

## Required Reading

### **6.1 – WG12 Forensic Issues in Trade Secret Disputes – Draft Outline Discussion of Topics Currently Anticipated for BSG3 Drafting Team**

## **WG12 Forensic Issues in Trade Secret Disputes – Draft Outline Discussion of Topics Currently Anticipated for BSG3 Drafting Team**

### Purpose

- To date, lawyers have used forensic data in different ways to achieve goals in their litigation. This paper is designed to help you best use the data at various stages in litigation.
  - The purpose is to provide the best practices of using forensic experts or consultants in trade secret misappropriation cases
  - The intended audiences are outside counsel, organizations, and courts

### Goals/Objectives

- Principles as discussed below

### Pre-Litigation Forensic Investigations

[Proposed] Guideline No. 1 – When appropriate, a party contemplating bringing an action alleging misappropriation of a trade secret or breach of a duty of confidentiality concerning electronically stored information should [discussion point: should, should consider, may] conduct a forensic investigation of relevant devices and accounts in its possession, custody, or control, including computers, smartphones, online storage, and email accounts before filing a complaint alleging misappropriation of trade secrets or breach of a duty of confidentiality.

- What is a pre-litigation forensic investigation?
- When is a forensic investigation necessary?
  - A forensic investigation may be helpful when there is a reasonable suspicion or threat of misappropriation, a high-risk employee departs, or to uncover further misappropriation after it is discovered, for example, that the departing employee sent confidential or trade secret information to a personal email account.
- What information is relevant to a forensic investigation and should be preserved?
  - Identify examples of the types of info that are relevant to a pre-litigation investigation.
  - Discuss best practices for preservation of potentially relevant forensic information.
- Who conducts a pre-litigation forensic investigation?
  - Again, this is very fact specific.
  - In some circumstances, this can be done by company IT personnel if they have the appropriate tools and training. In other circumstances, an outside expert is necessary.
- Evidentiary concerns
  - Will the investigator submit a declaration in connection with a request for a TRO, be subject to expedited discovery, or have to testify at a preliminary injunction hearing?

- How to conduct the investigation in a manner that leads to useful testimony and admissible evidence.
- E.g., chain of custody issues
- Litigation Benefits
  - Helpful in jurisdictions like CA and MA and other state or federal courts that require plaintiffs to identify the alleged misappropriated trade secrets with reasonable particularity before discovery can be conducted by the plaintiffs.
  - May be helpful in securing a TRO.
- Time considerations
  - Pre-litigation forensic investigations will typically be subject to substantial time pressure, and thus the amount of investigation differs from a post-litigation/post-TRO forensic investigation.

### Forensics in Expedited Discovery Proceedings

[Proposed] Guideline No. 2 – Where parties are engaged in expedited discovery proceedings in advance of a hearing on a motion for preliminary injunctive relief based on allegations of misappropriation of trade secrets or breach of a duty of confidentiality, they should discussion point: should, should consider, may provide non-privileged discovery concerning forensic investigations, forensic reports, and forensic experts if they intend to rely on that information in support of the motion for preliminary injunctive relief.

- Key issue: What role should forensics have in expedited discovery proceedings in connection with a motion for preliminary injunctive relief?
  - Courts should be comfortable with expedited discovery proceedings in trade secret matters.
- Quintessential character of trade secrets is the threat of disclosure and potential irreparable harm. Cross-reference equitable remedies commentary. That risk often constitutes “good cause” under Rule 26.
- Moreover, expedited discovery can result in the prompt identification and sequestration of misappropriated information, reducing the chances of further copying, use, or dissemination of the information, and the extent of remediation.
  - But expedited discovery should not be viewed as a substitute for full case discovery.
- Insert cases with disputes over expedited discovery.
- Insert cases with orders addressing requests for expedited discovery (both stipulated and opposed) for baselines.
  - Expedited forensic discovery should be proportional and targeted to the issues presented in the motion for preliminary equitable relief.
- Wholesale provision of images may be agreed to by the parties, but the existence of relevant forensic data does not necessarily entitle the requesting party to full images.
- Accommodate privilege and privacy concerns.
- Forensic discovery can have longer collection periods because of the requirements inherent in appropriately preserving forensic discovery. Additional protection measures, such as two factor authentication or encryption can delay the imaging process, and the

parties and court should be cognizant of what is feasible within expedited discovery parameters.

- Preliminary injunctions should not be a trial by ambush. The relevant underlying forensic data should be provided to the opposing party as part of the expedited discovery process versus included only in the response.
- Parties should confer regarding the parameters and extent of forensic discovery.
- It is important to have a clear understanding of scope and what can be accomplished in expedited discovery.
  - Will the forensic expert be neutral or retained by one party with confidentiality restrictions?
  - What will be handled under the protocol?
  - Who will retain possession of sources?
  - How will the data be maintained, and when will it be accessible by one or both parties?
  - What reports will be generated? Will they be provided to all parties or only certain parties? When will they be generated and exchanged?
  - How will searches for misappropriated files be done?
  - Who will get the reports and underlying substantive files?
  - Under what circumstances can a party include additional terms or search criteria?
  - Do all requests for work under the protocol need to be mutual?
  - Will the neutral provide a final report for authenticity/admissibility?
  - How will disputes about the forensic process be resolved?
  - Under what circumstances can the neutral communicate with only one party?
  - Who pays the neutral's fees and expenses?
  - What happens to imaged materials, reports, and exports when the case is over?
- Remediation in expedited forensic discovery
- Early remediation activity may help mitigate damage, prevent intentional or inadvertent disclosure, and allow for the return of otherwise quarantined devices. But proper remediation requires understanding the character of relevant sources, the exfiltrated data, and any subsequent migration to other sources.
- There are stronger obligations associated with affirmative actions (mandatory injunctions) as part of injunctive relief. Consider whether remediation should be occurring on an expedited basis.
- Parties should retain forensically sound litigation copies of remediated data for use in litigation.

### The Role of Court Appointed/Independent Forensic Neutrals and Forensic Experts

[Proposed] Guideline No. 3 – In advance of commencing litigation asserting that another engaged in misappropriation of trade secrets or breach of a duty of confidentiality, the parties should [discussion point: should, should consider, may] consider using an independent forensic neutral or one party's forensic expert to conduct a forensic investigation and perform a

remediation of devices and accounts to attempt to resolve the dispute without the need for litigation.

Proposed] Guideline No. 4 – Where a party seeks forensic images of another party’s computers, smartphones, or accounts, including personal devices and accounts, the court may appoint and the parties should [discussion point: should, should consider, may] consider using a forensic neutral or one party’s forensic expert to perform the investigation in order to resolve concerns about privilege, privacy, or sensitive business information that is not relevant to the allegations of misappropriation of trade secrets or breach of a duty of confidentiality.

### Key issues

- Can courts adopt a standard set of protocols for the use of independent forensic neutrals or the parties’ forensic experts?
- Recommendations Regarding Initial Disclosures and Discovery of Forensics
- Should the parties meet and confer pursuant to Rule 16 (federal court proceedings) or in advance of an initial case management conference regarding the need for, timing, and scope of forensic discovery, any remediation of devices or accounts, and the return of any electronically stored information or documents reflecting potentially confidential, proprietary, or trade secret information?
- Should discovery concerning forensic evidence (including forensic and logical images and forensic reports) be provided early to facilitate the plaintiff in identifying the trade secrets at issue with reasonable particularity and prior to expert discovery?

### Considerations for Drafting Team

- The role of a neutral in pre-litigation matters
- Difference between an independent consultant or expert versus a forensic neutral (e.g., one party retains an independent but opposing party agrees to abide by protocol being executed by one side’s retained consultant, versus both parties retaining regardless of who pays)
- Should you use a neutral for expert opinions?
- The background needed for an effective protocol
- How involved should the neutral be in the drafting or agreement of a drafted protocol before it is stipulated/ordered?
- Sedona stance on the use of Sedona issued sample protocols (e.g., neutral, recommended use, simplifying offering suggestions, etc.)
- Protocol Samples
  - Devices to consider (e.g., laptops, servers, external drives, etc.)
  - Accounts to consider
  - Cloud repositories
  - Mobile devices
  - Social media
  - Other forms of electronic media
  - What types of reporting and is that dependent on the matter (e.g., connected devices, search hit reports)

### Forensic Remediation as a Remedy

[Proposed] Guideline No. 5 – Where an action alleges misappropriation of trade secrets or breach of a duty of confidentiality concerning electronically stored information, the parties should [discussion point: should, should consider, may] meet and confer pursuant to Rule 16 (federal court proceedings) or in advance of an initial case management conference regarding the need for, timing, and scope of forensic discovery, any remediation of devices or accounts, and the return of any electronically stored information or documents reflecting any potentially confidential, proprietary, or trade secret information

[Proposed] Guideline No. 6 – Parties should [discussion point: should, should consider, may] seek forensic analysis and remediation in appropriate trade secret matters as a part of a temporary restraining order, preliminary injunction, or permanent injunction in order to identify, quarantine, and render inaccessible confidential, proprietary, and trade secret information on the defendant's devices and accounts.

- Courts have the power to issue injunctive and other affirmative relief in trade secret matters. *See, e.g., CUTSA*. Injunctions can be prohibitory or mandatory. In a prohibitory injunction, court orders party to refrain from taking actions, e.g., accessing or using trade secrets. In mandatory injunction, court orders party to take affirmative actions, e.g., searching for and destroying copies of misappropriated trade secret information. Forensics are helpful for both.
- Prohibitory injunction:
- Explanation, and types.
- Injunction to refrain from “accessing” trade secrets can be too broad. [See cases.] Injunction can avoid being too broad by referring to specific files or methodologies for search appropriately tailored to identify the trade secrets.
- Even if court does not require any forensics, defendant can use forensics to help itself comply with injunction, by identifying, forensically preserving, isolating trade secrets and confidential information, and as appropriate, deleting them from their original sources.
- Mandatory injunction:
- In many cases, prohibitory injunction may be sufficient; companies can be trusted to comply with the threat of sanctions or reopened proceedings. Indeed, in some cases, forensic evidence establishes that while files containing trade secrets may have been misappropriated (*i.e.*, taken through improper means), there is no evidence they were used/copied. *E.g.*, no evidence of opening from jmp/link/shellbag, no evidence of being disseminated to cloud storage locations, or sent via email, as examples. In that case, an injunction to remove known files may be sufficient.
- But in some cases, Plaintiff may seek more extensive remedies, *e.g.*,

- if initial misappropriation not limited to one person, or if evidence is that person used trade secrets extensively or spread them to others. If forensic evidence of opening, emailing, printing, copying, etc., a higher escalation of forensic work may be appropriate.
- In appropriate cases, court can
  - order defendant to affirmatively search for, identify, and then return, quarantine, or destroy trade secret information. *E.g.*, particular files, particular content (ESI search), etc. (Party could also, in theory, be required to take any other appropriate action, such as conducting additional diligence to determine how trade secrets may have been used.)
  - create ongoing monitoring and validation protocols, with continued jurisdiction. Cite.
- Court can:
  - leave compliance in hands of defendant, subject to motion practice from plaintiff;
  - order certificate of compliance from defendant;
  - order parties to meet-and-confer on an appropriate protocol, including forensics, and enter protocol as a court order;
  - order court-appointed or neutral forensic expert;
  - order that plaintiff's or defendant's forensic expert shall conduct forensics;
  - coordination of forensic work with additional remediation activities.
- *See generally Allergan v. Merz. The Sedona Conference, Commentary on Equitable Remedies in Trade Secret Litigation, 23 SEDONA CONF. J. 591 (2022).*
- Other considerations
- Boundaries, costs and termination of injunction.
- Consider the potential anticompetitive nature of certain trade secret actions (drown defendant in costs for exhaustive forensic review when misappropriation was limited)
- If court orders quarantine/destruction of trade secrets, how does that work where trade secrets have already been used to create derivative works? *E.g.*, scientists who have used trade secrets to inform their inventions and can't forget what they know.
- Data protection issues / foreign government issues:

- Court order may be impossible to comply with, e.g., changing access rights to certain files, where the files are not even within the defendant's "control" because they are hosted directly/by third party in a restricted jurisdiction.
- Or, forensic protocol conflicts with foreign data protection, localization, secrecy etc. laws restricting compelled actions.