STRATEGIC USE OF FORENSIC EXPERTS IN DEFENDING NON-COMPETE, TRADE SECRET AND BUSINESS TORT CLAIMS

presented by

MODERATOR:
Christina H. Bost Seaton, Esquire

SPEAKERS:
Sonya Richburg, Esquire
Cynthia N. Sass, Esquire
Adam Sharp, President of E-Hounds, Inc.

Section of Labor and Employment Law
American Bar Association
Employment Rights and Responsibilities Committee
Covenants Not to Compete Subcommittee
and Technology Subcommittee
Midwinter Meeting
Clearwater Beach, Florida
March 24, 2018

Available Courtesy of:
SASS LAW FIRM
601 West Dr. Martin Luther King Jr. Boulevard
Tampa, Florida 33603
813.251.5599
www.EmploymentLawTampa.com

EMPLOYEE PERSPECTIVE ON STRATEGIC USE OF FORENSIC EXPERTS IN DEFENDING NON-COMPETE, TRADE SECRET AND BUSINESS TORT CLAIMS[1]

Cynthia N. Sass, Esquire[2]
SASS LAW FIRM
601 West Dr. Martin Luther King Jr. Boulevard
Tampa, Florida 33603
813.251.5599
www.EmploymentLawTampa.com

I. RECOGNIZE THE DIFFERENT TYPES AND USES FOR A COMPUTER FORENSIC EXPERTS

A. THE COURTROOM EXPERT

1. **For Motions**:

- Motion to Compel Inspection. To testify or provide affidavits as to the burden(s) of accessing information or need for certain format or discovery requests and relevance of same or significance of certain electronic information and basis for inspection.

- Motions for Spoliation of Evidence. To testify as to metadata data of documents, alterations to electronic files and/or deletion and whether any deleted information is recoverable.

2. **In Trial**:

- To lay the foundation to admit certain electronic data

- To explain the timing of the creation of data

- To identify the location of electronic data and storage of same

- To explain the manner in which such electronic data was accessed and when

- To explain whether electronic data was copied and/or transferred to third parties or non-company devices – such as thumb drive- and when this occurred

---

[1] These materials are distributed by the Sass Law Firm for informational purposes only. These materials should not be considered legal advice and should not be used as such.

[2] Thank you to Yvette D. Everhart, Esquire, B.C.S., and law clerk Marielly Abzun of the Sass Law Firm, for their assistance in preparing these materials.

- To identify which electronic data was taken and the security measures taken to keep information confidential

- To explain information contained in equipment such as smart phones – photographs (timing of when photographs taken and location of photographs), location of phone (may show address or GPS location of where employee was at certain times),

- To explain authenticity of emails, texts and other electronic data with regard to tracking software

- To explain whether certain data was destroyed – i.e. use of wiping software on laptops – when such occurred

3. **Practice Point**: If you use your trial expert in the capacity of a consulting expert as well, you run the risk that the employer bringing the claims will move to discover all communications you had with the trial expert in preparation or defense of your case as generally, all information or communications trial expert is privy to, is discoverable by opposing counsel. To avoid this from occurring, do not have expert also be investigator of data.

B. **CONSULTING EXPERT**:

1. **Use of a Consulting Expert**:

a. Pre-suit and during litigation

- Assist with return of electronic information, deletion and preservation and storage of mirror image data before deletion

- Assist in preservation of electronic data:
  - In the cloud
  - On smartphones
  - On laptops
  - On tablets and iPads
  - With social media
  - On servers

- Assist with understanding the information contained in the electronic data – time of creation, whether it has been copied and when, and information contained on smart phones

- Assist with preparation for case management conference, including:
  - The format you want to request data to be produced

- Developing search terms
- Identifying where data is kept

- Assist with preparation of discovery requests

- Analysis of electronic data provided in response to discovery requests

- Communicate with company IT person to assist with discovery of relevant information

- Prepare for deposition questions regarding electronic data

- Conduct forensic investigation of equipment of opposing party

2. **Practice Point**: Advise your client upfront that the hiring of this consulting expert is an essential cost for him or her if litigation is anticipated or if there is a dispute about the return of property.

C. **NEUTRAL EXPERT**:

1. **Hired by Both Parties**:

- To preserve electronic data and assist in returning/removing data, if necessary

- To conduct forensic investigation based on what each party expressly states they are looking for in the investigative process

2. **Practice Point**: This option can be a win/win, in certain circumstances, as it reduces costs by splitting it among parties.

II. PRE-SUIT PROCEDURES AND COMPUTER PROTOCOLS FOR THE EMPLOYEE ADVOCATE

A. AT INITIAL CONSULT WITH EMPLOYEE:

1. **Policies**. Review all agreements and policies with employee as to his/her obligations as to non-competes, trade secrets and confidentiality agreements contained in documents, including:

- Separation Agreements
- Stock Agreements
- Bonus Agreements
- Ownership Agreements
- Non-Disclosure Agreements

- Arbitration Agreements
- Handbook policies:
  - Electronic data policies
  - Confidentiality policies
  - Exit policies
- Non-Compete/ Non-Solicitation agreements
- Initial hire letters
- Employment Agreements

2. **Equipment and Access**. Ascertain whether employee still has employer equipment and access to employer data:

   - Email access, server/remote access, cloud storage
   - Laptop, iPad, smart phone, thumb-drives, external hard drives

3. **Preservation**. If employee still has equipment and access and has not taken anything, then advise the employee not to take/copy or delete any data.

4. **Practice Point**: If there are documents/files that may be relevant to any future litigation, advise the employee to make a running index or list of any such documents or data to keep instead of the confidential documents themselves. If employee is still employed, then all the electronic data and documents can be sent to in-house counsel with index and request preservation of same.

B. **RECOVERY OF TRANSFERRED DATA TO THIRD PARTIES AFTER AN EMPLOYEE LEAVES**

1. **Return of Documents**. Does any agreement require the employee to return documents?

   - Need to determine what should be returned:

     - Are documents confidential or available for employee's reuse?
     - What is the electronic data policy?
     - Who owns the equipment, software, cloud services?

   - Ethical Considerations:

     - Can employee counsel review data if confidential/trade secret?
       - Check state bar professional rules of conduct.
       - *Defend Trade Secrets Act of 2016* also provides immunity protections to employees who disclose trade secrets to the government and/or their attorney to report suspected violations of law or in retaliation lawsuits. See 18 U.S.C. §1833(b).

2. **Common Issues**. When electronic data needs to be returned and company information is commingled with employee's personal data or personal equipment:

- Without Expert. Try to work with company to return data/equipment without an expert to allow employee to delete data that is confidential and/or proprietary company property or information. If he or she is permitted to remove it, then have the employee sign affidavit that:
  - He or she has not disclosed to any third parties
  - That the information has been deleted
  - Affirming that the employee has not retained any copies

- With Expert. If the company is not willing to let the employee handle without a computer expert:

  i. *Neutral Expert*. Retain a neutral expert to assist with return or deletion of documents and ask the company to pay associated costs, then:

  - Agree on a protocol for the imaging and searching of the employee's data

  - Come to an agreement that only the expert will have access to the data, where applicable and will not share without express permission in writing

  - Come to an agreement that the search will be narrowed to certain time frames and what is not subject to review – FOR EXAMPLE: Data that pre-dates your client's employment may not be relevant and should not be considered

  - Also try to agree to a procedure for going to the court if any issues between the parties cannot be resolved and who pays for expert

  ii. *Sample Protocol*:

  - The expert will make a mirror image of the data for searching/inspecting

  - Have employer provide search terms for expert to use in identifying potential company documents

    - If there is any objection to certain search terms, the parties should confer to see if any objection can be resolved

    - You can also ask the expert for any suggestions for search terms because certain words may return more irrelevant data than what is being sought

- Based on the search terms, the expert will run the search on the devices, and will produce a report of the files contained on the devices to producing party, and producing party will log any objection to specific items and those objection are subject to court protocol if the parties cannot work it out

- The expert can also provide a report of any data that has been transferred, copied or removed from the device if applicable

- Once both sides have the list of files (absent items that are subject to objections), both parties should identify what it deems to be company versus personal information

- Any doubts or questions about certain files can likely be resolved simply by the expert reviewing and identifying what is contained in the actual document

- After narrowing and/or identifying company v. employee private data, from there the expert can remove company data from the employee's devices and sign affidavit that the expert deleted the items

iii. *Separate Experts.* If the company does not want to use a mutual expert, then each party should retain its own expert. However, this typically tends to be the more time intensive and costly option.

  - When litigation is ongoing but data needs to be returned and deleted, get the expert to certify that he or she:

    - Deleted information from the employee's systems

    - Has retained a mirror image of the data

    - Will retain the unaltered mirror image for the duration of the litigation

  - Employee's transfer of data to third parties

    - Obtain affidavits from third parties affirming that they have not used or transferred to anyone else the data provided to them by the employee and affirming that they deleted data the provided to them

    - Obtain consent from the third party for a forensic expert to review the third party's equipment to confirm that the transferred data was deleted

    - Obtain consent from the third party for a forensic review of the third-party's equipment to search for what data was taken or transferred to the third party

- The expert should certify that the transferred data was deleted from the third-party's equipment/systems

- In addition, if litigation is anticipated, make sure the expert saves and retains a copy of the data transferred to the third-party data

Practice Point: Keep in mind that inspecting third-party equipment may get expensive and the third party may not consent to a voluntary search based on privacy and its own confidentiality concerns absent a court order.

C. **RETRIEVING AN EMPLOYEE'S ELECTRONIC DATA FROM COMPANY EQUIPMENT, SOFTWARE OR CLOUD BASED STORAGE**

1. Where possible ask your client to create an index of what personal data/files are maintained on the Company equipment, software, or cloud based services.

2. Contact the company regarding the employee's personal data and request the company to return and remove the employee's personal information.

   - Get an agreement from the company that it will not review, use or disclose to anyone the employee's personal data

   - Suggest the use of a forensic expert to create mirror images of the device(s) and label personal information for employee's removal

3. Where the employer does not want to return or delete the employee's personal information, considering bringing a claim against the employer for replevin.

   - Replevin is a procedure where a party requests from a court authorization to re-take personal property that is wrongfully taken. *Burriola v. Nevada*, No. 3:10-cv-00168-LRH (WGC), 2012 WL 2789648, at *1 (D. NV March 27, 2012); *Land–Cellular Corp. v. Zokaites*, 463 F.Supp.2d 1348, 1353 (S.D.Fla.2006) (replevin lies for any wrongful taking or wrongful detention of any specific personal property").

     - Employee could file a writ of replevin with the court, seeking return of documents, devices, or other taken items

     - Expedites return of personal property since it does not require a final adjudication

     - Have your computer expert go with law enforcement and take information off the company computer and permanently delete it from the system

4. Make sure employer did not improperly access employee's property and consider invasion of privacy or statutory claims outlined in Section V.

D. STEPS TO TAKE WHEN ANTICIPATING LITIGATION OR THREATENED LITIGATION FOR RESTRICTIVE COVENANT, TRADE SECRET VIOLATIONS OR THEFT OF CONFIDENTIAL INFORMATION OR OTHER BUSINESS TORTS

1. As an employee advocate:

- Review all the agreements listed in Section II(A)(1) above.
- Request any agreements and policies at issue from opposing counsel.
- Ask your client to identify all electronic equipment, electronic data and storage that may be related to the claims at issue. For example:
  - Emails forwarding company information to themselves
  - Thumb drives or external drives used to store or backup company information
  - Emails, texts, Snapchat, or any other means of communication as to the employee's job search efforts
  - Emails, texts, Snapchat, social media (Facebook® or LinkedIn®) or any other means of communication as to conduct that may violate non-competition or non-solicitation agreements
  - Any electronic communication with others transmitting company information
- Provide the employee with a preservation letter and have several conversations with employee regarding his/her obligations. *See William Coale v. Metro-North Railroad Company*, No. 3:08-CV-01307 (CSH), 2016 WL 1441790, at *2 (D. Conn. Apr. 11, 2016) citing *Kronisch v. U.S.*, 150 F.3d 112, 126 (2d Cir. 1998) (An "obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation," including "when a party should have known that the evidence may be relevant to future litigation."); *McBride v. Coca-Cola Refreshments, USA, Inc.*, No. 8:12–cv–275–T–AEP, 2012 WL 12915435 (M.D. Fla. 2012) (the duty to preserve arises when litigation is pending or when a party reasonably anticipates litigation)
- Ensure that all relevant data is preserved
  - Retain an expert to preserve information upfront from cell phones, computer, social media, cloud based storage, external drives and thumb drives

- Have expert retain mirror image to avoid chain of custody issues

- At this stage, the upfront costs will be minimal

2. Send preservation letter to opposing counsel and specify what needs to be preserved by identifying:

- Time frame
- Users and custodians
- Equipment, workstations, group shares, servers and peripheral devices
- Programs, such as email, instant messaging, document management system, etcetera
- Voice message systems
- Cloud storage
- Specific items known to exist, like texts, social media postings or videos
- Request discontinuation of back up tape rotation and records destruction or auto-delete policies
- Third-party providers who may have access to the information

III. FORENSIC EXPERT FOR LITIGATION PURPOSES

A. USE EXPERTS IN CASE MANAGEMENT AND DEVELOPING ESI PROTOCOL

1. **Case Management**:

- Have forensic expert attend the case management meeting to understand how opposing party stores information and to understand what is needed for the case.

- Should consider need for forensic expert and set up procedures that experts of both parties should follow:

- Provide definitions for terms found in protocol

- Use of search terms to help eliminate irrelevant ESI. *See Progressive Cas. Ins. Co. v. Delany*, No. 2:11-cv-00678-LRH-PAL, 2014 WL 3563467, at *2 (D. NV. July 8, 2014) (showing how the use of search terms cut down the documents from 1.8 million to 565,000)

- Whether to propose or oppose predictive coding and coming up with search terms and connectors for predictive coding. *See F.D.I.C. v. Bowen*, 2014 W.L. 2548137 (S.D. Fla. 2014) (suggesting that the parties use predictive coding production of ESI); *Dynamo Holdings Ltd. Partnership v. C.I.R.*, 143 T.C. 183, 184–86 (2014) (opposing a party's request to use predictive coding because its

considered "unproven technology" but it is a method to "efficiently and economically help identify the nonprivileged information that is responsive to respondent's discovery")

- Forensic expert could help determine in what format(s) ESI should be produced as well as any necessary applications that may be needed to view the data in its native format.

b. **ESI Protocol**

- Parties can submit joint proposal or separate competing proposals to court as to ESI protocol.

- The purpose is to outline the scope of investigation for the expert to follow.

- It lists what one or both parties have agreed will be inspected.

    - Could be a whole computer, phone or tablet, or portions of a device, cloud based storage, etcetera

- In *William v. Acxiom Corp.*, the court ordered the parties' counsel to "meet and confer over the next 21 days and satisfy their obligations to develop ESI protocol." No. 2:15-CV-08464-ES-SCM, 2017 WL 945017 at *5 (D. N.J. Mar. 10, 2017).

- It should include timeframes to focus investigation, specific keywords or verbiage to search in documents, emails, or software, specify the information of specific employees/managers which will be investigated, and what information will be detailed in the expert's written report of the inspection of device(s).

- Propose terms that will provide maximum control over the investigative process and minimize control of opposing party.

- As more information is gathered, scope of expert may be modified, with the parties' or court's approval.

- ESI protocol should be "appropriate, reasonable and consistent with principles of proportionality when dealing with ESI." *F.D.I.C. v. Brundnicki*, 291 F.D.R. 669, 675 (N.D. Fla. 2013). Expert can help with proportionality argument show costs, access and time needed to complete discovery.

- Help identify where relevant information is stored.

- Help identify search terms that will be productive.

- Discuss with IT person discovery protocol.

- Identify proper format for production of data.

c. **Discovery – Use of Expert**

a. Assist in identifying and formulating production requests for data available depending on software used by company.

b. Include definitions, instruction and specific questions on electronic discovery.

- May want to target a specific hard drive

c. To know what ambient documents should be requested.

- Active v. Ambient data

  - Active: tangible documents
  - Ambient: hidden data not usually accessible to user

d. Prepare discovery to include original media.

e. Assist in specifying the format for production of discovery.

f. Assist in gathering information necessary for motions to compel and motion for forensic review and/or motions for spoliation.

g. Assist in identifying information about data such as:

- Number of times an account is accessed from a device

- Original media of a document to know when created and or altered

- Number of individuals who read employee's email

- Whether trade secrets or confidential documents copied or distributed to others

- Supervisor emails that included employee's name

h. Assist in Rule 30(b)(6) deposition preparation for testimony to establish proportioning arguments, cost, access, protocol of company, and location of data.

i. Assist in deposition questions for fact witnesses as to potential deletion, data transfer, as applicable.

B. **COMPELLING FORENSICS**

1. Computer-generated data is discoverable. Fed. R. Civ. P. 34.

2. Compelling forensic examination when opposing party in possession of a device is allowed. Fed. R. Civ. P. 37.

3. *Crabtree v. Angie's List, Inc.*, No. 1:16-cv-00877-SEB-MJD, 2017 WL 413242 (S.D. Ind. Jan. 31, 2017). The Advisory committee notes of the Federal rules recommend courts be cautions when determining if a forensic examination of electronic devices is necessary, as it could gravely interfere with a party's privacy. *Id.* at *3.

4. Motions to compel forensic examination:

   a. Under Rule 37(a) it can be filed when party does not respond to discovery request or response is incomplete. *Daniels v. Spencer Gifts*, LLC, No. 10 C 5345, 2012 WL 488099, at *3 (N.D. Ill. Feb. 4, 2012).

   b. Scope of forensic inspection should be focused on the topics or issues of litigation. *See U.S. v. Kellogg Brown & Root Services, Inc*., 284 F.D.R. 22, 37 (D.C. 2012) (stating that discovery should not be a fishing expedition but should be constructed to the issues of the case).

      - Overly intrusive searches, generally denied. *See In re Ohio Execution Protocol Litigation*, 845 F/ 3d 231, 236 (6th Cir. 2016) (stating that discovery should be proportional to the needs of the case).

   c. Proportionality:

      - Rule 26(b)(2)(C) requires that discovery "must be measured against the yardstick of proportionality." *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.D.R. 497, 523 (D. Md. 2010).

      - Requires a balance between the benefits of obtaining the information against the burden and costs of procuring said information. *Id.* (stating that a party can choose to deny a discovery request if its burdens and costs are excessive). The parties and the court have a duty to consider and discuss proportionality of discovery, when there is a discovery problem. *Samsung Electronics America Inc. v. Yang Kun "Michael" Chung*, — F.D.R. —, *14 (N.D. TX. Mar. 7, 2017).

      - *Health Management Ass., Inc. v. Salyer*, Case No. 14-14337-CIV-ROSENBURG/LYNCH, 2015 WL 12778793, at *1–2 (S.D. Fla. Aug. 19, 2015). The court balanced the uncooperative nature of the defendant, when he failed to disclose ESI, against the privacy concerns when evaluating a motion to compel a forensic exam of the defendant's yahoo account. *Id.* at *2. The court

granted the motion to compel the forensic examination of defendant's email account on all his devices, but allowed the defendant to be present and to participate. *Id.*

d. Use of expert to support motion for forensic examination:

- To show cost
- To show exam is not intrusive
- To propose protocol that is non-intrusive and effective
- To show how the forensic examination would be performed
- To show why forensic exam is necessary based on ESI discovery already produced. *See White v. Graceland College Center for Professional Development & Lifelong Learning, Inc.*, 2009 WL 722056 (using computer expert to support motion to compel production of native electronic data where there was a discrepancy as to date of creation of electronic data).

5. Plaintiff requested a forensic image of opposing party's electronic devices, without concern for irrelevant, confidential, and private documents. The court found this request overly broad and denied the motion to compel the forensic exam. *Brand Services, LLC v. Irex Corp.*, No: 15-5712, 2017 WL 67517 at *2–3 (E.D. La. Jan. 6, 2017). Further, parties need to establish a ESI protocol, which discusses keyword searches, privacy concerns, and ensuring parties do not stray from relevant information to the case. *Id.* at *3.

6. When compelling examination, party must show/proffer reliable information that opposing party is unwilling to produce or withheld computer-generated documents now or in the future.

- *U & I Corp. v. Advanced Medical Design, Inc.*, 251 F.R.D. 667, 675 (M.D. Fla. 2008). The court granted forensic examination of defendant's computer during a specified time due to defendant's continually delayed production of documents, neglect to inform plaintiff of failure with hard drives, and could not recover emails that had been requested during discovery. *Id.* at 675 (wait to disclose these issues until the motion to compel was filed).
- *Wynmoor Community Council, Inc. v. QBE Ins. Corp.*, 280 F.R.D. 681 (S.D. Fla. 2012). If a party requesting a forensic examination presents good cause and responding party presents an undue burden, the court must weigh the burden against the need for the case to determine if the forensic exam should be granted. *Id.* at 685.

7. Information presented to court must be reliable and not solely speculative or conjecture

   - *Brown Jordan Int'l, Inc. v. Carmicle*, Case No.3:15-MC-000270GNS, 2015 WL 6142885 (S.D. Fla. Oct. 19, 2015). The plaintiff's presented forensic evidence, which demonstrated a third party's iPhone held documents or ESI that was relevant to the case. *Id.* at *3. Plaintiffs also used defendant's deposition where it was possible he had used the third party's phone for work. *Id.* The court determined that the plaintiff presented sufficient evidence to compel a forensic examination of the third party's iPhone. *Id.* at *4.

   - *Lawrence v. Rocktenn CP LLC*, Case No. 16-821, 2017 WL 2951624 (Mag. W.D. La. April 19, 2017). Defendant requested texts, emails, and photographs in plaintiff's possession around the time of plaintiff's accident and that discuss the accident. *Id.* at *1. Plaintiff objects to request as being overly broad and views request as an invasion of privacy. *Id.* The court granted defendant's motion to compel, finding these items relevant. *Id.* Defendant also requested messages on dating sites post-accident since plaintiff claimed mental anguish of marriage disintegrating. *Id.* at *2. Plaintiff objected as overly broad and invasion of privacy. The court granted defendant's motion to compel, finding relevance in request. *Id.*

   - *Bradfield v. Mid-Continent Cas. Co.*, Case No. 5:13-cv-222-Oc-10PRL, 2014 WL 4626864, at *3–4 (M.D. Fla. Sept. 15, 2014) (failing to provide good showing to compel a forensic exam). Defendant failed to provide good showing to the court when argued in favor of compelling a forensic exam of plaintiff's devices to search, when defendant could not state what might be found on Plaintiff's devices or how it would be used in this litigation. *Id.* at *2. Further, the plaintiffs presented sufficient evidence that the forensic exam created an excessive burden and costs. *Id.* (citing cases which state that ESI is not considered reasonably accessible when an outside expert is required).

C. **FORENSIC EXAMINATION**

1. Create mirror image of device (computer hard drive, cell phones, tablets, etcetera) and ensure integrity and chain of custody.

2. Experts review information according to parameters of ESI protocol.

   a. May be able to recover deleted information (deleted emails or documents) or break passwords, if allowable.

   b. Trace device usage (patterns of computer usage, edits/modifications of documents, time/date stamps, GPS location of specified time, etcetera).

c. Once data is recovered, its converted to a usable format for litigation purposes.

D. **FAILURE TO PRESERVE OR DISCLOSE ESI**

1. **Use of Expert to Support Motion for Sanctions**

- *Jones v. BAE Sys., Inc.*, 106 F. Supp. 3d 179 (D.C. 2015) (using a computer expert to support motion for sanctions, where expert was used to determine whether emails deleted by the opposing party were recoverable)

2. **Possible Sanctions**. Court-ordered sanctions vary from monetary fines to adverse inference instructions and dismissal of defenses/counterclaims.

- *Shawe v. Etling*, 157 A. 3d 142 (Del. Feb. 13, 2017). Plaintiff's sanctions were affirmed after intentionally and carelessly deleting emails, text messages and other ESI. Plaintiff hired a computer forensic expert to investigate defendant's computer in secret. Plaintiff also committed perjury a multitude of times when discussing ESI problems. Plaintiff's sanctions included 100% of defendant's fees for bringing the motion for sanctions and 33% percent of overall fees of litigation. Fees and costs to be paid by plaintiff totaled $7.1 million.

- *Walker v. Carter et al*, Case No. 12-05384-ALC-RLE, 2017 WL 3668585 (S.D.N.Y. July 12, 2017). Court affirmed monetary sanctions placed on plaintiffs for failing to disclose relevant text messages, over an extended period in breach of contract and copyright suit. The sanction included attorney's fees for the motion for sanctions.

- *First Financial Security Inc. v. Lee et al*, Case No. 14-CV-1843 (PJS/SER), 2016 WL 881003 (D. Min. March 8, 2016). Defendants had been compelled by court to present plaintiffs with texts and emails around or after May 10, 2014, but failed to do so. Some texts and emails either lost or deleted. *Id.* at *1–2. Defendant was sanctioned by the court with adverse inference instructions since the defendant did not comply with court ordered discovery and attorney's fees and costs for the plaintiff's motion for sanction proceedings. *Id.* at *7–8.

IV. <u>TRIAL</u>

A. The focus at this stage of litigation is the presentation of evidence gathered.

1. Is evidence authentic and admissible?

2. What is the difficulty of presenting evidence to the jurors?

B. Evidence obtained from forensic examination may be difficult to present to jurors:

1. Ambient data, like computer code, appears as jibberish and needs a translator.

    - Example: Patterns of computer usage or how often a specific program is used by an employee, like when text messages are reproduced in an Excel format and includes ambient data.

2. Active data may also be in a format difficult to understand

3. Trial experts can help explain ESI or forensic analysis to jurors.

C. Ensure the ESI is allowed as evidence under the applicable state or federal rules of evidence.

D. Two important evidence rules to keep in mind:

1. F.R.E. 702: Expert testimony:

    a. If trial expert is used, will need to be qualified and credible.

    b. Qualifications can be through "knowledge, skill, experience, training, or education"

    c. Trial forensic expert helps explain what the forensic investigation found, especially with intangible findings (limit knowledge to avoid unfavorable discoverability from opposing party)

    d. Courts will analyze whether a computer forensic expert can testify at trial by determining if the expert is qualified and whether the expert's opinion is reliable under the *Daubert* standard. *Marten Transport, Ltd. v. Platform Advertising, Inc.*, 184 F.Supp.3d 1006 (D. KS. 2016). Under the *Daubert* standard, there are three areas of inquiry: qualifications, relevance, and reliability. *Furmanite America, Inc. v. T.D. Williamson, Inc.*, 506 F. Supp. 2d 1126, 1129 (M.D. Fla. 2007).

    e. The most litigated issue for expert testimony is reliability. *Id*. at 1129. *Daubert* lists several factors the court would be appropriate to consider:

> (1) whether the methodology has been, or is amenable to, testing; (2) whether it has been subjected to peer review and/or publication; (3) the known and potential error rate of the methodology; and (4) whether it has been generally accepted in the relevant [] community."

Id. at 1130 (this is a non-exclusive list of factors that Daubert states). *See also U.S. v. Springstead*, 520 Fed. Appx. 168, 170 (4th Cir. 2013) (finding a computer forensic expert qualified even though the district court did not use all reliability factors in *Daubert* because "the test of reliability is flexible and Daubert's list of

specific factors neither necessarily nor exclusively applies to all experts or in every case.").

2. F.R.E. 902: Self-authenticating evidence:

   a. Section (14) amended in 2016.

      - Electronic data that is recovered by digital identification is self-authenticating and will not need expert testimony to introduce it at trial

      - Will need a written certification by a qualified person

V. COMPUTER CRIME STATUTES THAT COULD BE POTENTIALLY APPLICABLE WHEN LITIGATING NON-COMPETE CLAIMS, TRADE SECRET AND BUSINESS TORTS.

A. The employee advocate should be aware of the various computer statutes, some of which have both civil and criminal penalties for violating.

B. An expert may be useful to determine if the former employer in any way violated these statutes giving rise to counterclaims.

   - You will need an expert to opine as to potential violations.

C. The employee advocate should ensure that he or she or his or her client does not violate these statutes when dealing with electronic data.

D. THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030 ("CFAA")

1. **General Law**.

   - The CFAA prohibits unauthorized access of a computer or exceeding authorized access of a computer, when done to obtain information or damage computer functionality. Thus, a CFAA violation occurs if a defendant either (1) damages a computer system or (2) obtains information to which he or she is not entitled.

   - The CFAA is primarily a criminal statute with criminal penalties, including fines and imprisonment for up to 10 years. 18 U.S.C. §1030(c); *Trademotion, LLC v. Marketcliq, Inc.*, 857 F. Supp. 2d, 1287, 1290 (M.D. Fla. 2012). However, the CFAA also "provides a private right of action to '[a]ny person who suffers damage or loss by reason of a violation of this section' who 'may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.'" *Trademotion*, 857 F. Supp. 2d at 1290 (quoting 18 U.S.C. §1030(g)). In a civil action under the CFAA, the plaintiff must demonstrate actual

damages or loss resulting from the violation of the CFAA. *Brooks v. AM Resorts, LLC*, 954 F. Supp. 2d 331, 337 (E.D. Pa. 2013).

- It can also apply when employers attempt to access an employee's devices and steal information of the employee. *See*, *e.g.*, *Brooks*, 954 F. Supp. 2d at 332-333 (former employee sued former employer for allegedly gained unauthorized access to his computer and e-mail account in violation of the CFAA). The statute focuses on whether the access of the computer was without authorization or exceeded any authorization that was granted. As discussed below, there is disagreement among the circuits as to when an employee acts with the requisite authorization.

2. **Narrow Construction**. Although there is no consensus, most jurisdictions have adopted a narrow construction of the CFAA which interprets "without authorization" or "exceeding authorization" as applying only to the defendant's access to the information in question, rather than the defendant's use of that information. *Power Equip. Maint., Inc. v. Airco Power Servs.*, 953 F. Supp. 2d 1290, 1295 (S.D. Ga. June 28, 2013). This narrow construction limits liability under the CFAA. Under the narrow construction, "the proper inquiry is whether an employer had, at the time, both authorized the employee to access a computer and authorized that employee to access specific information on that computer. In this respect, the actions of the employer are more dispositive that those of the employee." *Id.* That is, "[i]t is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'" *Trademotion*, 857 F. Supp. 2d at 1291. "The same is true regarding whether an employee exceeded his authorized access: it is the employer's decision as to what the employee can access that determines whether an employee exceeded his authorized access." *Power Equip. Maint., Inc.*, 953 F. Supp. 2d at 1296.

3. **Broad Construction**. On the other hand, however, courts in various jurisdictions have adopted a broad construction of authorized access under the CFAA. A broad construction increases liability under the CFAA. Courts that adopt a broad construction of authorized access under the CFAA "use an agency theory to conclude that an employee's access automatically terminates or is exceeded when his actions are no longer taken in the interest of his employer." *Power Equip. Maint., Inc.*, 953 F. Supp. 2d at 1296.

4. **Examples of Violation of CFAA**:

- *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (Court adopted a broad construction of the CFAA, that "without authorization" and/or "exceeds authorized access" includes employee misusing employer information that he or she is otherwise permitted to access. Employee found guilty for accessing information that was not in the furtherance of his job duties).

- *Ryan, LLC v. Evans*, 2012 U.S. Dist. LEXIS 59692 (M.D. Fla., Apr. 30, 2012) (relying on *Rodriguez* declined to follow magistrate's finding no unauthorized access where employees had unfettered access to employer data, information and computers and the right to add to, delete from and upload or download information).

- *See also Eagle v. Morgan*, 2012 U.S. Dist. LEXIS 143614 (E.D. Pa. Oct. 4, 2012) (employer's access to a former employee's LinkedIn® site that was associated with the employer may have violated the CFAA, but summary judgment granted for the defendant because the plaintiff could not prove a cognizable loss as a result of the access).

5. **Examples of No Violation of CFAA**:

- *Keen v. Bovie Med. Corp.*, 2013 U.S. Dist. LEXIS 64999 (M.D. Fla. May 7, 2013) (employee's access to employer-owned laptop was authorized and not violative of CFAA).

- *Trademotion, LLC v. Marketcliq, Inc.*, 857 F. Supp. 2d 1285 (M.D. Fla. Feb. 14, 2012) (because an employee had been granted full administrative access, a claim could not be brought under the CFAA regardless of how access was used).

- *Lee v. PMSI, Inc*., 2011 U.S. Dist. LEXIS 52828 (M.D. Fla. May 6, 2011) (no violation of CFAA where employee accessed personal websites from employer computer while working; further, employer could not show that employee was without authorization to access work computer).

- *Clarity Servs. v. Barney*, 698 F. Supp. 2d 1309 (M.D. Fla. 2010) (CFAA claim failed because employee had authorized access to computer although used authorization to access an e-mail from the employer's e-mail account after his termination and deleted customer information on employer's laptop).

- *See also Power Equip. Maint., Inc. v. Airco Power Servs.*, 2013 U.S. Dist. LEXIS 91484 (S.D. Ga. June 28, 2013) (cannot state a claim under the CFAA where employee had authorized access, properly accesses information, and merely uses it to employer's detriment).

E. THE STORED COMMUNICATIONS ACT, 18 U.S.C § 2701, ET SEQ. ("SCA")

1. **General Law**. The SCA prohibits intentionally accessing stored electronic or wire communications without authorization or in excess of authorization. Congress enacted the SCA "to protect privacy interests in personal and proprietary information from the mounting threat of computer hackers 'deliberately gaining access to, and sometimes tampering with, electronic or wire communications' by means of electronic trespass." *Devine v. Kapasi*, 729 F. Supp. 2d 1024, 1026 (N.D. Ill. 2010) (internal citation omitted).

2. **Remedies**. The SCA provides both criminal and civil causes of action and remedies. 18 U.S.C. §§ 2701, 2707. The possible criminal penalties include a fine and imprisonment for up to 10 years. 18 U.S.C. §2701(b). The civil remedies include preliminary and other equitable or declaratory relief as may be appropriate, actual damages suffered by the plaintiff, any profits made by the violator as a result of the violation, punitive damages where appropriate (for willful or intentional violations), reasonable attorneys' fees, and other litigation costs reasonably incurred. 18 U.S.C. §2707(b) and (c). The SCA provides that in no case shall a person entitled to recover under the Act receive less than the sum of $1,000. 18 U.S.C. §2707(c).

3. **Exceptions**. The SCA "does not apply with respect to conduct authorized (1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. §2701(c); *Ehling v. Monmouth-Ocean Hospital Service Corp.*, 961 F. Supp. 2d 659, 669 (D. N.J. 2013). The second exception is known as the authorized user exception. *Ehling*, 961 F. Supp. 2d at 669. "The authorized user exception applies where (1) access to the communication was 'authorized,' (2) 'by a user of that service,' (3) 'with respect to a communication . . . intended for that user.'" *Id.* (quoting 18 U.S.C. §2701(c)(2)). "Access is not authorized if the purported authorization was coerced or provided under pressure." *Id.* (internal quotations omitted).

4. **Examples of Accessing Employees' Electronic Communications**. Performing searches of employees' e-mail (particularly private e-mail accounts where the log-in information may be saved on a company computer) or social media profiles may violate the SCA.

    - *Ehling v. Monmouth-Ocean Hospital Service Corp.*, 961 F. Supp. 2d 659, 662-663, 665, 669-670 (D. N.J. 2013) (Plaintiff-employee maintained a non-public Facebook® account that allowed only her Facebook® "friends" to view her wall posts. A co-worker who was plaintiff's Facebook® "friend" took a screenshot of plaintiff's controversial Facebook® wall posts and provided them to management without any prompting by defendant-employer. Employer suspended plaintiff because of the Facebook® posts, and she sued employer for violations of the SCA. The Court held that plaintiff's non-public Facebook® wall posts were covered by the SCA because she "chose privacy settings that limited access to her Facebook wall to only her Facebook friends." Nevertheless, the authorized user exception applied where employee's co-worker/Facebook® friend provided unsolicited information to employer from employee's Facebook® page.).

    - *Rodriguez v. Widener University*, 2013 WL 3009736, Case No. 13-1336 (E.D. Pa. June 17, 2013) (denying employer's motion to dismiss claims under the SCA and the Electronic Communications Privacy Act where employer allegedly accessed

employee's Facebook® images and there was a factual issue as to how employer accessed or obtained the Facebook® images).

- *Castle Megastore Grp. v. Wilson*, 2013 WL 672895, Case No. CV–12–02101–PHX–DGC (D. Az. Feb. 25, 2013) (dismissing employer's SCA claim against former employee where employer alleged that employee changed the company's Facebook® password following termination; the court dismissed the claim because employer's bare assertion that employee changed the Facebook® password was insufficient to support that the Facebook® page constituted an electronic communication service under the SCA).

- *Snyder v. Fantasy Interactive, Inc.*, 2012 WL 569185, Case No. 11 Civ. 3593 (WHP) (S.D. N.Y. Feb. 9, 2012) (holding that plaintiff-employee stated a claim for violation of the SCA where employer accessed plaintiff's private Skype™ instant messages outside of the office).

F. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. § 2510, ET SEQ. ("ECPA")

1. **General Law**. The ECPA provides civil and criminal causes of action and penalties for the unlawful interception, disclosure, or use of electronic communications; and it most often arises in the labor context where employers monitor and intercept communications between employees. However, under the ECPA, consent to the interception is a defense to a violation. Title I of the ECPA is called the Wiretap Act and Title II is the SCA.

2. **Remedies**. The ECPA has criminal penalties including a fine and imprisonment for up to five years. 18 U.S.C. §2511(4). In a civil cause of action a plaintiff may recover preliminary and other equitable or declaratory relief as may be appropriate, declaratory damages, punitive damages where appropriate, reasonable attorney's fees and other litigation costs reasonably incurred. 18 U.S.C. § 2520. Notably, the ECPA provides that the plaintiff will receive at a minimum $10,000, regardless of a showing of any actual damages. 18 U.S.C. §2520(c)(2)(B). In addition, if the communication involves certain radio or private satellite video communications, the violator may be subject to suit by the federal government. 18 U.S.C. §2511(5).

3. **Interception**.

- *Shefts v. Petrakis*, Case No. 10-cv-1104, 2012 WL 4049509 (C.D. Ill. Sept. 13, 2012) (in an action between owners of a telecommunications company, co-owners' conduct constituted interceptions in violation of the ECPA where they accessed plaintiff's Yahoo!-based e-mails using a screen-capture software that took images of plaintiff's computer activities).

- *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010) (jury found violation of the Wiretap Act where employee went on his supervisor's computer while she was away and activated a "rule" on her e-mail account so that any e-mail that was sent to the supervisor was also forwarded to the employee).

4. **No Interception**.

- *Ehling v. Monmouth-Ocean Hospital Service Corp.*, 872 F. Supp. 2d 369 (D. N.J. May 30, 2012) (dismissing claim under analogous state wiretap act against employer who accessed employee's private Facebook® page via another employee's account because the Facebook® posting accessed was in "post-transmission storage" and was not in the course of transmission when employer viewed it).

- *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 883-884 (9th Cir. 2002) (An airline pilot sued employer under the ECPA after a company executive, using log-in information for another employee, accessed the pilot's private website, which contained derogatory comments of upper management. The court held that viewing the website was not an interception as defined by the ECPA.).

G. THE ECONOMIC ESPIONAGE ACT OF 1996, 18 U.S.C § 1831, ET SEQ. ("EEA")

1. **General Law**. The Economic Espionage Act of 1996 ("EEA") punishes an individual who, with the intent to convert a trade secret, "(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;" or attempts or conspires to do any of the foregoing acts. 18 U.S.C. §1832(a).

- *Lear v. Seattle Housing Authority*, 2014 WL 1089273 (W.D. Wash. March 17, 2014) (holding that for the EEA to apply, the offense must benefit a foreign government, foreign entity, or foreign agent. Further, there is no indication in the statute that it provides for a private cause of action).

2. **Penalties**. One who violates the EEA shall be subject to a fine or imprisonment of up to ten years. 18 U.S.C. §1832(b).

H. WIRE FRAUD STATUTE, 18 U.S.C. § 1343

1. **General Law**. The Wire Fraud statute, 18 U.S.C. §1343, is identical to the Mail Fraud statute. The only difference is that it requires use of wires in furtherance of the scheme,

rather than use of mail. The defendant need not have knowledge that the wires are being used.

2. **Remedies**. Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both

3. **Essential Elements**. The elements of a federal wire fraud violation are: (1) a scheme and intent to defraud; (2) money or property as object of the scheme; and (3) use of wires to further that scheme. *Fountain v. U.S.*, 357 F.3d 250, 255 (2nd Cir. 2004); *U.S. v. McNeil*, 320 F.3d 1034, 1040 (9th Cir. 2003); *Cesnik v. Edgewood Baptist Church*, 88 F.3d 902, 906 (11th Cir. 1996). The elements of a federal mail fraud violation are the same, except it requires the use of mail (not wires) in furtherance of the scheme. *Fountain*, 357 F.3d at 255; *Cesnik*, 88 F.3d at 906.

4. **Telephone Constitutes Use of Wires**. There is a much greater chance for prosecution under the Wire Fraud statute than under the Mail Fraud statute because using a telephone qualifies as "use of the wires." *See Banco de Desarrollo Agropecuario, S.A. v. Gibbs*, 640 F. Supp. 1168, 1175 (S.D. Fla. 1986) (holding that the existence of a scheme to defraud, along with one jurisdictional telephone call made in furtherance of that scheme, satisfied the requirements of the Wire Fraud statute).

I. STATE STATUTES

1. Uniform Trade Secrets Act

a. General. The Uniform Trade Secrets Act (UTSA) is a model rule that was published by the Uniform Law Commission (ULC) in 1979 and has not been amended since 1985. The ULC promulgated the UTSA in order to provide a uniform legal framework to protect against the misappropriation of trade secrets.

b. States that have Enacted the UTSA. As of February 2015, 47 states have enacted the UTSA, as has the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. Only New York, North Carolina, and Massachusetts have not enacted the UTSA.

c. Statutory Language Differs Among States. States are not required to have incorporated the UTSA into their statutory schemes verbatim, and some have made amendments to the Act. See, e.g., *JustMed, Inc. v. Byce*, 600 F.3d 1118, 1128-1129 (9th Cir. 2010) (noting that "Idaho has adopted a slightly modified version of the" UTSA that "explicitly includes a definition of 'computer program' as a protectable trade secret"). Thus, language of the UTSA varies by state.

d. Basic Elements. Generally, to establish a violation of the applicable UTSA, the plaintiff must prove that (1) the defendant wrongfully acquired, disclosed, or used (2) information constitutes a trade secret, and (3) the plaintiff took reasonable precautions to prevent disclosure of the information.

e. Remedies. The UTSA provides for several potential remedies for violations of the Act, including injunctive relief, damages, and attorney's fees.

f. Application to Cyber Theft. The information stolen or misappropriated from an employee or employer may constitute a trade secret of that employee or employer and, thus, implicate the version of the UTSA enacted in the relevant state.

2. **Law Prohibiting Employers from Requesting Social Media Information**

a. General Issue. With the proliferation of social media, employers have begun asking employees to turn over the usernames or passwords for their personal social media accounts. "Some employers argue that access to personal accounts is needed to protect proprietary information or trade secrets, to comply with federal financial regulations, or to prevent the employer from being exposed to legal liabilities." *See* The National Conference of State Legislators, *Employer Access to Social Media Usernames and Passwords*, available at http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx.

b. Statutory Development. States continuously introduce legislation pertaining to social media user names and passwords. In 2017, two states passed such a bill and in 2016, four states also passed similar bills prohibiting employers from requesting or requiring an employee or applicant to disclose a user name or password for a personal social media account. National Conference of State Legislators, *Access to Social Media Usernames and Passwords*, Jan. 8, 2018, available at http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2017.

3. **Civil Theft**

a. General Law. Various states provide a private cause of action for civil theft. In most states, a cause of action for civil theft derives from the applicable criminal statute setting forth the elements of theft, larceny, or conversion and the civil statute granting private parties a cause of action for a violation of the criminal statute. *See*, *e.g.*, *Farmington Hills Employees Retirement System v. Wells Fargo Bank, N.A.*, 979 F. Supp. 2d 981, 996 (D. Minn. 2013); *Palmer v. Gotta Have it Golf Collectibles, Inc.*, 106 F. Supp. 2d 1289, 1303 (S.D. Fla. 2000); *Voll v. Dunn*, Case No. X10UWYCV 126018520, 2014 WL 7461644, at *9 (Conn. Super. Nov. 10,

2014); *VPP Group, LLC v. Total Quality Logistics, LLC*, Case No. 13-cv-185-wmc, 2014 WL 1515510, at *7 (W.D. Wis. April 18, 2014).

b. Damages. Numerous civil theft statutes provide for treble damages, attorney's fees, and costs. *See*, *e.g.*, Colo. Rev. Stat. §18-4-405 ("the owner may recover two hundred dollars or three times the amount of the actual damages sustained by him, whichever is greater, and may also recover costs of the action and reasonable attorney fees"); Conn. Gen. Stat. §52–564 ("Any person who steals any property of another, or knowingly receives and conceals stolen property, shall pay the owner treble his damages."); Fla. Stat. §772.11(1) ("Any person who proves . . . that he or she has been injured in any fashion by [theft or exploitation] has a cause of action for threefold the actual damages sustained and, in any such action, is entitled to minimum damages in the amount of $200, and reasonable attorney's fees and court costs in the trial and appellate courts."); Wis. Stat. §895.446(3).

c. Other States. States such as Minnesota and Texas, provide for monetary damages beyond the actual value of the stolen property but short of treble damages. Minn. Stat. §604.14 ("A person who steals personal property from another is civilly liable to the owner of the property for its value when stolen plus punitive damages of either $50 or up to 100 percent of its value when stolen, whichever is greater."); Tex. Civ. Prac. & Rem. Code §134.005 (a civil theft victim may recover from the perpetrator "the amount of actual damages found by the trier of fact and, in addition to actual damages, damages awarded by the trier of fact in a sum not to exceed $1,000"). Moreover, states like Wisconsin allow a civil theft victim to recover "[a]ll costs of investigation and litigation that were reasonably incurred, including the value of the time spent by any employee or agent of the victim." Wis. Stat. §895.446(3)(b).

d. Liability. Some civil theft statutes allow the owner to maintain an action against a subsequent purchaser of the property stolen from the owner. See, e.g., Colo. Rev. Stat. §18-4-405 ("All property obtained by theft, robbery, or burglary shall be restored to the owner, and no sale, whether in good faith on the part of the purchaser or not, shall divest the owner of his right to such property. The owner may maintain an action not only against the taker thereof but also against any person in whose possession he finds the property. . . . [B]ut monetary damages and attorney fees shall not be recoverable from a good-faith purchaser or good-faith holder of the property.").

4. **Breach of Fiduciary Duty (Duty of Loyalty)**

a. General Law. The law of most, if not all, states dictates that an employee owes a fiduciary duty of loyalty to his or her employer. *See*, *e.g.*, *Synthes, Inc. v. Emerge Medical, Inc.*, 25 F. Supp. 3d 617, 667 (E.D. Pa. 2014) ("Pennsylvania law dictates that an employee, as the agent of his employer, owes his employer a duty of loyalty."); *First Financial Bank, N.A. v. Bauknecht*, 71 F. Supp. 3d 819, 837 (C.D.

Ill. 2014) ("Under Illinois law, an employee owes a fiduciary duty of loyalty to his employer."); *EndoSurg Medical, Inc. v. EndoMaster Medical, Inc.*, 71 F. Supp. 3d 525, 556 (D. Md. 2014).

b. Elements of Breach of Duty of Loyalty. To establish a breach of duty of loyalty, the plaintiff must prove (1) a fiduciary duty of loyalty existed; (2) the defendant breached this duty; and (3) such breach proximately caused the plaintiff's injury. *See Bauknecht*, 71 F. Supp. 3d at 837; *Synthes*, 25 F. Supp. 3d at 667.

5. **Restrictive Covenants**. An employer may require its employees to sign a restrictive covenant, the construction and enforcement of which is subject to the applicable law governing the agreement. These restrictive covenants may include non-compete, non-solicitation, and/or confidentiality or non-disclosure clauses. Any restrictive covenant for employment should explicitly describe the employee's duties and obligations, and contract law generally governs any dispute. Public policy may operate to reduce the scope of a restrictive covenant, but this varies along with the state.

6. **Tortuous Interference with a Contract or Business Relationship**. Many states have law prohibiting a party from interfering with the contractual or business relationship of two other parties under certain circumstances. The elements of a claim for tortious interference with a contract or business relationship differ from state to state, but the generally require: (1) the existence of a contractual or business relationship between the plaintiff and a third party; (2) the defendant intentionally and unjustifiably interfered with this relationship; and (3) the interference caused the plaintiff actual damages.

7. **Statutes Pertaining to Electronically Stored Communications**

   a. Numerous states have enacted statutes regulating electronically stored communications. *See* Charles Doyle, *Privacy: An Overview Of The Electronic Communications Privacy Act,* Congressional Research Service, Oct. 9, 2012, available at, http://fas.org/sgp/crs/misc/R41733.pdf.

   b. States have a statute regarding electronically stored communications; provisions may differ among states.

   c. States also have statutes that regulate electronically stored communications; provisions may differ among states.

8. **Computer Crime Statutes**. Each state has enacted a computer crime statute, although the statutory provisions differ among the various states. *See* Doyle at 86.

9. **Statutes Prohibiting Offenses Against Intellectual Property**. To the extent that cyber theft involves intellectual property, the act of cyber theft may also implicate a cause of action under state statutes protecting intellectual property. Statutory

prohibitions of offenses against intellectual property may be included in computer crime statute of the particular state. Review whether your state law protects intellectual property and could apply to cyber theft.

10. **Statutes Prohibiting Conversion**. "Conversion consists of a tortious detention or destruction of personal property, or a wrongful exercise of dominion or control over the property inconsistent with or in defiance of the rights of the owner." Ritter, Laber and Assoc., Inc. v. Koch Oil, Inc., 680 N.W.2d 634, 640 (ND 2004). "A conversion claim, unlike an unjust enrichment claim, requires the plaintiff prove the defendant had an intent to deprive the plaintiff of the property." *McColl Farms, LLC v. Pflaum*, 837 N.W.2d 359, 367 (N.D. 2013).

11. **Wiretap Statutes**. Most states have enacted statutes that mirror the Federal Wiretap Statute. However, the statutory provisions differ among states. For instance, some wiretap statutes require the consent of one party before a communication may be recorded, while other states require consent from all parties to the communications. *See, e.g.*, Fla. Stat. §934.02(a)(12) (consent of all parties is required as long as the communication is made in Florida or at least one of the parties is a Florida resident); 720 Ill. Compiled Stat. §§5/14-1 and 5/14-2 (consent of all parties required unless interceptor is law enforcement officer acting within the scope of the criminal law); Cal. Penal Code §632 (all parties to the communication must give permission unless the communication was made in a public place, during a court proceeding, or under circumstances in which the parties could reasonably expect interception or recording of their communications).

DISCLAIMER

The laws and cases referenced in these materials may have changed since the date of publication.

These materials are being made available for informational purposes only and are not to be relied upon as legal advice.

If you have an employment law question,
we urge you to seek legal counsel.