The Intersection of Non-Competes and Employee Mobility

Seyfarth Shaw LLP

Legal Disclaimer

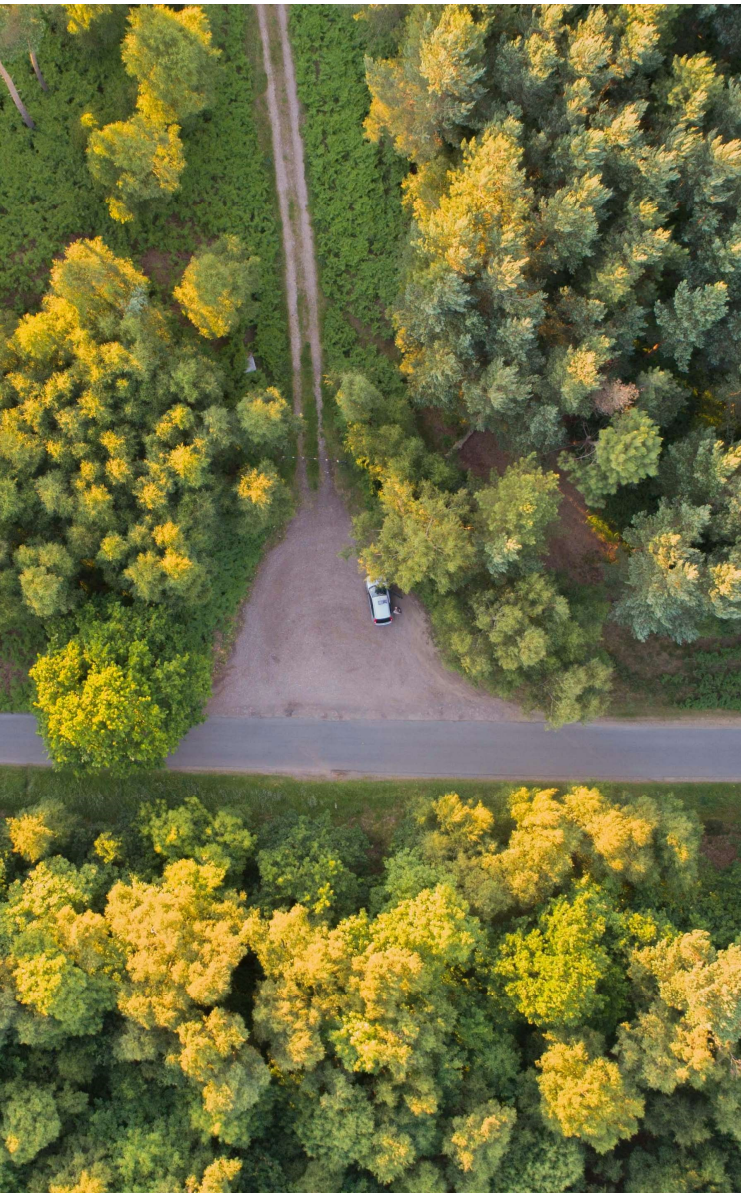
This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Speakers

Kate Perrelli
Partner
Boston Office

Dan Hart
Partner
Atlanta Office

Cat Johns
Associate
Boston Office



Agenda

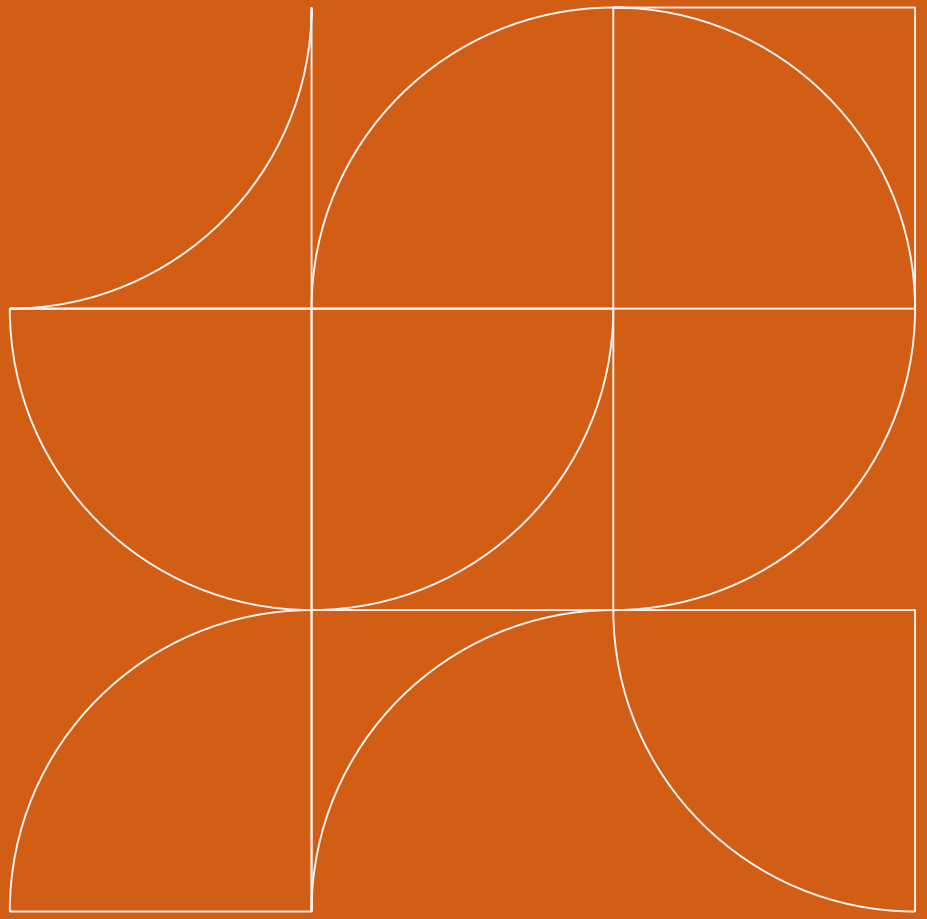
1 | Protecting Confidential Information in the “New” Workplace

2 | Trade Secrets Worthy of Protective Measures

3 | Use of Non-Competes – What is the State of Play?

4 | Tools and Tips to Shore Up and Reinforce Other Protections

Protecting Confidential Information in the "New" Workplace



Increased Risks in the “New” Workplace

40%
of the U.S. workforce works remotely at least part of the time.

1 in 4
Projections anticipate that 1 in 4 Americans will be working remotely by 2025.

~20%
Trade secret theft increased in the last year.

85%
of trade secret theft is committed by employees or business partners.

Over the past few years, the number of trade secret misappropriation lawsuits has continually increased.

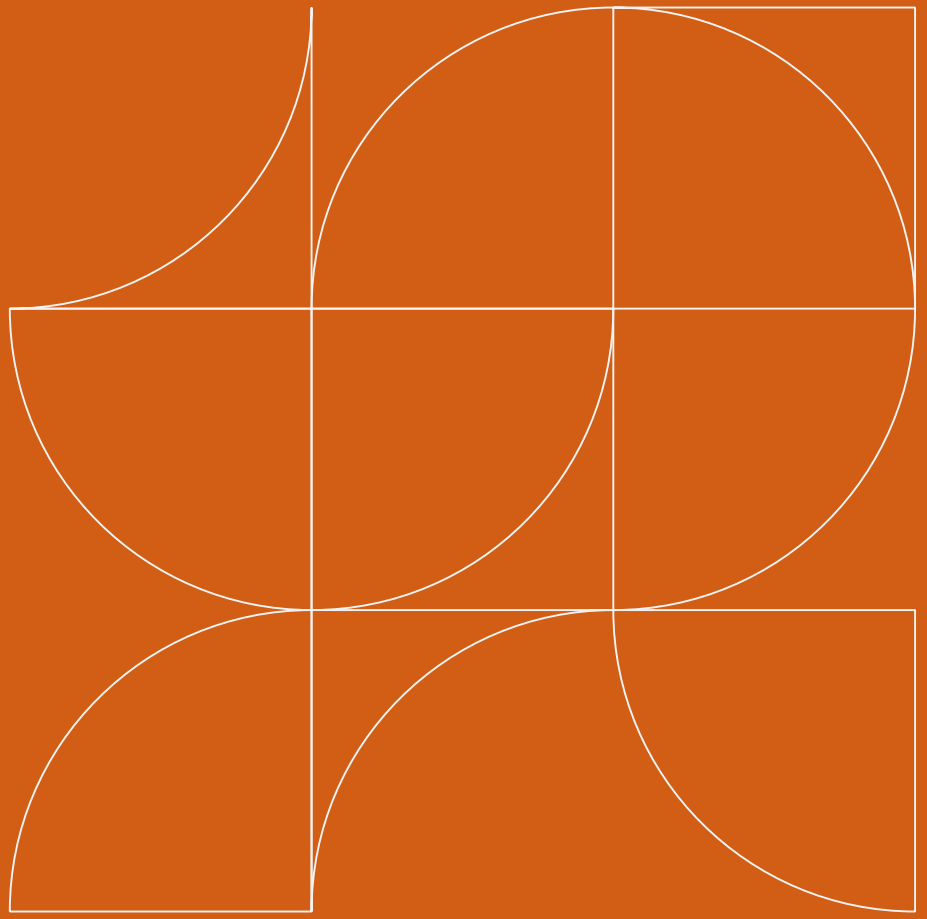
Remote Work Environments Challenges

- Relaxation of document management rules or and security measures
- Belief that employees have wider latitude to email, copy, send, print, or download information.

Heightened risks of trade secret/confidential information theft/disclosure because of remote work and mobile employees

- unsecure personal and public wi-fi networks
- unsecure personal devices
- loss or theft of devices
- unsecure personal email accounts to transfer corporate data
- syncing with unsecured personal cloud storage accounts
- unsecure printed materials
- unencrypted portable electronic storage devices
- unsecure connections to employers' systems
- unsecure conference call lines
- increased visibility in public locations of confidential information
- opportunities for roommates, spouses, and other co-habitants to access trade secrets
- increased phishing schemes and other fraud
- subpar video conferencing platforms
- decreased familiarity with what is and is not confidential

Types of Trade Secrets



Standards for Protecting Trade Secrets

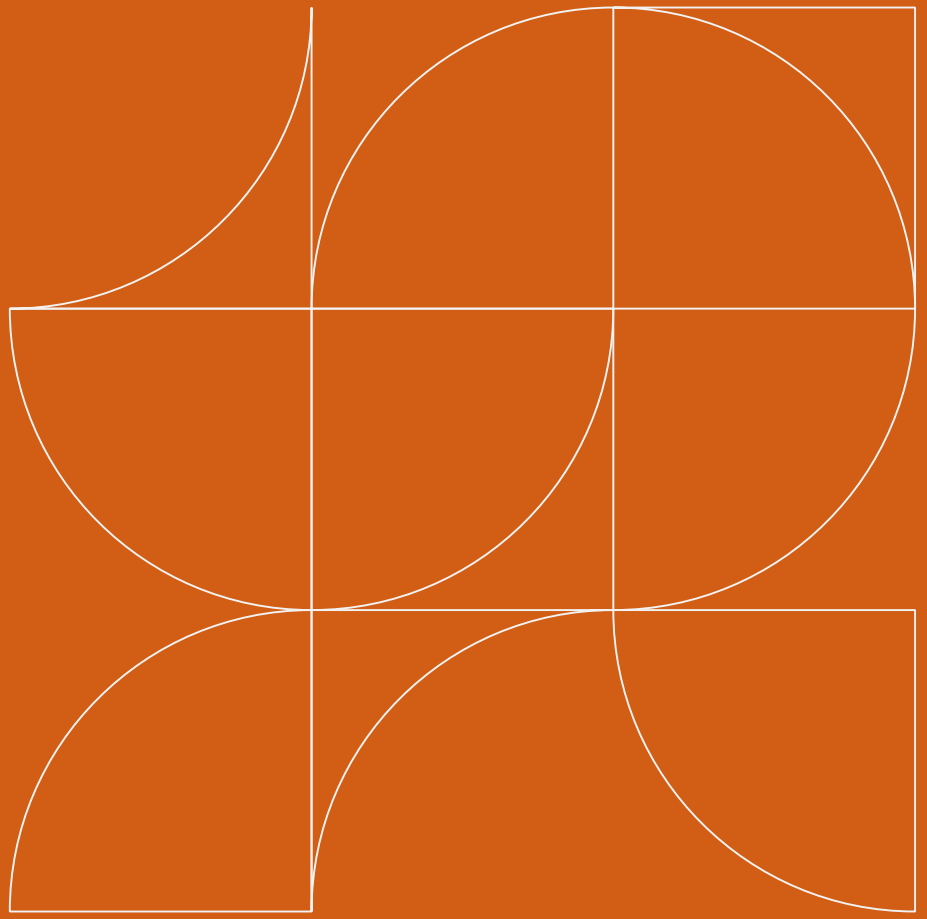
- Defend Trade Secrets Act of 2016
- Uniform Trade Secrets Act

Examples of Information that May Be **Trade Secrets**

- Product Formulas
- Manufacturing Processes
- Marketing Strategies
- Business Plans
- Sensitive Financial Information
- Pricing/Cost Information
- Unique Software & Source Code
- Customer Information (e.g., requirements, preferences, order history, purchasing trends)
- Internal Opportunities/Trends
- Negative Research Results
- Know How

Use of Non-Compete Agreements To Protect Against Use/Disclosure of Trade Secrets/Confidential Information–

What is the State of Play?



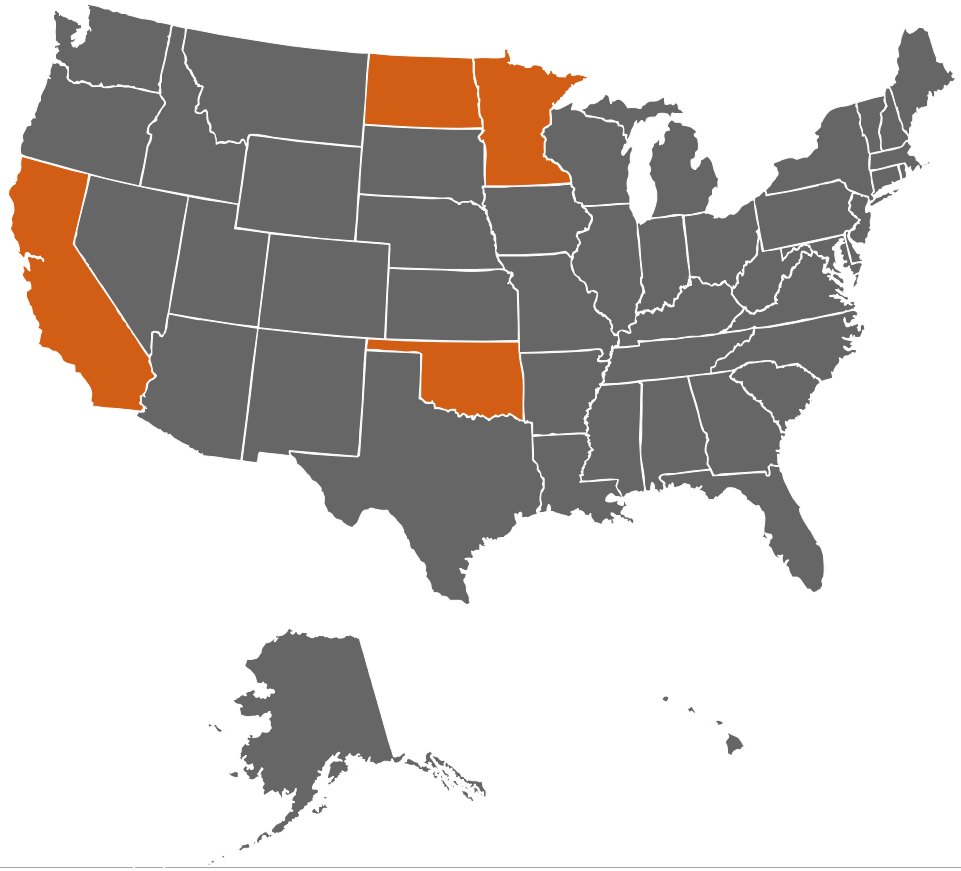
On **January 5, 2023**, the FTC published a proposed rule banning all non-compete agreements:

- A vote on the rule is expected in April
- If passed, likely to face an immediate challenge

The NLRB General Counsel released a memo claiming non-competes in employment and severance agreements typically violate the NLRA

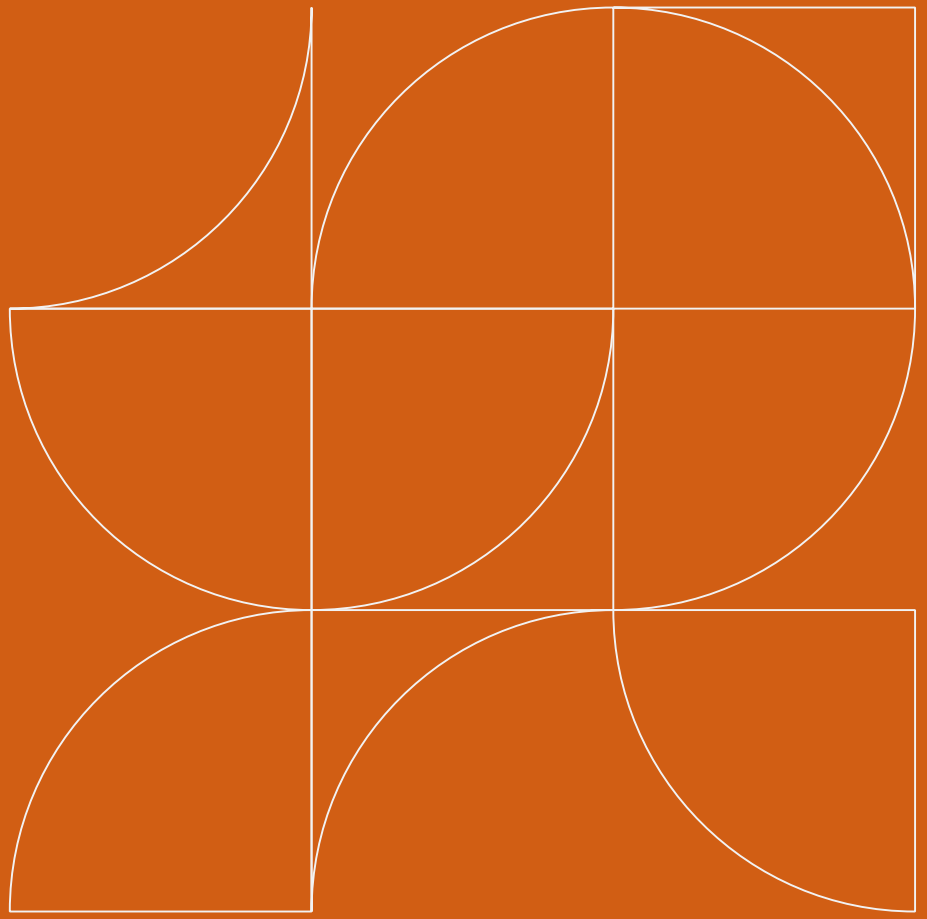
Several states have statutory restrictions on non-competes, and four have complete bans: California, Minnesota, North Dakota, and Oklahoma.

Noncompete Federal and State Landscape

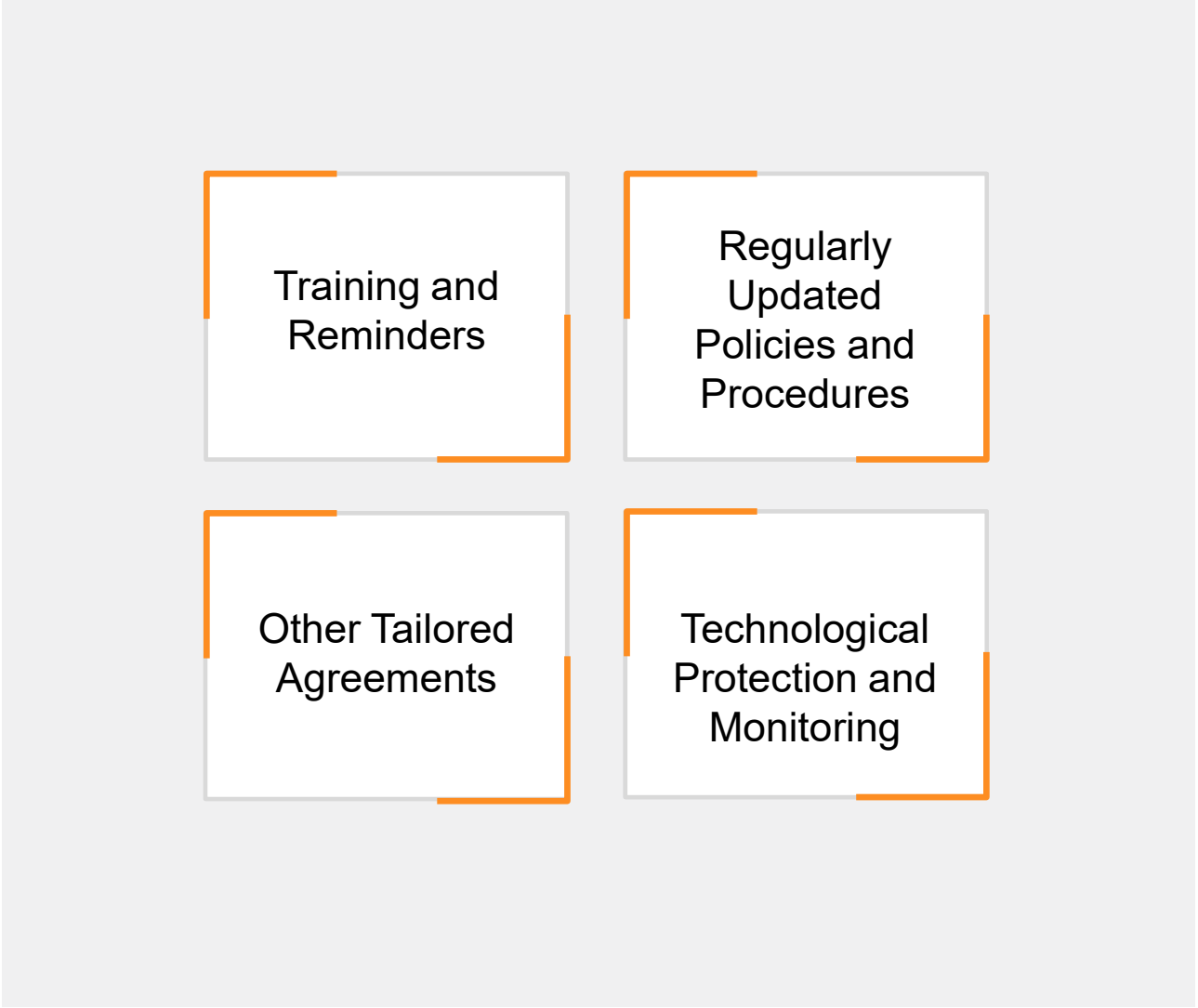


Keeping Non-Compete Agreements Compliant with Evolving Law

Tools and Tips Beyond Non-Compete Agreements – *Shore up Other Protections*

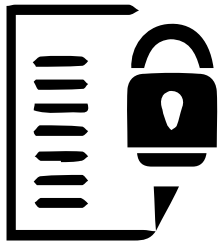


Critical Assets



Other Employment Agreements

Policy Examples

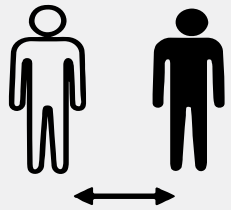


- Code of Conduct
- Confidentiality
- Bring Your Own Device (BYOD)
- Company Device
- Internet Usage
- Data and Cyber Security
- Remote Work
- Workplace Visitors
- Acknowledgement of Receipt
- Exit Interview

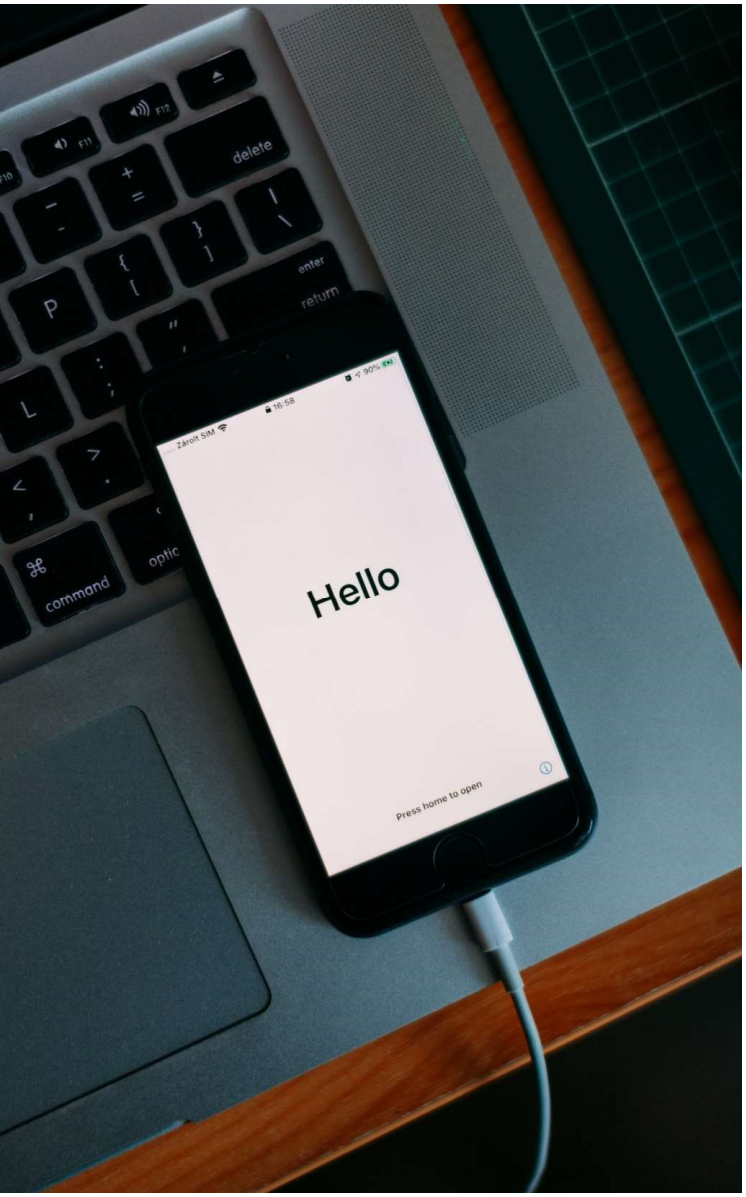
Remote Work Environment Best Practices

1. Choose videoconference platforms wisely and require the use of approved platforms.
2. Remind employees regularly of confidentiality obligations.
3. Ensure you have written policies for remote work protocols, including a prohibition on sharing documents, and disseminate early and often.
4. Increase monitoring to detect exfiltration of company data.
5. Ask employees what devices they are using from home.
6. Only allow remote access through a secure VPN with encryption.
7. Prohibit work from public places (coffee shops etc.) and on public Wi-Fi.
8. Be mindful of sharing home office space.

Protocols: From “Arrival” to “Departure”



- Consider confidential information (yours and others) from the time of recruitment to the time an employee leaves
- Part of protecting your trade secrets is ensuring that new employees aren’t bringing their prior employers’ trade secrets with them
- Care is needed when hire or departure involves competitors and/or companies with their agreements



On-Boarding Procedures

1. **Create and maintain a culture of confidentiality**
   - Ensure employees understand what is considered confidential
   - Mark things confidential
   - Consistency is key
2. **Policies and procedures distributed with the new-hire package**
3. **Interactive training**
   - Implement early and, if not part of onboarding, offer later
   - Consider trackable e-modules

Departing Employee Procedures

1. Exit Interview protocols (checklist of items to go over; have them sign)
2. Provide copies of agreements and go over them to remind of obligations
3. Shut off computer access
4. Return of property
5. Preserve devices
6. Consider forensic review.
7. Review internal logs – printing, access, etc.

Departing Employee Procedures

- ❑ Ensure that arrangements are made to have all company data removed from any personal devices
- ❑ Disable access to company computer networks and devices
- ❑ Make sure you obtain usernames and passwords for all company social media accounts
- ❑ Inform the employee of continuing obligations under agreements with the company and provide copies of applicable agreements
- ❑ Consider a letter to the new employer and employee with a reminder of continuing obligations and copies of agreements
- ❑ Consider preserving departing employee's emails and devices and/or forensically imaging devices with a chain of custody certification
- ❑ Consider using an exit interview certification

Exit Interviews & Processes

- **Must adapt due to inability for in-person exit interview but the same steps are key:**
  - Prepare for the interview, identify the trade secret and confidential information the employee accessed/used
  - Consider having in-house counsel or HR and the employee's manager present via video conference as appropriate
  - Check employee's computer activities and work activities in advance of the meeting
- **Arrange for remote remediation of company data**
- **Ensure that all company property, hardware, and devices have been returned, including email and cloud data, and social media accounts; consider using an inventory list**
- **Offer to have materials picked up from the house, if necessary**

Train, Train, and Train Some More

- Keep confidentiality top-of-mind not only at hiring but throughout employment
- Interactive training helps employees learn and retain key information
- Use email reminders to keep policies “top of mind”
- Routine follow-up for sensitive hires

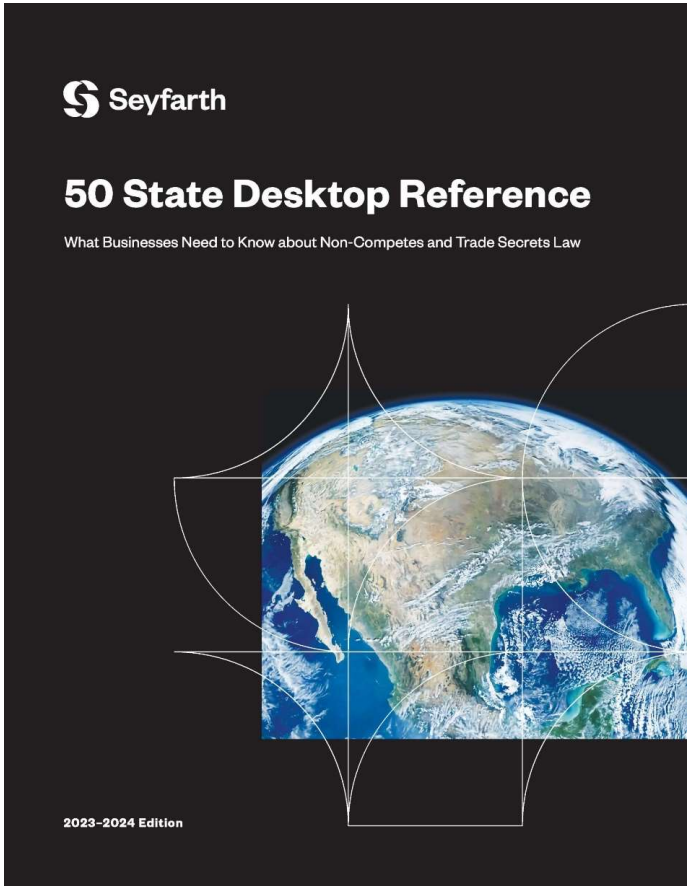
Takeaways

1. Maintain a robust system for data safety, including monitoring protocols
2. Various third-party tools and applications help monitor employees' use and access to confidential information
   - Some programs provide security alerts and/or screenshots when documents are used irregularly (e.g., uploaded to file-share sites)
3. Implement forensic reviews and device preservation for a deeper dive into how documents were accessed and used


ASK
ASK

CLE CODE

Stay Up to Date on Non-Compete Issues



www.TradeSecretsLaw.com

thank you

For more information, visit:
www.tradesecretslaw.com