developing a strategy (with the client and forensic examiners) to address a breach
    - Advising as to legal and regulatory requirements when a breach has occurred

VORYS

Ethics Rules: Confidentiality

- **<u>Rule 1.6 – Confidentiality of Information</u>**
  - (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).
  - Relevant Commentary:
    - (14) A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.

VORYS

Ethics Rules: Confidentiality

- **Rule 1.6 – Confidentiality of Information (Relevant Commentary, cont'd)**
  - (15) When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

VORYS

Ethics Rules: Safekeeping Property

- **Rule 1.15 – Safekeeping Property**
  - (a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. Funds shall be kept in a separate account maintained in the state where the lawyer's office is situated, or elsewhere with the consent of the client, third person, or both in the event of a claim by each to the property. The separate account referred to in the preceding sentence shall be maintained in a bank which has agreed to notify the Kentucky Bar Association in the event that any overdraft occurs in the account. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of five years after termination of the representation.

VORYS

Ethics Rules: Confidentiality and Safekeeping Property

- Confidentiality
  - Lawyers and law firms are prime targets for cybercriminals due to the types of documents and information with which they are entrusted
  - Potential Targets:
    - Privileged and confidential documents
    - Financial records
    - Trust Account

VORYS

Ethics Rules: Confidentiality and Safekeeping Property

- A lawyer's / law firm's adoption of appropriate and reasonable cybersecurity measures and protections fall within the scope of the Confidentiality and Safekeeping Property Rules
- Such steps are required by the lawyer's duty to take "reasonable precautions to prevent the information from coming into the hands of unintended recipients" and to ensure that client property is "appropriately safeguarded"

VORYS

Questions?

Eric W. Richardson and Brent D. Craft

Vorys, Sater, Seymour and Pease LLP
513.723.4000 | ewrichardson@vorys.com | bdcraft@vorys.com

VORYS

Thank you!
Please return your completed CLE forms to the check-in table

VORYS