



SIMMONS PERRINE MOYER BERGMAN PLC

115 3rd Street SE, Suite 1200 | Cedar Rapids, IA 52401 | 319.366.7641 • 1150 5th Street, Suite 170 | Coralville, IA 52241 | 319.354.1019

www.spmblaw.com



Banking & Finance: Employment Matters

July 7, 2022

2022 Summer Webinar Series

Continuing Legal Education

CLE Notice: This presentation is an accredited program under the regulations of the Iowa Supreme Court Commission on Continuing Legal Education. This program will provide a maximum of 1 hour of regular credit toward the mandatory continuing legal education requirements established by Rules 41.3 and 42.2. [Activity #380178]

Disclaimer: This presentation is designed and intended for general information purposes only and is not intended, nor should it be construed or relied on, as legal advice. Please consult your attorney if specific legal information is desired.



Today's Presenters:



Thomas N. DeBoom

(319) 896-4091

tdeboom@spmbllaw.com



Erin R. Nathan

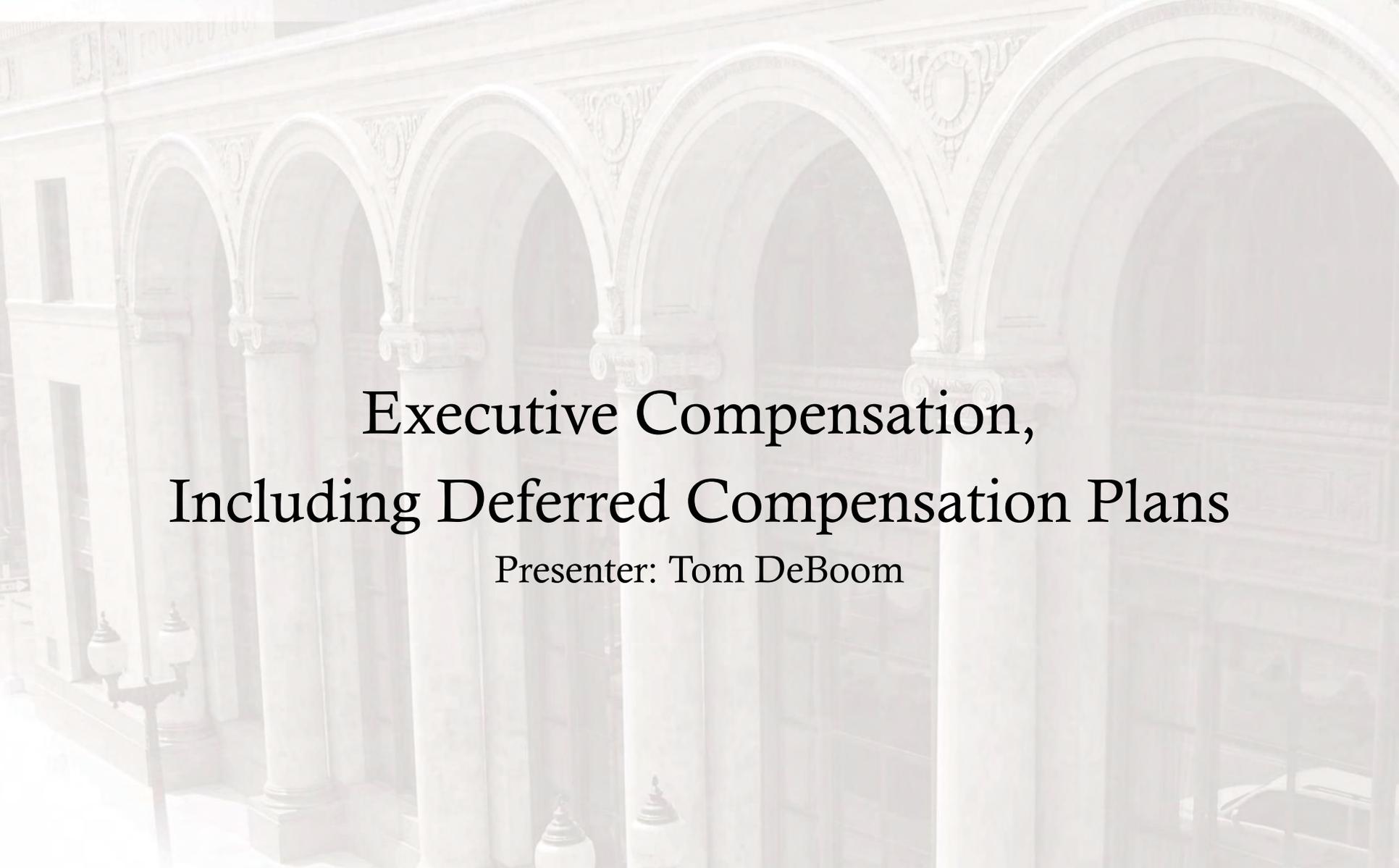
(319) 896-4013

enathan@spmbllaw.com



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmbllaw.com



Executive Compensation, Including Deferred Compensation Plans

Presenter: Tom DeBoom



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmbllaw.com

Types of Benefits

- **Equity:** The executive receives an award of some kind of equity-based benefit, such as:
 - Restricted stock
 - Stock appraisal rights
 - Stock options
- **Phantom Equity:** The executive receives an award that is not actually an equity interest in the company, but provides a benefit based upon the value or change in value of the company's stock/equity interests
- **Benefits Based upon Company Performance:** The executive receives an award based upon the company's performance (e.g., revenue or EBITDA)
- **Benefit Based upon Salary:** A deferred compensation arrangement with annual contributions based upon a percentage of salary



Types of Benefits, *continued.*

- **Bank-Owned Life Insurance and Split-Dollar Benefit:** Both a type of benefit and a method of funding a benefit. Generally, the company owns the policy, and the employee receives an economic benefit in the policy in the form of the death benefit and possibly some of the cash value
- **Split-Dollar Loan Arrangement:** Generally the employee owns the policy with the company loaning funds to pay the premium and receiving a collateral assignment in the policy to secure repayment of the loan
- **Other Types of Benefit:** Defined benefit or defined contribution plans



Golden Handcuff Features

- **Vesting:** The executive's right to receive the benefit is subject to satisfaction of certain contingencies – generally based upon remaining employed:
 - For a certain number of years (cliff-vesting and graded), or
 - Until the occurrence of a specified event (e.g., change of control, death, disability, termination without cause)
- **Forfeiture:** Plans may provide that an executive's vested benefit is forfeited in the event of termination for cause or breach of a restrictive covenants agreement
- **Restrictive Covenants Agreement:** Plans may condition receipt of a benefit on the executive signing a restrictive covenant benefit
- **Retention Bonus Agreement:** A bonus structured to retain an executive until the company is sold or for a limited period of time following the sale



Payout Method and Timing

Flexibility in structuring how and when an award is paid out



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmblaw.com

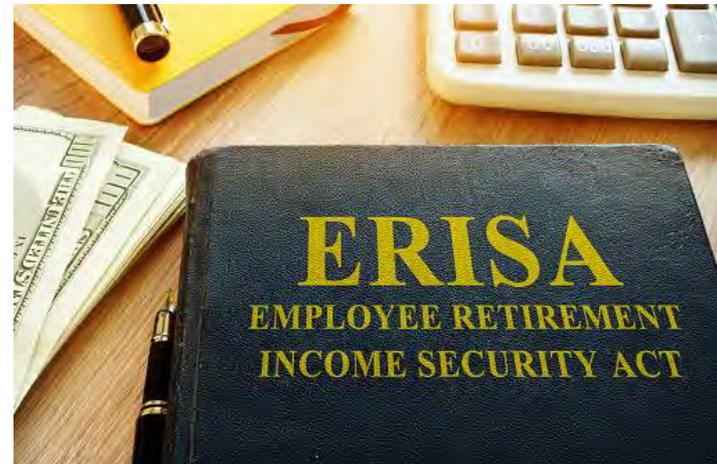
Funding

- Generally non-qualified deferred compensation is “unfunded” in that the executive is an unsecured creditor of the company
- There are limited exceptions – split-dollar life insurance benefits and Rabbi Trusts



ERISA

- **ERISA applies to deferred compensation plans that are designed to deferred income until an employee's termination of employment**
 - Generally, if an arrangement covers more than one employee and its benefits are designed to be paid after the termination of employment, then ERISA likely applies
- **ERISA has many parts and requirements:**
 - Funding
 - Non-discrimination
 - Vesting
 - Fiduciary duties
 - Reporting
 - Claims



ERISA, *continued.*

■ **Top Hat Exemption:**

- Unfunded plan that is designed to cover a select group of management or highly compensated employees
- Exempt from ERISA's funding, non-discrimination, vesting, and fiduciary requirements. Also, if a one-time filing is timely made with the DOL, the plan is exempt from ERISA's reporting requirements
- Top Hat plans are subject to ERISA's claims administration procedures



Internal Revenue Code 409A

- **Short-Term Deferral Exemption:** A deferred compensation arrangement is exempt from 409A if the benefit must be paid within 75 days after the end of the year in which the participant's right to the benefit is no longer subject to a "substantial risk of forfeiture."
- **409A requirements:**
 - Benefit may only be paid based upon specified trigger events
 - Limitations on accelerating the payout of benefits, amending plans and terminating plans





Restrictive Covenant Agreements and Employee Theft of Electronic Data

Presenter: Erin Nathan



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmbllaw.com

Are Restrictive Covenants Legal?



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmlaw.com

What is the Difference Between a Non-compete and a Non-solicitation?

Non-Compete: “*Super Confidentiality Agreement.*” The information the employee knows is so confidential that the employee should not be allowed to work for a competitor as to do so with give that future employer a competitive advantage

Non-Solicitation: Cannot contact either customers or employees



Non-Solicitation – Considerations

- Direct v. In-direct
- Current customers versus current and prospective customers
 - *What is a prospective customer?*
- Employees – how much contact with employees?



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmbllaw.com

Are Restrictive Covenants Enforceable?

In Iowa requirements:

- Reasonable in duration/time (typically 2 years or less)
- Reasonable in geographic scope
- Necessary to protect business interests
- Is the non-compete unreasonably restrictive on former employee
- Any public policy considerations



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmbllaw.com

Broad Non-Compete vs. Narrow Non-Compete

- Strategies
- Pros / Cons



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmbllaw.com

How Can A Company Protect its Intellectual Property / Data?



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmblaw.com

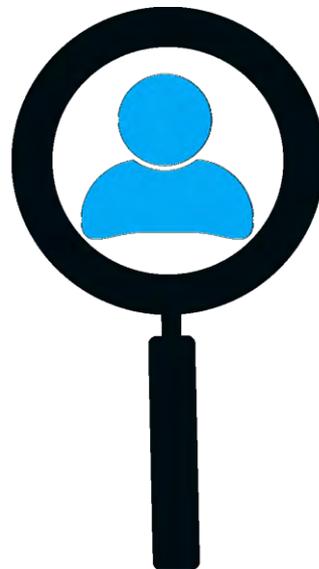
Employee Data Theft

- Employees may feel justified or entitled to take electronic work product in ways they never felt with hard copy material
- With email, external electronic devices and cloud-based storage options—stealing electronic data can be done with the click of a mouse



Employee Theft of Electronic Data

1. How to Prevent Employee Theft of Electronic Data
2. Red Flags to Watch for When Employees Leave
3. What to Do if You Suspect Employee Theft



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmblaw.com

Employee Data Theft -- Prevention

- A clear, strong policy emphasizing the proprietary character of company information and work product
- Institute and carry out Company culture of taking data security seriously

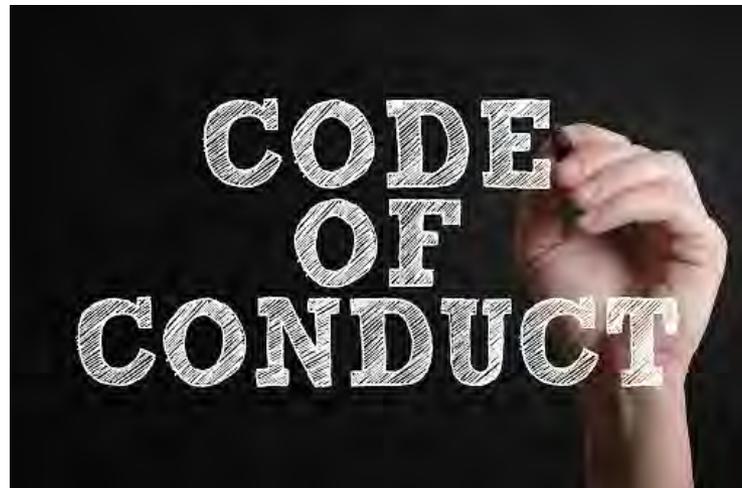


SIMMONS PERRINE MOYER BERGMAN PLC

www.spmblaw.com

Evaluate Your Company

- Does your Company have a sound Code of Conduct in place protecting your electronic proprietary data?
- Does your Company institute a culture of taking data security seriously?
- Do you institute restrictive covenant agreements?



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmbllaw.com

Instituting Sound Code of Conduct

- Electronic Security and Privacy Policy
 - 1) Detail Prohibited Conduct, such as:
 - ✓ Forwarding internal data to personal email accounts or non-employees
 - ✓ Connecting personal hard drives, thumb drives or other storage media devices to Company computers
 - ✓ Storing Company data, including email, on non-company computers or networks



Instituting Sound Code of Conduct, *continued.*

- 1) Detail Prohibited Conduct, such as:
 - ✓ Using another employee's login credentials
 - ✓ Installation or use of data wiping, encryption, "privacy" or other anti-forensic software, other than by IT as authorized by management

- 2) Explain that a violation of this policy will result in disciplinary action, up to termination

Instituting Sound Code of Conduct, *continued.*

3) Explain Employee Privacy Rights:

- ✓ Company has the **right to monitor** any and all aspects of its electronic communications systems
- ✓ Electronic transmissions sent or received through the Company's electronic communication systems are the **property of the Company**, and employees have **no right to privacy** in these transmissions



Instituting Sound Code of Conduct, *continued.*

- ✓ The Company retains the **right to review and monitor** any internal or external transmissions sent or received over its electronic communication systems, and may access, read, and **disclose to third parties** any such transmissions
- ✓ All employees of the Company **waive any right to privacy** in anything they create, store, send or receive via electronic communications including the Internet



Create A Departing Employee – Checklist

1. Did you create a hiring checklist?
 - Details devices, access points, passwords for that employee.
2. Request that employee sign an exit statement of compliance with electronic security and privacy policy – Dissuade taking data
3. Request employee to return all Company documents (electronic and hardcopy) and property. Catalog and cross-check the returned property. Ask employee to sign-off on the date issued and the date returned.



Departing Employee Checklist, *continued.*

3. Examples of Property Employee Must Return:

- ✓ Laptop and desktop machines
- ✓ Handheld devices and cell phones
- ✓ External hard drives
- ✓ Thumb drives and media cards
- ✓ Recordable optical media
- ✓ Secure access devices (key cards, security token generators)



Departing Employee Checklist, *continued.*

4. Don't allow the employee the time to change, wipe or disable phones, computers and storage media
5. Ask for passwords to any device, file or account used to store Company data

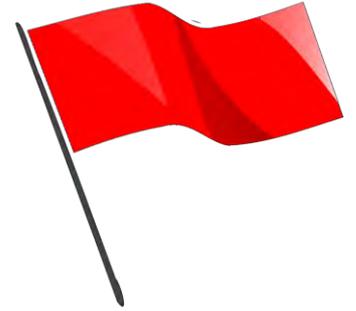


Departing Employee Checklist, *continued.*

6. Immediately suspend the former employee's access to your Company's computer system
7. Do not allow departing employee to purchase his/her computer or other devices



Red Flag Alert



- You suspect your former employee has taken Company information ---

NOW WHAT???

- Preserve the Metadata on all devices (computer, phone)
- Consider hiring third-party to investigate the suspected theft (forensic accountants, lawyers)
- Extreme cases: consider criminal prosecution



Departing Employee Checklist, *continued.*

Consider:

8. Suspending any automatic deletion or purge settings of the departing Employee's email until an evaluation is made concerning theft

9. Preserving the full contents of the departing Employee's Company email account



Departing Employee Checklist, *continued.*

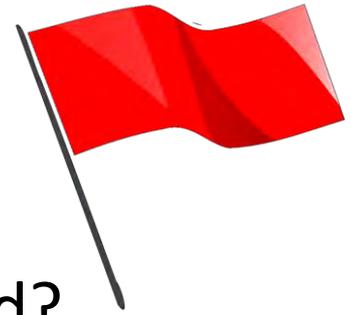
Consider:

10. Backing up the departing Employee's computer hard drive, other electronic devices or network storage locations

11. Not re-using the departing Employee's computer hard drive



Employee Data Theft: *Red Flags*



- Has the hard drive recently been replaced?
- Is the machine functional?
- Is the recycle bin empty?
- Is the user's login identity visible?
- Does the machine hold documents and email of the volume expected by the user?



Employee Data Theft: *Red Flags*



- Is the user's local or network email gone?
- What programs were recently installed? Any wiping software?
- Does the machine contain a recently created folder holding proprietary information?
- Has the user lately sent email and attachments to the user's personal email?



Causes of Action for Employee Theft

■ Contractually-Based

- Breach of Confidentiality Agreement
- Breach of Non-Compete or Non-Solicitation Agreement
- *Handbooks do NOT create contractual rights, nor do you want them to do so*

■ Statutorily-Based

- Breach of Iowa Trade Secrets Act
- Breach of Computer Fraud and Abuse Act
- Federal criminal prosecution under Economic Espionage Act

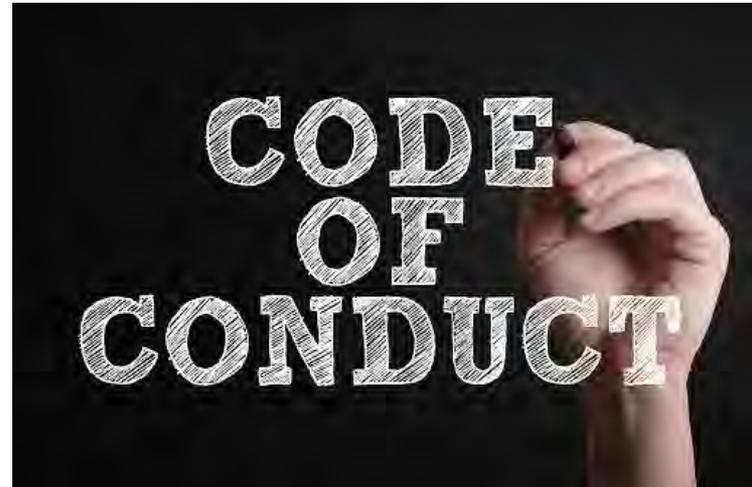
■ Common Law-Based

- Breach of Fiduciary Duties (Loyalty and Care)



Codes of Conduct for All Employees

- Confidentiality
- Return of Company Property
- Employee Privacy
- Computer / Device Use
- Social Media
- Internet Usage
- Conflicts of Interest



Codes of Conduct

▪ Confidentiality

- Employee acknowledgement of employee's access to confidential information
- In addition to “catch-all”, specify specific information that the Company considers to be confidential
- Return of Confidential information “whether acquired and/or developed by the employee”

▪ Company Property

- Employees are responsible for safekeeping of company property
- At end of employment must return ALL property, including digital



Codes of Conduct

- **Employee Privacy**

- Advise employees they can have no expectation of privacy when using the Company e-mail or accessing the Internet using Company resources or on Company time, or when using Company equipment / property

- **Computer / Device Equipment Use**

- Consider a stand-alone agreement that issues a certain device to certain employee with responsibility for security of device and outlines privacy expectations and permitted uses of equipment.



Agreements For Certain Individuals

- **Non-Disclosure Agreements**
 - Independent Contractors
 - Prospective Customers
 - Potential Business Partners
 - Potential Investors



Agreements For Certain Employees

▪ Intellectual Property Agreements

- Ownership of “Works” created by Employee
- Consider “Works” created after employment ends, created during off-hours, whether subject matter dependent

Are patent applications critical?

Magic Present Tense Language: I agree to assign, transfer and set over, and I do hereby assign, transfer and set over to the applicable Owners, all my rights, title and interest in and to any and all Intellectual Property. This is an agreement to assign, and a present assignment that effects the transfer when the invention is made .



Agreements For Certain Employees

- **Trade Secret Agreements**

- Specifically List the Trade Secrets, the more specific the better

- **Non-Compete and Non-Solicitation**

- Is the information such that the employee will inherently take that knowledge with them to their next employer?
- This will ensure that the information is “stale” by the time the individual goes to work for your Company’s competitor



Defense of Trade Secrets Act of 2016

- Allows Federal Court Jurisdiction if the following insert is in the Agreement for misappropriation of trade secrets on or after May 11, 2016 and in extremely limited circumstances allows for an ex parte seizure order:

Pursuant to the Defend Trade Secrets Act of 2016, I understand that:

An individual may not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that: (a) is made (i) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (b) is made in a complaint or other document that is filed under seal in a lawsuit or other proceeding.



Please Contact our Presenters with Questions:



Thomas N. DeBoom

(319) 896-4091

tdeboom@spmbllaw.com



Erin R. Nathan

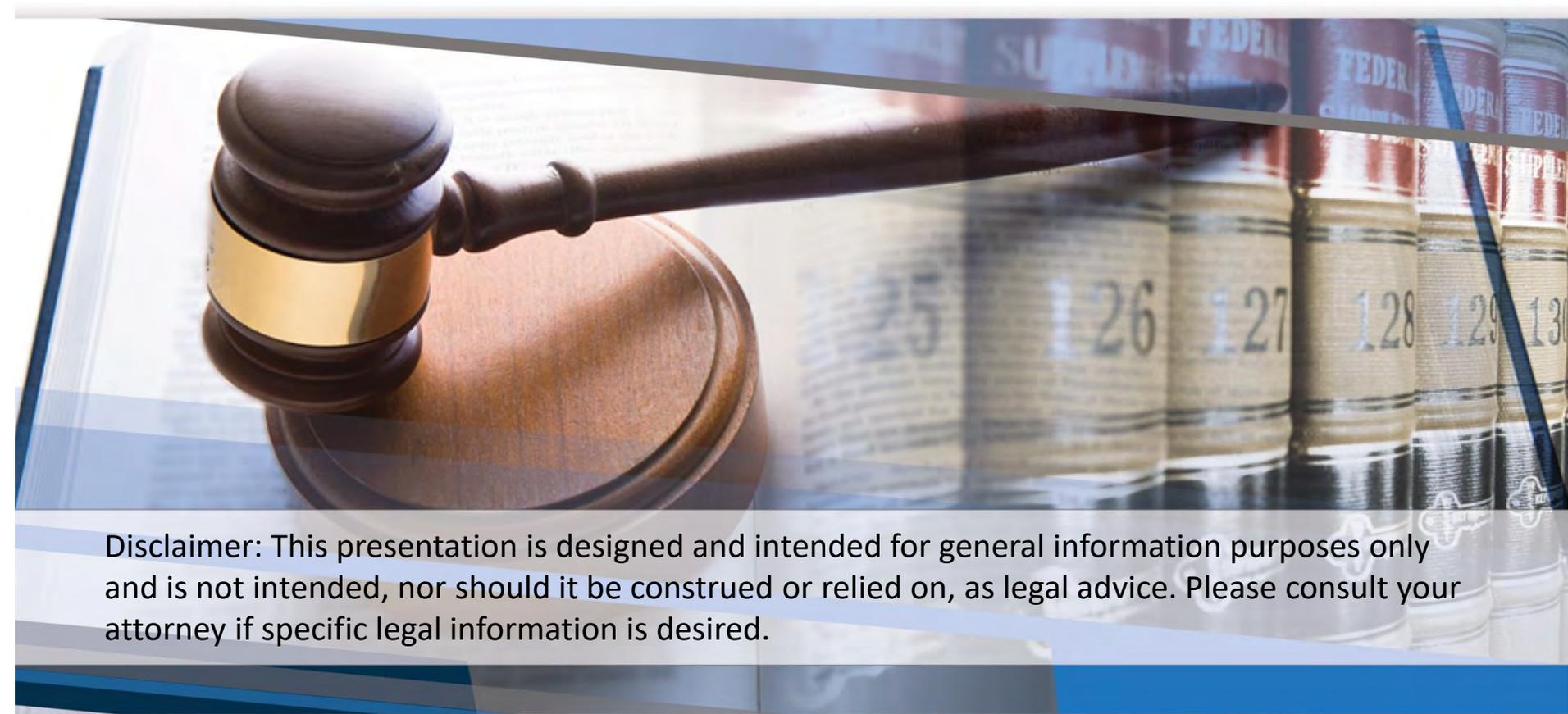
(319) 896-4013

enathan@spmbllaw.com



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmbllaw.com



Disclaimer: This presentation is designed and intended for general information purposes only and is not intended, nor should it be construed or relied on, as legal advice. Please consult your attorney if specific legal information is desired.



SIMMONS PERRINE MOYER BERGMAN PLC

www.spmbllaw.com

115 3rd Street SE, Suite 1200 | Cedar Rapids, IA 52401 | 319.366.7641

1150 5th Street, Suite 170 | Coralville, IA 52241 | 319.354.1019