Dentons In-House Counsel Webinar Series: Grow, Protect, Operate & Finance
March 2, 2022

大成 DENTONS BINGHAM GREENEBAUM

Tax Update for In-House General Counsel

Mark A. Loyd
Partner · Co-Leader, Tax National Practice Group
Louisville, Kentucky

(502) 587-3552
mark.loyd@dentons.com

Ryan Dunn
Partner, Tax National Practice Group
Lexington, Kentucky

(502) 587-3538
ryan.dunn@dentons.com

Bailey Roese
Partner, Tax National Practice Group
Louisville, Kentucky

(502) 587-3522
bailey.roese@dentons.com

Agenda

Discuss major tax trends and issues facing employers, including:

- Remote work and implications for employers
- Marketplace facilitator rules and updates
- Sales tax and exemptions related to asset purchases
- Tax savings strategies on acquisitions and divestures

Remote Work: Trends

- Remote working arrangements were already on the rise before the pandemic, but appear to be here to stay
- Searches for remote jobs are at an all-time high – from June 2019 to June 2021, candidates seeking remote work increased by 360%
- In workforce surveys, 2/3 of employees in banking, finance, accounting, insurance, and IT stated their jobs could be done entirely remotely
- Finance and tech industries seem to be leading the charge in the transition to remote work
- Even as pandemic restrictions have lifted, employees increasingly say they want flexibility to work from home, or a permanent work from home arrangement
- Bottom line: Remote work is here to stay.

- Source: *Employee Benefit News*

It’s 2022. Do you know where your employees are?

- Many taxing authorities offered some grace in 2020 for pandemic-related temporary remote working arrangements, either formally or informally.
- However, states and localities are becoming more aggressive as revenue impacts have started to hit.
- Employers should begin reviewing their current policies and realities to prepare for federal, state, and local tax implications, which can include:
  - State Nexus for sales tax purposes
  - Withholding and employment tax obligations
  - Corporate income tax compliance/doing business
  - Permanent establishment (for foreign businesses)
  - Local license taxes

Sales Tax & Income Tax

- States may impose a sales tax where there is physical presence
  - Can include employees
  - Having employees in a state may trigger sales tax collection and reporting obligations, even where the taxpayer does not meet economic nexus standards
- Many states impose corporate income tax or franchise tax on taxpayers that are "doing business" in their state
  - "Doing business" can include employees *but* don't forget about PL 86-272
    - Prohibits states from imposing an income tax on a taxpayer whose sole connection to the state are employees who engage in mere "solicitation"

Employee withholding and payroll tax

- An employee is subject to tax on all of the employee’s income in the state in which they reside.
- An employee is also subject to income tax in the state in which the employee performs services, and an employer is obligated to withhold state income taxes on such services, absent a safe harbor or a reciprocal agreement.
- Only a few states provide a safe harbor, meaning that an employee may work in a state for up to a certain number of days without triggering the employee’s obligation to pay taxes and the employer’s obligation to withhold taxes.
- However, most states do not have a safe harbor and tax is due for as little as one day’s work in a state.
- Reciprocal agreements exempt state income from tax in the state in which the employee works, effectively making the employee’s income subject to tax only in their state of residency

Employee withholding and payroll tax

- Many states have reciprocal agreements with border states that allow taxpayers to pay tax only where they live, instead of where they work.
- Certain other states (e.g., New York, Delaware, Nebraska, Pennsylvania, and Connecticut) have rules and requirements for withholding that depend on whether the employee is working from home for his or her own convenience or the convenience of the employer.
- Localities may have license or occupational taxes based on where work is physically performed.
- Each of these issues can create withholding obligations for the employer, or more.

Nexus and Telecommuting Example: Kentucky

- The Kentucky Department of Revenue does not administer license, occupational, or other excise taxes imposed by **cities, counties, and other local** jurisdictions in this state. For Kentucky state income tax purposes, employers employing Kentucky residents, and/or nonresidents who reside in states with which Kentucky has a **reciprocal agreement**, will not need to change their current withholding practices during the period when these employees are working from home. Requirements for withholding of tax in either case remain unchanged by restrictions related to the COVID-19 public health emergency. KDOR FAQ
- DOR will continue reviewing Kentucky state income tax nexus determinations on a case-by-case basis. KDOR FAQ

International Remote work

- Additional costs, complexity, and burdens for both employer and employee
  - Taxable presence risk
  - Tax return filings (even if no income tax due)
  - Payroll tax filings
  - Foreign tax withholding obligations
  - Right to work / visa compliance
  - Foreign employment law
  - Employee tax residency

Inbound Illustration

- A foreign person must file a U.S. tax return and pay U.S. tax on its “effectively connected income” when it is “engaged in the conduct of a trade or business in the United States” (“ETOB”).
    - ETOB is somewhat of an amorphous standard. All facts and circumstances are considered.
        - If a foreign entity performs “personal services within the United States” through its employees, the foreign entity will be ETOB.

Income Tax Treaties

- Does the U.S. have an income tax treaty with the foreign country?
- Will the foreign employer have a permanent establishment in the U.S.?
    - a fixed place of business through which the business of a foreign person is wholly or partly carried on.
        - This is typically an office or a place of management. An office of an affiliate that has space available for the foreign entity can be considered a PE.
    - An employee in the U.S. that habitually exercises in the U.S., an authority to conclude contracts in the name of the foreign entity.
    - "Services PE" – (i) the foreign entity performs services for third parties (and not the foreign entity itself) in the U.S. and (ii) the services are provided in the U.S. for an aggregate of 183 days or more in any twelve-month period with respect to the same or connected project for customers who are residents of the U.S.
- What functions will the employee be carrying out?

Employee Considerations

- Employees must be aware of individual residency rules
- Even if the foreign employer does not have a PE in the U.S., the foreign employer needs to withhold U.S. income tax from employee's wages.
  - Some treaties (*e.g.* Canada) allow for U.S. wage withholding to be avoided. However, it requires the employee to obtain an ITIN. Obtaining an ITIN can take months, because the employee must first apply for (and be denied) a social security number.
- Tax return filing requirements

What Employers Can Do

- Gather relevant teams (HR, Legal, Accounting, Payroll) to best understand the current state of remote work at your company
- Locate or gather key information from employees. Have employees transitioned to remote work permanently? Where do they live? Do some employees work remotely part time?
- Are there policies in place for employees? Is there a system in place for recording work location?
- Ensure employees understand their personal tax responsibility vis a vis the employer's (*i.e.*, withholding)
- Review information and identify any new risks or compliance obstacles

Marketplace Facilitators/Providers

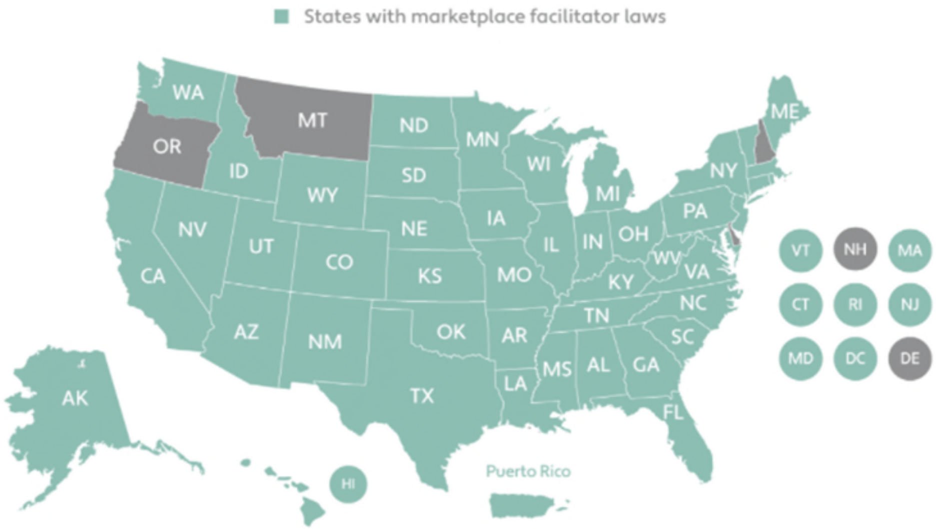
- Marketplace facilitators or providers are those that sell products on behalf of individual sellers (for example, Amazon or Etsy)
- Marketplace facilitator laws impose an obligation on the marketplace facilitator to collect and remit sales tax to states on behalf of the individual marketplace sellers
- Before these laws began to appear, marketplace facilitators could take the position that they were not the actual seller under the sales tax law, and thus were not responsible for collecting and remitting the tax.
- For many states, compliance obligations began in the last few years.
- Many states have thresholds similar to remote seller economic nexus registration requirements (i.e., $100k or 200 transactions in a year). If a marketplace facilitator has a physical presence in the state, the threshold would not apply and registration would be required regardless.
- Requirements vary widely by state.

Marketplace Facilitators/Providers

- Some states require the marketplace facilitator to identify sales made on behalf of marketplace sellers separately from its own direct sales
- Some states require or allow the marketplace facilitator to file a separate return for any third-party sales
- Some states require certification that the marketplace facilitator will collect and remit tax on behalf of the marketplace seller

Marketplace Facilitators/Providers

As of June 30, 2021. Source: Avalara



Sales Tax Exemptions: Asset Purchases

- Is your company looking to acquire another business? Or, are you looking to sell? Depending on the structure of the deal, sales tax could apply.
- If structured as an asset sale, any sale of tangible personal property involved in the deal (*e.g.*, machinery, inventory, office equipment, raw materials) could potentially trigger a sales tax liability.
- Luckily – there are a number of sales tax exemptions that may apply, too.

Common exemptions

- Intangible personal property not typically subject to sales tax (*e.g.*, goodwill)
- Many states exempt "occasional sales" or "casual sales" from sales tax.
  - Isolated sales that do not typically occur, either because the seller is not regularly engaged in the business of making retail sales, or because the type of transaction is not a typical one
  - Caution: many states are vague about whether an asset sale would be considered an occasional sale
  - Can also be known as "bulk sale" exemption – but often comes with disclosure requirements
- Purchases for resale
  - To avoid pyramiding of tax, states exempt TPP that is purchased to be resold.
  - For example, inventory.
  - In an asset sale, if the inventory is being purchased to be resold to customers, it likely qualifies for the resale exemption

Common exemptions

- Exempt purchaser
  - *E.g.*, government entity, nonprofits
- Industry-Specific exemptions
  - Manufacturing exemptions: many states exempt manufacturing equipment, tools and supplies, and raw materials used in the manufacturing process.
  - Extremely state-specific and facts-and-circumstances specific. Examples:
  - Kentucky: Exemption for Machinery for New and Expanded Industry. Exempt if 4 requirements are met:
    - machinery;
    - used directly in the manufacturing process;
    - incorporated for the first time into plant facilities established in Kentucky;
    - not replace other machinery.
  - Indiana: Machinery and equipment used to directly manufacture pre-fabricated construction materials sold at retail.

Ensuring exemption is received

- Document, document, document.
  - Obtain/provide and properly fill out resale or exemption certificate
- Review exemptions carefully to ensure availability and applicability to assets (e.g., manufacturing equipment)
- Review bulk sale disclosure and filing obligations
- Careful drafting of the Asset Purchase Agreement can save headaches down the road.
  - Ensure assets are separately listed and invoiced where needed to avoid subjecting entire purchase to sales tax
- Negotiate tax provisions where possible, but understand it may not save you from liability.

Tax savings strategies on acquisitions and divestitures

- 26 U.S. Code § 1202. Partial exclusion for gain from certain small business stock
- (a) Exclusion
  - (1) IN GENERAL - In the case of a taxpayer other than a corporation, gross income shall not include 50 percent of any gain from the sale or exchange of qualified small business stock held for more than 5 years.
  - (2) * * *
  - (3) * * *
  - (4) 100 PERCENT EXCLUSION FOR STOCK ACQUIRED DURING CERTAIN PERIODS IN 2010 AND THEREAFTER - **In the case of qualified small business stock acquired after the date of the enactment of the Creating Small Business Jobs Act of 2010—**
    - **(A) paragraph (1) shall be applied by substituting "100 percent" for "50 percent",**
    - (B) * * *
    - (C) * * *

Potential benefit

- Maximum amount of exclusion is $10 million (or, if greater, 10x basis of stock) <u>per shareholder</u>
- Benefit is also available on asset sales followed by a liquidation. Corporation would pay 21% on appreciated assets, but then $10 million of liquidation proceeds would be tax free to <u>each shareholder</u>.
- Rollovers / reorganizations

Major Requirements

- C corporation stock issued directly to taxpayer in exchange for money, property, or compensation for services (*i.e.* not purchased from third party)
- At all times before the issuance of the stock and immediately after, the corporation had less than $50 million in gross assets
- Stock held at least 5 years
- During substantially all (80%? *e.g.* 4 out of 5 years) of the taxpayer's holding period, the corporation met the active business requirement.
  - 80% (by value) of the corporation's assets are used in a qualified trade or business
  - Cash is generally not used in trade or business
  - FMV of intangibles including goodwill can be used in the trade or business

Qualified Trade or Business

- For purposes of this subsection, the term “qualified trade or business” means any trade or business other than—
- (A) any trade or business involving the performance of services in the fields of health, law, engineering, architecture, accounting, actuarial science, performing arts, consulting, athletics, financial services, brokerage services, or any trade or business where the principal asset of such trade or business is the reputation or skill of 1 or more of its employees,
- (B) any banking, insurance, financing, leasing, investing, or similar business,
- (C) any farming business (including the business of raising or harvesting trees),
- (D) any business involving the production or extraction of products of a character with respect to which a deduction is allowable under section 613 or 613A, and (oil/gas/etc.)
- (E) any business of operating a hotel, motel, restaurant, or similar business.

Questions?

Mark A. Loyd
Partner · Co-Leader, Tax National Practice Group
Louisville, Kentucky

(502) 587-3552
mark.loyd@dentons.com

Ryan Dunn
Partner, Tax National Practice Group
Lexington, Kentucky

(502) 587-3538
ryan.dunn@dentons.com

Bailey Roese
Partner, Tax National Practice Group
Louisville, Kentucky

(502) 587-3522
bailey.roese@dentons.com

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Enterprise, Dentons' wholly owned subsidiary of innovation, advisory and technology operating units. Dentons' polycentric approach, commitment to inclusion and diversity and world-class talent challenge the status quo to advance client interests in the communities in which we live and work. www.dentons.com.

Follow the Data: How Regulators, Criminals, and Compliance Programs are Planning for 2022 and Beyond

CLE Seminar In-House Counsel Webinar Series
March 2, 2022

Allison Bender / allison.bender@dentons.com
Ramy Fayed / ramy.fayed@dentons.com
Peter Stockburger / peter.stockburger@dentons.com

Agenda

- **Regulatory datapoints and priorities**. 2022 priorities for state, federal, and healthcare regulators.

- **Criminal datapoints and trends**. Trends for data crime in the US, internationally, and specific to the healthcare sector.

- **Compliance program datapoints and priorities**. 2022 priorities for clients subject to the evolving state, federal, and healthcare regulatory compliance frameworks.

Introductions

Allison J. Bender
Partner
+1 202 202 496 7362
allison.bender@dentons.com

Ramy Fayed
Partner
+1 202 408 6193
ramy.fayed@dentons.com

Peter Stockburger
Partner
+1 619 595 8018
peter.stockburger@dentons.com

Regulators Follow the Data

State, Federal, and Health Regulatory Datapoints and Priorities

US Privacy Legal and Regulatory Landscape

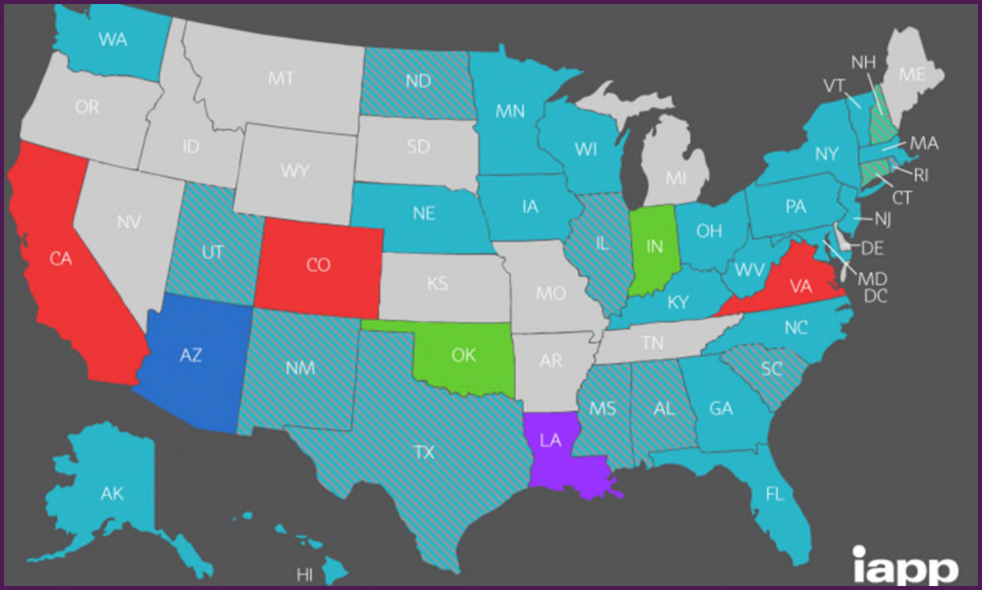
Federal

- Unfair Business
  - FTC Act
- Children
  - COPPA
- US Federal Financial Laws
  - Fair Credit Reporting Act
  - GLBA
- US Federal Healthcare Laws
  - HIPAA / HITECH
  - 21st Century Cures Act

State

- Data breach
- Consumer privacy laws
- Health information
- Cybersecurity
- Children
- Biometric information
- Insurance information
- Financial information

State Regulator Datapoints



- Since 2018, **50%** of US states have either signed (3) or introduced (22) updated data privacy legislation.
- **24%** of introduced/passed data privacy laws include some form of private cause of action.
- **195+** lawsuits have been filed citing the California Consumer Privacy Act.
- 280 incidents reported to Washington State Attorney General in 2021 mark a **500%** increase from 2020.
- **$10 million** in state funding allocated to the California Privacy Protection Agency to enforce CA privacy laws
- Indiana's Consumer Data Protection Act passed through the Senate on February 1, 2022 and is pending House approval. If signed, Indiana will the **fourth** state with a comprehensive consumer protection law.

State Regulator Priorities
Biometric Laws

- **Definition**. “Biometric identifiers” and “biometric information”.
- **50 State Data Security Laws**. Biometric data in definition of personal information for security and breach notification.
- **Illinois**. Biometric specific law with significant liability exposure. Notice and consent requirements.
- **New York State**. Biometric specific law relating to employment.
- **New York City**. Biometric specific law with signage requirements.
- **Portland**. Biometric specific law prohibiting facial recognition technology in place of public accommodation within city limits.
- **Baltimore**. Ban on facial recognition systems within city limits.
- **Texas / Washington**. Biometric specific law that requires notice and consent.
- **Pending state laws**. Maryland, Massachusetts, New Jersey, New York, South Carolina, Vermont, West Virginia.

State Regulator Priorities
Developing Landscape

- **<u>Increased enforcement</u>**. State AGs and regulatory agencies have been increasingly active in investigating and enforcing violations of state data privacy and protection laws, as will states that begin to enforce their implemented laws, currently Virginia and Colorado
- **<u>Developing state law</u>**. State law is still developing on several key issues related to data privacy and consumer protection, including: preemption; AI and other novel technologies; privileged nature of data breach forensic investigations; standing to bring suit based on risk of future harm.
- **<u>Legislative processes</u>**. Introduction and passing of bills during a period of increased politicization.

Federal Regulator Datapoints

- DOJ launched Civil Cyber-Fraud Initiative in October 2021. In 2020, the DOJ collected **$2.2 billion** in settlements/judgments for civil cases brought pursuant to the False Claims Act.
- **$100 million** SEC settlement with crypto platform BlockFi for certain registration and disclosure failures. This follows SEC's new proposed rules that include a **48-hour** data breach notification requirement.
- Estimated **250,000** Microsoft Exchange servers impacted by 2021 zero-day compromise, resulting in FBI actions to unilaterally scan for and contact companies who did not patch vulnerability.
- **24** data privacy bills have been introduced by this Congress, **6** with bipartisan sponsors.
- **$768.2 billion** in spending authorized under 2022 National Defense Authorization Act.

Federal Regulator Priorities
Developing Landscape

<u>Signed Law:</u>
- FY22 National Defense Authorization Act

<u>Pending Legislation</u>:
- Strengthening American Cybersecurity Act of 2022
- The CISA Cyber Exercise Act
- The Pipeline Security Act
- Stop China IP Theft Act
- Data Elimination and Limiting Extensive Tracking and Exchange (DELETE) Act

<u>Regulations, Directives, Guidance</u>:
- Ongoing implementation of President Biden’s Executive Order on Improving the Nation’s Cybersecurity.
- FBI/CISA/NSA guidance and alerts regarding ongoing threats related to the December 2020 SolarWinds incident, Accellion incident, Microsoft Exchange incident, and others.
- OFAC updated advisory regarding sanctions and ransomware.
- Federal Reserve, OCC, and FDIC 36-hour notification requirement for certain cybersecurity incidents.
- TSA Security Directive on Pipelines.

Healthcare Regulator Datapoints

- HHS-OCR resolved over **26,000** complaint investigations
- Over **500** healthcare organizations reported breaches to HHS-OCR involving 500+ records (over **23M** individuals impacted)
- Healthcare entities accounted for **79%** of reported data breaches in 2020
- **68** health care providers impacting over **1,200** healthcare sites disrupted by ransomware attacks in 2021
- Over 250 bills or resolutions in virtually every state are being prepared or have been introduced specifically addressing cybersecurity

Healthcare Regulator Priorities

- Amendment to HITECH Act
- NIST call for public comment
- HHS-OCR Cybersecurity Newsletters (Controlling Access and Securing Legacy Systems)
- Balance access and interoperability against cyberattacks, patient safety, uninterrupted care, and healthcare consumer confidence
- Address increased risk associated with telehealth and virtual care
- Compliance with Information Blocking Rule

Criminals Follow the Data

Cyber Crime Datapoints and Trends

United States Cybercrime Datapoints

- The average cost for a data breach in the U.S. in 2020 was **$9.05 million**.
- **4.8 million** reports of identify theft and fraud to FTC in 2020; 45% increase from 2019.
- **58%** of US companies reported revenue loss following a ransomware attack.

FBI Internet Crime Report 2020:

- **791,790** cyber crime complaints were submitted in 2020, a **69.4% increase** from 2019, and a 165% increase from 2016.
- **$4.2 billion** in losses were reported.
- **69,541** victims were located in California, the most of any US state.

United States Cybercrime Trends
Supply Chain Hacks

- Kronos – Ransomware on December 11, 2021 impacting approximately 2,000 organizations, and resulting in inability to issue paychecks or W-2s. Some companies still have not caught up.
- Kaseya - Used by ransomware gang REvil to simultaneously hit between 800 and 1,500 downstream companies.
- SolarWinds – Software with malicious code used by approximately 33,000 customers.

United States Cybercrime Trends

2021 Proliferation

Colonial Pipeline Company

Exchange

KIA

JBS FOODS

CNA

LOG4J

acer

International Cybercrime Datapoints

- The average time to identify and contain a data breach in 2020 was **287 days**.
- Ransomware incidents expected to cost the global economy an estimated **$20 billion** in 2021.
- A business email compromise in 2020 resulted in an average fraudulent payment of **$1.17 million** to threat actors.
- Responding to phishing attacks and attempts cost organizations on average **$1,500** per employee in 2020.
- **54%** of companies that detected ransomware attacks said the cybercriminals succeeded in encrypting their data.

International Cybercrime Trends

Nation-state actors:

- SolarWinds attributed to Russian state actors
- Exchange zero-day attributed to Chinese state actors
- Russia-Ukraine conflict demonstrating role that cyberwarfare will play in coming years.

But, increased international cooperation:

- Russian Bulletproof Hosting Kingpin Gets Five Years
- Ukrainian indicted in US for Kaseya ransomware attack
- Police Arrest Five Members Tied to the REvil Ransomware Gang
- Feds indict 4 from China in state-sponsored cyber attacks

International Cybercrime Trends
IP Theft

"[T]he value of theft of intellectual property from American industry… represents the **single greatest transfer of wealth in history.**"

Former director of NSA and commander of USCYBERCOM

Healthcare Cybercrime Datapoints

- In 2021, there were over **700** major health data breaches affecting over **45** million individuals
- Based on data in the HIPAA Breach Reporting Tool **73%** of all breaches in 2021 were identified as hacking/IT incidents and those incidents were responsible for about **94%** of individuals affected
- Medical records are among the hottest commodities on the dark web (SSNs are available for as low as **$1**; compared to medical records at around **$250**
- Average cost of healthcare data breaches is about **$9.4M** per incident. Average cost of ransomware attacks is about **$4.6M** per incident
- Ransomware attacks cost healthcare organizations over **$20B** in downtime

Healthcare Cybercrime Trends

- Cyberattacks expected to triple. Nearly three quarters of health systems, hospitals and physician organizations report that their infrastructures still are not prepared to respond
- Supply chain management, even for high-performing healthcare organizations, represents high risk
- Shift from “spray and pray” to “big game hunting”
- Exploit security vulnerabilities and inability to patch IoMT

Compliance Programs Follow the Data

State, Federal, and Health Compliance Datapoints and Priorities

Compliance Program Datapoints

- Security awareness training reduces phishing expenses by **more than 50%** percent.
- Maintaining an incident response capability plan cuts data breach costs by nearly **55%**.
- Out of 25 potential cost factors, non-compliance with regulatory requirements was the **top cost amplifier**.
- **61%** of cybersecurity professionals consider their organization’s cybersecurity team understaffed.
- **47%** of consumers who follow data privacy issues have switched companies over data policies or data sharing.

Compliance Program Takeaways (Representative HHS-OCR Settlements 2021)

Peachstate Health Management, dba AEON Clinical Laboratories

- Diagnostic/ clinical/ genetic testing lab provider in Georgia
- Systemic noncompliance with the HIPAA Security Rule
- Failures to conduct an enterprise-wide risk analysis, implement risk management and audit controls, and maintain documentation of HIPAA Security Rule policies and procedures

Excellus

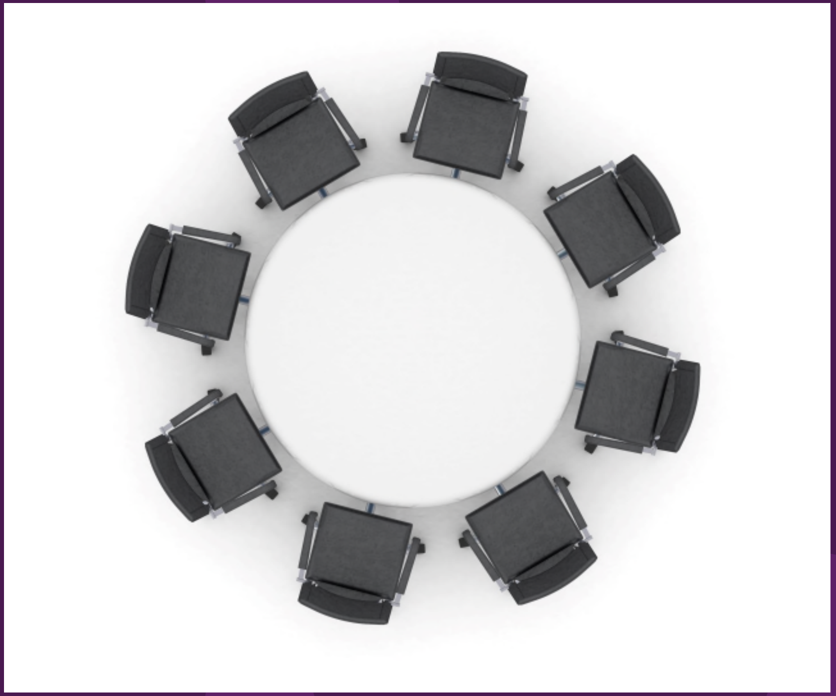
- Health insurer in New York
- Data breach affecting 9.3M individuals
- Failures to conduct an accurate and thorough risk analysis, implement sufficient security measures (i.e., risk management), implement policies and procedures to review information system activity and access management for ePHI

Compliance Program Priorities
Key Takeaways

- **<u>Prepare Now</u>**. 2023 is fast approaching. Lookback to 2022. Don't sleep on preparation. Starting now saves time and effort.
- **<u>Be Proactive</u>**. As more states and industries are regulated, expect your operations and data to be covered by multiple frameworks soon.
- **<u>Data Map</u>**. Know what data you have, where it's stored, who is touching it, and where it is going.
- **<u>Strategic Considerations</u>**. Omnibus approach or state specific? Market leading? Compliance focused?
- **<u>Employee / Contractor Programs</u>**. Assuming no legislative change in California, HR programs will need to be stood up around the CPRA. What about production staff and contractors?
- **<u>Cookies / Digital Collection Methods</u>**. This area of practice is under a microscope. Audit, update, correct.
- **<u>Don't Sleep On Security</u>**. Data breaches are largest source of liability. What is "reasonable" under CA law and elsewhere?
- **<u>Documentation Matters</u>**. Informal processes are not enough – documented policies and procedures help.

Compliance Program Priorities
Action Items

- Proactive gap analysis/risk assessment and legal consultation for applicable existing and incoming regulations.
- Document and implement an information security plan that includes reasonable operational, physical, and technical safeguards for data.
- Map all data that you maintain and process.
- Audit vendor and third-party access configurations, data security standards, and contractual language.
- Revisit existing data backup contingencies.
- Mandatory and periodic employee phishing, cyber, and data privacy training.
- Designate employee(s) responsible for information security and data privacy compliance.
- Review and update policies and procedures.
- Implement zero-trust.



Questions?

大成 DENTONS

Thank you

Allison Bender, Partner
D +1 202 496 7362
M +1 703 853 7999
allison.bender@dentons.com

Ramy Fayed, Partner
D +1 202 408 6193
M +1 202 256 1882
ramy.fayed@dentons.com

Peter Stockburger, Partner
D +1 619 595 8018
M +1 619 876 1971
peter.stockburger@dentons.com