AMERICAN BANKRUPTCY INSTITUTE

# 2019 Central States Bankruptcy Workshop

*Business/Consumer Crossover Session*

# E-Discovery and Cybersecurity for Insolvency Professionals


**Hon. Mary Ann Whipple, Moderator**
*U.S. Bankruptcy Court (N.D. Ohio); Toledo*

**Mark Kindy**
*Alvarez & Marsal; New York*

**Megan P. McKnight**
*Tealstone Law, PLC; Royal Oak, Mich.*

**Elizabeth B. Vandesteeg**
*Sugar Felsenthal Grais & Helsinger LLP; Chicago*


CONCURRENT SESSION

2019


**Moderator:**

**Hon. Mary Ann Whipple**
United States Bankruptcy Judge
Northern District of Ohio

**Panelists:**

**Elizabeth Vandesteeg**
SFGH
Sugar Felsenthal Grais & Helsinger LLP

**Mark Kindy**
A&M

**Megan McKnight**
TEALSTONE LAW

# Program Overview

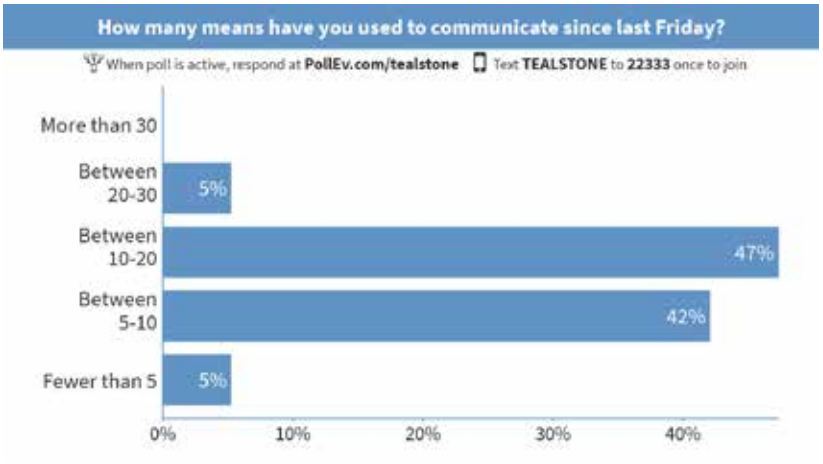


# Poll Everywhere

- 1. Text TEALSTONE to 22333
- 2. Wait for confirmation.
- 3. Text the letter associated with your response.
- Notes: Standard text messaging rates apply. All responses are private.
- We are not able to link back to anyone's responses.


# Results: Michigan State Law Students March 2019

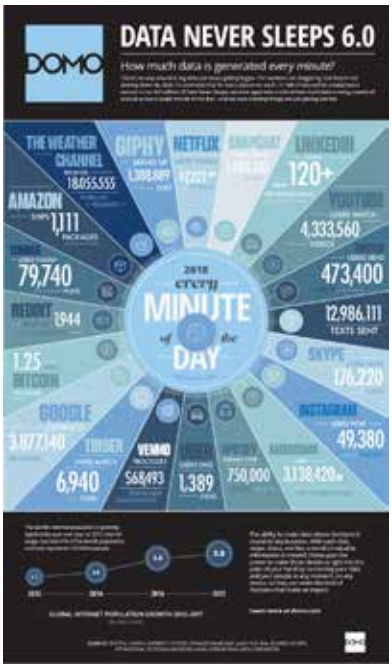
# Results: Michigan State Law Students March 2019




Big Data & the Communication Explosion


Permission to use infographic in this slide deck only rec'd via twitter to @megpmck from @LoriLewis & @OfficiallyChadd on 4/23/19.

Big Data & the Communication Explosion




Permission only to use infographic in this slide deck rec'd via twitter to @megpmck from @domo on 4/23/19.

LAWYERS' DUTY OF TECHNOLOGICAL COMPETENCY: ETHICAL OBLIGATIONS AND DATA SECURITY BEST PRACTICES FOR BANKRUPTCY PROFESSIONALS

# Ethical Obligations: Sources of Duties and Guidance

- ABA MRPC 1.1 Competence (Cmt. 8)
- ABA MRPC 1.6 Confidentiality of Information
- ABA Formal Opinion 477
- ABA MRPC 1.15 Safekeeping Property
- ABA MRPC 5.3 (Cmt. 3) Responsibilities Regarding Nonlawyer Assistants
- ABA Formal Opinion 483

# ABA MRPC 1.1: Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation necessary for the representation.

Cmt [8]

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology….

Language added in 2012

## State Specific Analogs to MRPC 1.1 [Cmt. 8]

- Illinois amended its Cmt 8 to Rule 1.1 to add the "including the benefits and risks associated with relevant technology language," eff. January 1, 2016
- Indiana amended its Cmt 6 to Rule 1.1 to add the "including the benefits and risks associated with relevant technology language," eff. January 1, 2018
- Michigan has not amended its Rule 1.1 or the comments to add the ABA comment language, nor is there such a duty expressly appearing in or connection with any other rules

## State Specific Analogs to MRPC 1.1 [Cmt. 8], cont.

- Ohio amended its then Cmt 6 now Cmt 8 to Rule 1.1 to add the "including the benefits and risks associated with relevant technology language," eff. April 1, 2015
- Wisconsin *see* its Cmt 6, amended and renumbered as Cmt 8 to Rule 20:1.1 to add the "including the benefits and risks associated with relevant technology language," eff. January 1, 2017 (comments not adopted but published and available for guidance)

# ABA MRPC 1.6: Confidentiality of Information

**Imposes a duty of confidentiality, which includes protecting client information:**

**"(c)** A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information related to the representation of a client.

Adopted in some form in: Illinois (as Rule 1.6(e)); Indiana (as Rule 1.1 cmt 16]; Michigan (as Rule 1.6(d)-least similar language to MRPC 1.1(c)); Ohio (as Rule 1.6(d)); and Wisconsin (as Rule 20:1.6(d))

# ABA MRPC 1.6: Confidentiality of Information, cont.

**Cmt [18]** Division (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating int eh representation of the client or who are subject to the lawyer's supervision. The unauthorized access to or the inadvertent or unauthorized disclosure of information related to the representation of a client does not constitute a violation of division (c) if the lawyer has made **reasonable efforts** to prevent the access or disclosure.

# ABA MRPC 1.6: Confidentiality of Information, Cmt [18] cont.

**Cmt [18]** identifies the following factors to be included, but not limited to, in considering whether a lawyer's efforts are reasonable:

- the sensitivity of the information
- the likelihood of disclosure if addt'l safeguards are not employed
- the cost of additional safeguards
- the difficulty of implementing the safeguards
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.* making device or software too hard to use)

# ABA MRPC 1.6: Confidentiality of Information, Cmt [18] cont.

Cmt [18] also provides that:

"A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forego security measures that would otherwise be required by this Rule."

AND

"Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state or federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules."

# ABA MRPC 1.6: Confidentiality of Information, cont.

**Cmt [19]**

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take **reasonable precautions** to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may require special precautions.

Cmt [19] identifies the following non-exclusive factors to in considering whether a lawyer's precautions are reasonable:

- the sensitivity of the information
- the extent to which the privacy of communications is protected by law
- the extent to which the privacy of communications is protected by a confidentiality agreement

# ABA MRPC 1.6: Confidentiality of Information, Cmt [19] cont.

**Cmt [19]** (similarly to **Cmt [18]**) also states that:

"A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule."

AND

"Whether a lawyer may be required to take additional steps in order to comply with other law, such as state or federal laws that govern data privacy, is beyond the scope of these Rules."

**Cmt [20]**

"The duty of confidentiality continues after the client-lawyer relationship has terminated…"

# State rule analogs to ABA MRPC 1.6: Confidentiality of Information, Cmts. [18-19]

Indiana (Rule 1.6, Cmt. 17)

Illinois (Rule 1.6, Cmts. 18-19)

Michigan (none)

Ohio (Rule 1.6 Cmts. 18-19)

Wisconsin (Rule 20.1.6, *see* cmts. [18]-[19]-comments not adopted but published and available for guidance)

# ABA Formal Opinion 477: Securing Communication of Protected Client Information (May 4, 2017)

Pointing to Model Rule 1.6(c), cmt [18], Opinion 477 does not mandate specific cybersecurity measures but instead requires "reasonable efforts" to ensure client confidentiality when using any form of electronic communications, including email, text messaging, and cloud based document sharing. It sets out seven factors to consider when determining the appropriate level of cybersecurity:

- The nature of the threat
- How client confidential information is stored and sent
- The use of reasonable electronic security measures
- How electronic communications should be protected
- Need to label client information as privileged and confidential
- Need to train lawyers and nonlawyer assistants
- Need to conduct due diligence on vendors who provide technology services (for guidance, see ABA formal Opinion 08-451)

# ABA MRPC 1.15: Safekeeping Property

(a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. Funds shall be kept in a separate account…Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer…

Safekeeping duty adopted in some form but with significant variations in details and language in various states: Illinois (in Rule 1.15(a)); Indiana (as Rule 1.15(a) and very similar to MRPC 1.15(a)); Michigan (similar reqm'ts at Rule 1.15(b)(2) and (d)); Ohio (as Rule 1.15(a) and very similar to MRPC 1.15(a)); and Wisconsin (in Rule 20:1.15)

# ABA MRPC 5.3: Responsibilities Regarding Nonlawyer Assistance

With respect to a nonlawyer employed by or retained by or associated with a lawyer:

- Lawyers with managerial authority in a law firm must take reasonable efforts to ensure that the law firm or government agency has in effect measures giving reasonable assurance that the person's conduct is compatible wit the professional obligations of the lawyer
- Same obligation as to lawyer with direct supervisory authority over nonlawyer
- Lawyer is responsible for conduct of nonlawyer that would violate the MRPC if:

**(1)** lawyer orders or ratifies specific conduct with knowledge of it, or

**(2)** lawyer knows of conduct at a time when consequences can be avoided or mitigated but fails to take reasonable remedial action

# ABA MRPC 5.3: Responsibilities Regarding Nonlawyer Assistance, cont.

**Cmt [2]**

…A lawyer must give such assistants [*e.g.* secretaries, investigators, law student interns, and paraprofessionals-whether employees or independent contractors] appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product…

*See* Indiana (Rule 5.3 and comments); Illinois (Rule 5.3 and comments); Michigan (Rule 5.3 and comment); Ohio (Rule 5.3 and addt'l cmts); Wisconsin (Rule 20:5.3, referencing ABA comments))

# Limits of a Lawyer's Duties Under ABA MRPC 5.3:

"A lawyer's duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology," and "[w]hen it comes to the use of cloud computing [as a "non-lawyer" form of outsourcing the storage and transmission of data], the Rules of Professional Conduct do not impose a strict liability standard."

New Hampshire Bar Association Ethics Committee Advisory Opinion #2012-13/04 The Use of Cloud Computing in the Practice of Law

## ABA Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach (October 17, 2018)

Data breach defined: "a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform legal services for which the lawyer is hired is significantly impaired by the episode."

- Lawyers must take steps to proactively monitor for data breaches and cyber attacks
- If a breach occurs, lawyers must take steps to stop it, restore affected systems and notify current and former clients about the breach and any damage
- Adopt bests practices, including proactively developing an incident response plan and procedures for data breach response

## III. PRIVACY FOR BANKRUPTCY PROFESSIONALS

# What types of information and data do all companies need to protect?

- Personally identifiable information (PII): information that can be linked to a specific individual
  - Includes name, birthdate, social security number, driver's license number, account numbers
- Non-personally identifiable information: cannot by itself be used to identify a specific individual
  - Aggregate data, zip code, area code, city, state, gender, age
- Gray area – "anomyzed data"
  - Non-PII that, when linked with other data, can effectively identify a person
  - Includes geolocation data, site history, and viewing patterns from IP addresses

# What Data Must Be Protected?

- Personally Identifiable Information (PII)
  - Social Security number
  - Drivers license number
  - Credit/debit card numbers
  - Passport number
  - Bank Account Information
  - Date of Birth
  - Medical Information
  - Mother's maiden name
  - Biometric data (i.e., fingerprint)
  - E-mail/username in combination with password/security question & answer

# What Data Must Be Protected?

- Payment Card Information (PCI)
  - Primary Account Number (PAN)
  - Cardholder Name
  - Expiration Date
  - Service Code (3 or 4 digit code)
  - PIN

# What Data Must Be Protected?

- Business Information
  - Customer lists
  - Prospect lists
  - Trade secrets
  - Pricing information
  - Business plans and strategies
  - Employee lists

## Why do we need to protect it?

- Data is a corporate asset
- Corporate data is at a higher risk of theft or misuse than ever before

## Consumer Data Issues in Bankruptcy

- How does a business deal with sale of consumer data?
- Can it be sold?
- What about data collected with the express promise of "we will not sell your data"?
  - 11 U.S.C. § 363(b)(1) requirements for a hearing regarding sale of PII
- Government (FTC) intervention/involvement
- Federal Rule of Bankruptcy Procedure 9037 – Privacy Protection for Filings Made with the Court

# Consumer Data Issues in Bankruptcy Continued

- Section 341 notice – SSN listed and sent to all creditors
- HIPAA – patient records
- UST involvement and oversight

# Compliance Problems and Issues: Personally Identifiable Information ("PII")

**(1)** Noncompliance with Bankruptcy Rule 9037: Privacy Protection for Filings Made With the Court

Examples of problem filings: schedules, pay advices, claims, motions for relief from stay, reaffirmation agreements (especially supporting documentation), motions to redeem, trial exhibits

Under Bankruptcy Rule 9037(a), unless the court orders otherwise, special treatment and redaction is required in an electronic or paper filing for:

- Individual social security numbers (include only last 4 digits)(*but see* petition preparer disclosure form))
- Taxpayer-identification numbers (include only last 4 digits)
- Birth dates and names of minors (year of birth and initials only)
- Financial-account numbers (include only last 4 digits)

# Compliance Problems and Issues, cont.

**(2)** Free communication of client social security numbers by lawyers and staff to court staff to obtain case information—who are you really talking to?

**(3)** CM/ECF User password problems: Local Automation Specialists cannot retrieve a lost password or change it because they don't know who the requester is

**(4)** Malware and phishing emails sent to judge and likewise also clients from attorney e-mail addresses

**(5)** Other bankruptcy courts: reports of fake communications to clients purporting to be from lawyer, court or case trustee and directing turnover of personal information or money allegedly required as part of the bankruptcy case and requirements for discharge

**(6)** Other bankruptcy courts: reports of fake communications to lawyers purporting to be from clients or third parties directing turnover of personal information or money as part of an ongoing transaction or case

**(7)** Other courts: redacting pdfs incorrectly to disclose protected information (*Manafort* case)

# Best Practices:

**(1)** Promote compliance with Rule 9037 with careful review of every filing and submission to the court, electronic and otherwise, to prevent improper disclosures. Make sure staff is trained properly in these issues.

**(2)** Make sure your client understands the bankruptcy process and what will be likely to happen in a case, be it consumer or business, and what will be required and when of individual debtors or debtor employees.

**(3)** Develop a secure communication protocol with your client and make sure that your client understands that the court and the trustee will not be communicating with her directly by phone or e-mail except through DeBN. Make sure your client knows to contact you, and how and when to contact you, with respect to any request for information or documents or money from any person.

# Best Practices, cont.

**(4)** Become familiar with United States Trustee's Handbook Requirements for Chapter 7 Trustees, which provide good guidance for all of us:

Imposes specific restrictions on use of wire transfers

Requires specific computer security measures

Requires trustees to develop and maintain a business interruption plan

Requires specific records security and retention policies, including individual case records and tax returns

The United States Trustee's Handbook for Chapter 7 Trustees (pages 5-15 to 5-21).

# Privacy Ombudsmen

- Section 332(a):If a hearing is required under section 363(b)(1)(B), the court shall order the United States trustee to appoint, not later than 7 days before the commencement of the hearing, 1 disinterested person (other than the United States trustee) to serve as the consumer privacy ombudsman in the case and shall require that notice of such hearing be timely given to such ombudsman.

## How do privacy ombudsmen work on a practical level?

- Privacy ombudsman will provide information at a hearing on the potential sale of PII regarding the potential losses or gains of privacy and possible costs or benefits to consumers
- Can recommend certain mitigating steps to prevent privacy losses to consumers

## When is a privacy ombudsman necessary and what role will he/she play?

- Becoming more common in cases where PII is an asset to be sold
- Can provide recommendations, sometimes in concert with other concerned parties such as attorneys general or the FTC, regarding changes to potential sales of PII

# IV. ELECTRONIC DISCOVERY FOR INSOLVENCY PROFESSIONALS

2015 AMENDMENTS TO FEDERAL RULES OF CIVIL PROCEDURE ARE CHANGING EDISCOVERY PRACTICE

ALVAREZ & MARSAL

## Civil Rules Amendments That Became Effective on December 1, 2015: Case Management and Discovery Rules

Goals of the Discovery Amendments:

- Promote cooperation: Rule 1
- Early and active case management: Rule 16
  To expedite the initial stages of litigation and control the discovery process
- Focus the scope of discovery on what is necessary to resolve the case: Rule 26
  Emphasis on proportionality and reasonableness
- Address problems with vast amounts of ESI: Rules 16, 26 and 37
- Preservation of ESI and uniform national standard for sanctions for loss of ESI (spoliation)

These amendments became effective in bankruptcy practice through incorporation into the analogous Part VII Adversary Proceeding rules and in turn to contested matters, in part (not Rule 16 and the Rule 26(f) amendments), through Rule 9014(c).

*See also* Rule 9016 incorporating Rule 45 governing subpoenas and commands to produce ESI.

45

## Summary of Changes to the Discovery Rules Effective December 1, 2015

Amended rules recognize the exponential growth of ESI

New rules addressing the timing, sequencing and scope of discovery

The importance of proportionality in discovery has been magnified

Changes in how to respond to discovery requests

Changes to rules related to spoliation of ESI

"Corrective measures" for loss of ESI and how applied

46

## Scheduling Conferences and Orders: Rules 16 and 26

Under Rule 16(b)(3)(B)(iii) *Permitted Contents*, a scheduling order may provide:

> "for disclosure, discovery, or preservation of electronically stored information"

Under the Rule 26(f)(3) *Discovery Plan,* the plan to be developed in connection with the Rule 26(f)conference of the parties must state the parties' views and proposals on: …

> "(C) any issue about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced"

**Amended Rule 26(b)(1): Scope of discovery**

Unless otherwise limited by court order, the scope of discovery is now as follows:

Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense AND proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

## Rules Committee Comment on Change

The amendment is intended to restore the proportionality factors to their original place in defining the scope of discovery. This change reinforces the Rule 26(g) obligation of the parties to consider and certify compliance with these factors in making discovery requests, responses, or objections.

Restoring the proportionality calculation to Rule 26(b)(1) [from Rule 26(b)(2)] does not change the existing responsibilities of the court and the parties to consider proportionality, and the change does not place on the party seeking discovery the burden of addressing all proportionality considerations.

Nor is the change intended to permit the opposing party to refuse discovery simply by making a boilerplate objection that it is not proportional. The parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes.

49

## Also: exclusion of examples

Another portion of pre-amendment Rule 26(b)(1) is omitted from the amended rule. After allowing discovery of any matter relevant to any party's claim or defense, the prior rule added: "including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter."

Discovery of these matters is thought to be so deeply entrenched in practice that it is no longer necessary to clutter the text of Rule 26 with these examples. The discovery identified in these examples should still be permitted under the new rule when relevant and proportional to the needs of the case. For example, framing intelligent requests for ESI may require detailed information about another party's information systems and other information resources.

50

**Enforcing the New Rules:**
**Amended Rule 26(c)(1)(B)**

"A party or any person from whom discovery is sought may move for a protective order in the court where the action is pending … including one or more of the following: (B) specifying terms, including time and place or the allocation of expenses for disclosure or discovery."

The prior rule included authority to enter such orders and courts already exercise it. But explicit recognition was thought by the Rules Committee to forestall the temptation of some parties to contest this authority. Recognizing the authority does not imply that cost-shifting should become a common practice. According to the Rules Committee, courts and parties should continue to assume that a responding party ordinarily bears the costs of responding.

51

**Changes in Responding to Discovery: No More Boilerplate Objections**

(b) (2) *Responses and Objections. …*

(B) *Responding to Each Item.* For each item or category, the response must either state that inspection and related activities will be permitted as requested or state with specificity the grounds for objecting to the request, including the reasons. The responding party may state that it will produce copies of documents or of electronically stored information instead of permitting inspection. The production must then be completed no later than the time for inspection specified in the request or another reasonable time specified in the response.

Rule 34(b)(2)(B)

52

**Changes in Responding to Discovery: No More Boilerplate Objections, cont.**

Amended Rule 34(b)(2)(B) requires that objections to Rule 34 document production requests be stated with specificity.

This provision adopts the language of Rule 33(b)(4), eliminating any doubt that less specific objections might be suitable under Rule 34.

The specificity of the objection ties to the new provision in Rule 34(b)(2)(C) directing that an objection must state whether any responsive materials are being withheld on the basis of that objection.

53

**More Changes to Rule 34(b)(2)(B)**

Rule 34(b)(2)(B) is further amended to reflect the common practice of producing copies of documents or electronically stored information rather than simply permitting inspection.

The response to the request must state that copies will be produced.

The production must be completed either by the time for inspection specified in the request or by another reasonable time specifically identified in the response. When it is necessary to make the production in stages the response should specify the beginning and end dates of the production.

54

**Amended Rule 34(b)(2)(C)**

An objection must now state whether any responsive materials are being withheld on the basis of that objection. An objection to part of a request must specify the part and permit inspection of the rest.

The Rules Committee intends this amendment to end the confusion that arises when a producing party states several objections and still produces information, leaving the requesting party uncertain whether any relevant and responsive information has been withheld on the basis of the objections. The producing party does not need to provide a detailed description or log of all documents withheld, but does need to alert other parties to the fact that documents have been withheld and thereby facilitate an informed discussion of the objection. An objection that states the limits that have controlled the search for responsive and relevant materials qualifies as a statement that the materials have been "withheld."

55

**Rules Committee Note Explains:**

An objection may state that a request is overbroad, but if the objection recognizes that some part of the request is appropriate the objection should state the scope that is not overbroad.

Examples would be a statement that the responding party will limit the search to documents or ESI stored information created within a given period of time prior to the events in suit, or to specified sources.

When there is such an objection, the statement of what has been withheld can properly identify as matters "withheld" anything beyond the scope of the search specified in the objection.

56

## Amended Rule 37(e): ESI and Spoliation

FAILURE TO PRESERVE ELECTRONICALLY STORED INFORMATION. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:

(A) presume that the lost information was unfavorable to the party;

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment.

57

## Why Do We Care About Rule 37(e)?

**Guess what?** Bankruptcy debtors (individuals and entities alike) and creditors have abundant ESI

Examples of *individual* types of ESI: text messages
social media posting/social networks
e-mail accounts
photo storage sites
on line banking and credit card records
on line access to payroll info, retirement accounts, insurance policies

Examples of where it is stored: cell/smart phones
computers: work and home
tablets/iPads
external storage: hard drives, flash drives, the cloud
smart TVs

58

## Why Do We Care About Rule 37(e)?, cont.

Consider whether and when a debtor's or creditor's duty to preserve arises. Arguably, a debtor's responsibility for preserving ESI begins the minute a debtor contemplates filing for bankruptcy.

Rule 2004 does not specifically incorporate the procedural rules governing ESI, but in consideration of the possible outcomes of a Rule 2004 exam, it would be prudent to make sure that the relevant ESI is preserved.

The ABA Business Law Section published its Best Practices Report on Electronic Discovery (ESI) Issues in Bankruptcy Cases in the August 2013 issue of The Business Lawyer, Volume 68, No. 4. This Report contains an excellent survey of proposed Best Practices for all aspects of bankruptcy practice, including representation of (i) debtors (including individuals) and creditors in Chapters 7, 13 and 11, (ii) parties in adversary proceedings, and (iii) claimants in Chapter 7, 13 and 11 cases.



## More Points From the Committee Note to Rule 37(e)

Rule 37(e) applies only when information is lost. Because ESI often exists in multiple locations, loss from one source may be harmless if substitute information can be found elsewhere.

The new rule applies only if the lost information should have been preserved in the anticipation or conduct of litigation and the party failed to take reasonable steps to preserve it. Many court decisions hold that potential litigants have a duty to preserve relevant information when litigation is reasonably foreseeable.

Rule 37(e) is based on this common-law duty; it does not attempt to create a new duty to preserve. The rule does not apply when information is lost before a duty to preserve arises.

**Circling Back: ESI and the Proportionality Standard**

> Computer-based methods of searching ESI continue to develop, particularly for cases involving large volumes of electronically stored information. Courts and parties should be willing to consider the opportunities for reducing the burden or expense of discovery as reliable means of searching electronically stored information become available.
>
> From Rules Committee Note to Rule 26.

61

# Recent Cases – eDiscovery In Bankruptcy

## 2004 Exams – Convergence with Proportionality

- In rejecting a debtor's request for a broad 2004 exam, the Bankruptcy Court explained that, "Rule 2004 has not been similarly amended [to rule FRCP 26] but the spirit of proportionality is consistent with the historic concerns regarding the burden on the producing party and is relevant to the determination of cause." *In re Sunedison, Inc.*, 562 B.R. 243, 250 (Bankr. S.D.N.Y. 2017).

# Recent Cases – eDiscovery In Bankruptcy

**The Federal Court Rules Apply. Really.**

- *Ries v. Ardinger (In re Adkins Supply, Inc.)*, 555 B.R. 579, 593 (Bankr. N.D. Tex. 2016)
  - Rule 34: Court requires debtor's counsel to organize and label documents to respond to document requests, rejecting merely directing trustee to warehouse, explaining that, "defendants have provided no evidence to the Court that the current manner of storage in a warehouse meets the usual course of business option.
  - Protective Order: Court rejects request for broad protective order, because "Defendants have not submitted affidavits or demonstrated any specific facts to meet their burden of good cause."
  - Rule 33 & 26: Court overrules blanket and broad objections to interrogatories, explaining that "not a single interrogatory objection by defendants is proper."
  - *See also. . . .Trevino v. Caliber Home Loans, Inc. (In re Trevino)*, 564 B.R. 890 (Bankr. S.D. Tex. 2017)

# Recent Cases – eDiscovery In Bankruptcy

**Court Sanctions Non-Party and Debtor After Spoliation by Non-Party, 2004 Exam Witness**

- In re Correra, 589 B.R. 76 (Bankr. N.D. Tex., 2018)
- Former assistant of debtor wiped computer she had used while employed by debtor after computer requested at 2004 Exam and otherwise refused to cooperate.
- Court found sanctions appropriate pursuant to Section 105 of Bankruptcy Code and Inherent Power. Court looked to FRCP 37 "as a guide to determine proper level of response to contemptor's offense."
- Non-party sanctioned & ordered to pay Creditor and Trustee's attorney fees.
- Party/Debtor sanctioned.
  - Court explained that Debtor's duty to preserve extended to computer pre 2004 exam of non-party, continued after 2004 exam of non-party. Court relied on sections 521(a)(3), 521(a)(4) and 542 of the Code and in anticipation of litigation regarding exemptions.
  - Instead, Debtor did nothing to preserve computer and "actively opposed the Trustee's and the [Creditor's] efforts to recover the deleted evidence," including paying for the attorney of the non-party.
  - Debtor sanctioned & ordered to pay Creditor and Trustee's attorney fees (join and several liability with non-party).
  - Debtor ordered to turn-over additional data stores that may hold deleted evidence.
- Court ordered that a subsequent hearing as to whether it should "as a further sanction under Rule 37(e), infer that the spoliated ESI would have been unfavorable for the Debtor and would have established the invalidity of the exemptions he is claiming, to which the NMSIC and the Trustee have objected.
- See also Schlossberg v. Abell (In re Abell) (Bankr. Md., 2016)

PRESERVATION: DOCUMENT RETENTION AND STORAGE AND RESPONDING TO DISCOVERY REQUESTS

ALVAREZ & MARSAL

## Topics of Discussion

- People, Process, Technology
- Application Inventory & Data Map
- Standard Repeatable & Defensible Processes
- Tech to Tech Discussions
- Don't Play Game of Telephone
- Faster, Cheaper, Better – Creative Solutions to Discovery Obligations
- Proportionality – Understanding the Burden of Producing Systems Data
- Optimizing Accessibility of Document and Data Productions

## Client Perspective

*What to preserve?* **Balancing cost / spoliation concerns**

**Judgement is Required**

While the amended rules seek to clarify what triggers exposure for spoliation, sound judgment is still required.

A company must balance the need to delete ESI and manage data storage costs with:

1. The need to retain information for corporate and legal use and;
2. The need to continually evaluate this tension as the business and legal needs/obligations change over time.



## Client Perspective

*What to preserve?* **Balancing cost / spoliation concerns**

**Exposure:**

- Given number and scope of claims, obligation to preserve data and documents can be extraordinarily broad
- Shared access to documents and data with 3rd parties can further complicate the preservation/retrieval process
- Systems may be sold or decommissioned given ongoing business needs
- Cost of preservation for bankrupt and/or insolvent entity a serious concern

**Clients should have a deletion policy:**

- Big data initiatives often mean that we're saving everything we can – email, text message, social media - about our customers in the remote chance it may be useful later
- Saving data, especially email and informal chats, is a liability and a security risk
  - The best security against potential data theft is not to have the data in the first place
- Customer data should be deleted as soon as it is no longer useful
- Unless there are laws requiring an organization to save a particular type of data for a prescribed length of time, deletion should be the norm

## Electronically Stored Information (ESI) – Structured & Unstructured Data

*What to preserve?* **Balancing cost / spoliation concerns**

**What is Structured Data?**

- Data collected to conduct business transactions (i.e. trades, treasury, financial, general ledger, product customer, etc.)
- Companies use a variety of database management systems residing across various platforms

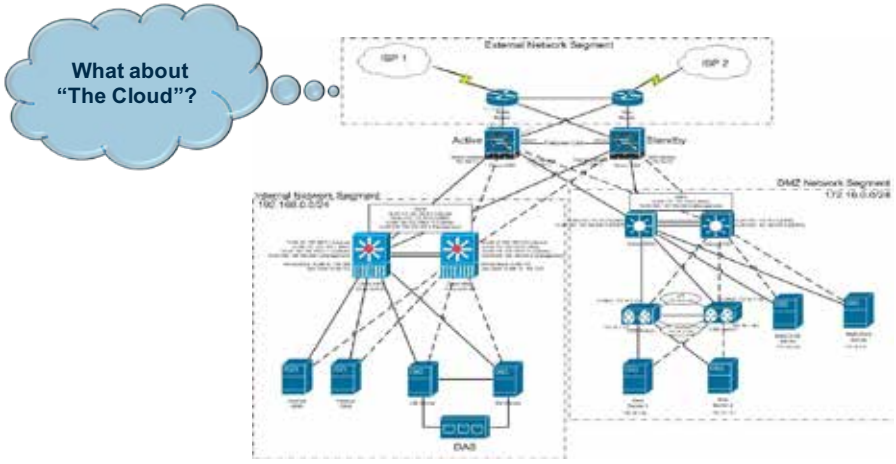
**What is Unstructured Data?**

- Relates to electronic communication data, network files and archived hard copy documents
  - User created files (groups and home shares)
  - Email communications
  - Instant messaging
  - Bloomberg messaging
  - Offsite archived bankers boxes
  - Twitter
  - Facebook



AMERICAN BANKRUPTCY INSTITUTE
ALVAREZ & MARSAL

## Do You Know Where Your ESI Is?






AMERICAN BANKRUPTCY INSTITUTE
ALVAREZ & MARSAL

## Technologist / Consultant Perspective

1. **Technology – Pre-Bankruptcy**
   - IT Resources
   - # of Servers
   - # of Data Centers
   - # of Devices
   - # of Applications
   - IT budget

2. **Identify, Interview, Catalogue & Preserve**
   - Volume of data supporting applications
   - Volume of communication data
   - Volume of messages
   - Volume of files
   - Volume of contracts/reports/agreements
   - Volume of boxes
   - Volume of backup tapes



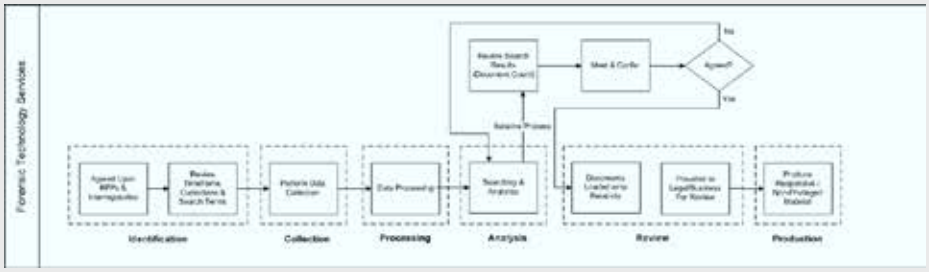


## Technologist / Consultant Perspective

3. **Preservation**
   - Identification
   - Interviews with owners – business, IT & SME's
   - Catalogue
   - Preserve
   - Collection
   - Extraction
   - Migration

4. **Operationalize**
   - People
   - Process
   - Technology

## Standard, Repeatable & Defensible Process






AMERICAN BANKRUPTCY INSTITUTE
ALVAREZ & MARSAL

OFFENSIVE DISCOVERY

ALVAREZ & MARSAL

## Document and Data Retrieval Obligations and Challenges

1. **Getting to the bottom of burden**
   - How much time will it take and how many people are needed – total person hours and system run time
   - Total costs – vendor charges and soft dollar employees diversion cost

2. **Relevance**
   - Consider framing as an opportunity to present your case and potentially condition the judge

3. **Proportionality**
   - Key consideration under amended rules
   - Tie potential damages to requested discovery





## Creative Solutions

1. **If requested discovery is genuinely viewed as irrelevant, consider reviewing only for privilege**
   - Shifting cost of review for irrelevant documents to your adversary can have material impact
   - Must consider harm to reputation from embarrassing documents and providing fodder for otherwise unrelated litigations

2. **Consider using low cost professions with expertise in underlying subject matter**
   - Training required; need critical mass of work to justify retention

## Partners at a Table




## Cost Effective & High Quality Analysis

- **Be thoughtful about who reviews discovery materials**
  - As with defensive discovery review, if subject matter is technical, consider using low cost professionals with expertise
  - Advantage for offensive discovery potentially far greater than defensive
  - Technical expertise can provide critical insight into significance of discovery
  - Translation/understanding of technical jargon/industry specific parlance can reveal the underlying story that might otherwise remain hidden
  - Cost savings can be enormous as compared to attorneys or even paralegals

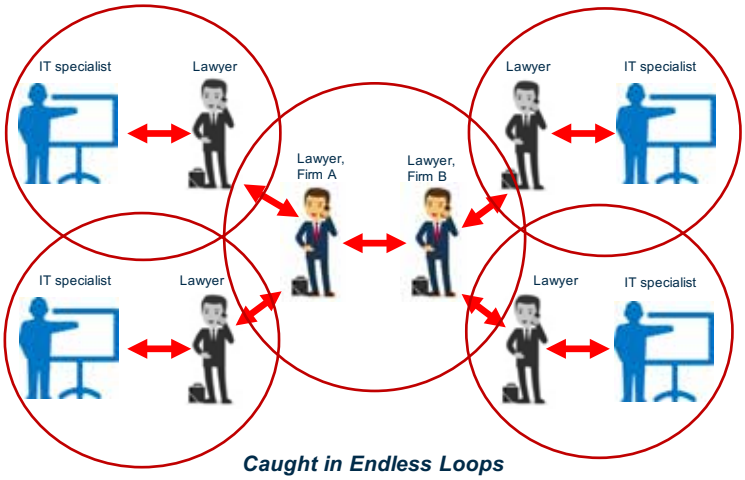
## Demand Detailed Explanations of Burdens and Costs

- Accounting of costs and time to produce must be crystal clear
- Involve IT professionals whenever burden is grounds for objection
- Don't wait for opposition to a motion to compel to request an affidavit
- Proportionality is not just a shield. If size of case and related damages are sufficient, use proportionality as a sword





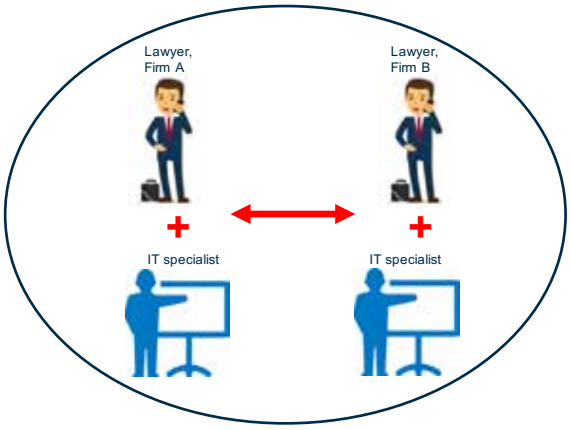
## Don't Play a Game of Telephone




***Caught in Endless Loops***

## Speaking a Common Language

**Tech-to-Tech Discussions**






## Don't Be Afraid to Go to the Judge

- The amended rules contemplate cooperation and early resolution of discovery disputes, but that's no reason to capitulate on important issues
- Expect to be tested and prepared to call a bluff
- Stand by your best judgement of what's justified/proportional
- Don't assume technical expertise – present in laymen's terms – keep it as simple and straightforward as possible

## Lessons Learned

1. Encourage your client to get organized and understand their IT environment
2. Identify technology SME's or consultants who can be spokespersons
3. Develop a standard, repeatable and defensible process
4. Early on and continuously throughout the matter have IT, business and legal at the table
5. Be specific about cost and burden and request your adversary to be specific as well
6. Defend and challenge "burden"
7. Don't be afraid to go to the judge





## V. CYBERSECURITY RISKS FOR INSOLVENCY PROFESSIONALS

## Understanding Cybersecurity Risk Pillars

'threat' = capability × intent | 'risk' = probability × harm

**Threat**

An action, potential action, or inaction, likely to cause damage, harm or loss.

**Vulnerability**

Specific gaps in the protection of assets that can be exploited by Threats in order to compromise the asset and realize a Risk.

**Risk**

The resulting damage, harm or loss of unmitigated Vulnerability to Threats



## Example of Vulnerabilities

- **Import of unknown client data**
  - Porous file transport site
  - Ineffective malware scanning and detection
- **Perimeter attacks**
  - Poorly configured or absent web application firewall (WAF)
  - No Intrusion Detection (IDS) or Prevention (IPS)
- **Social Attacks**
  - Ineffective user training and poor user account management
  - No File Integrity Monitoring or HIDS
- **Internal Actors**
  - No Network Access Control (NAC)
  - Ineffective Data Leakage Protection (DLP)

**Weakness to breakage or harm from threats**

## Example of Threats

- **Import of unknown client data**
  - Processing of Advanced Persistent Threats (APT)
  - Infection of third-party review systems
- **Perimeter attacks**
  - Perimeter attack and breach
  - Access to client or other sensitive data
- **Social Attacks**
  - Productivity attacks (Ransomware, DDoS)
  - Command and Control (CnC)
- **Internal Actors**
  - Corporate or legal espionage
  - Data theft and sabotage

**Any activity intended to cause damage or break through defenses**





## Example of Risks

- **Import of unknown client data**
  - Undetected network infection
  - Infection of third-party productions
- **Perimeter attacks**
  - Undetected loss of client or company data
  - Unavailable Web Applications
- **Social Attacks**
  - Inside-out perimeter breach
  - Easily established pivot point
- **Internal Actors**
  - Undetectable data exfiltration
  - Evasive techniques custom developed

**The damage caused, real or potential, and costs incurred with breakage**

## Breach Causality

The number one driver in most cybersecurity breaches is ineffective leadership and culture

**Contributing factors:**

- Cybersecurity awareness that is lacking or under informed
- Refusal to acknowledge threats
- Culture of ignoring risks and vulnerabilities over revenue
- Inexperience
- Hubris

*"Risk comes from not knowing what you are doing."*
– Warren Buffet



AMERICAN BANKRUPTCY INSTITUTE
ALVAREZ & MARSAL

## Applying to eDiscovery

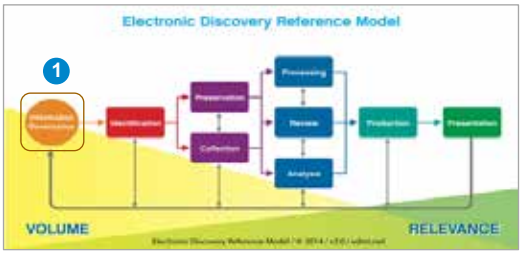
**Industry Related Vulnerabilities**

- Ineffective or non-existent data import security
- Weak detective and defensive posture
- No plan that considers detected malware in responsive evidence
- No regulatory or legal guidance for data analytics companies
- Myriad of client industry specific regulations



AMERICAN BANKRUPTCY INSTITUTE
ALVAREZ & MARSAL

## Cybersecurity and the EDRM



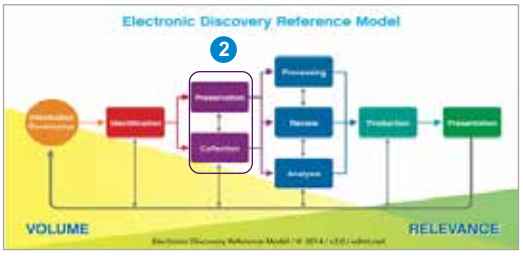

**1. Information Governance, Risk and Compliance**

- Unknown or misidentified and widely variant ambiguous regulatory controls
- Misunderstood or ignored industry specific security threats
- Underdeveloped or absent enterprise security policy
- Absent or ineffective corporate security governance and auditing





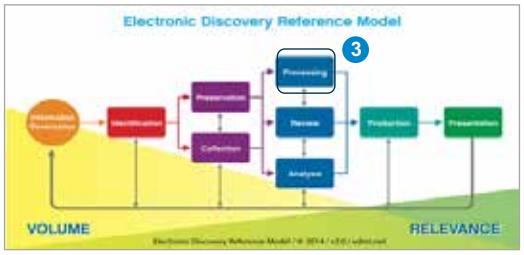
## Cybersecurity and the EDRM




**2. Preservation, Collection and Import**

- Data collectors and forensic examiners unaware of specific risks
- Unhygienic collection methodologies
- Poor data segmentation
- Processes that do not account for likely sources of infection (advanced malware scanning)

## Cybersecurity and the EDRM




**3. Processing and Analysis**

- Potentially infected files processed within the evidence population
- Infection of processing and review systems as well as the corporate network
- No network segmentation
- Ineffective or absent network and server log aggregation and analytics



AMERICAN BANKRUPTCY INSTITUTE
ALVAREZ & MARSAL

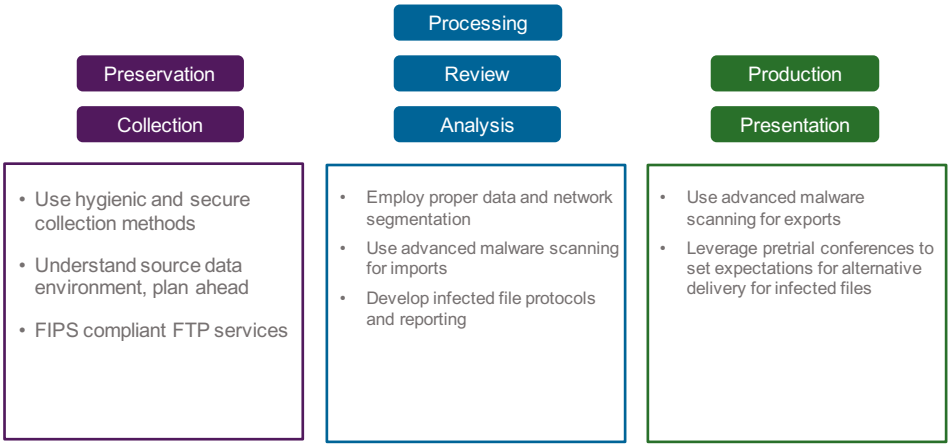
## State of Cybersecurity in eDiscovery Today

- Very little in the way of regulation or governmental guidance
- Courts and law firms are just beginning to comprehend the risks
- Cybersecurity increasingly a component of pretrial conferences
- Client flow-down cybersecurity assessments now commonplace
- Must understand client data security measures and their industry specific regulatory burdens (HIPAA, PCI) prior to collection
- Increase in the outsourcing of pre-processing
- Adoption of cloud services such as RelativityOne



AMERICAN BANKRUPTCY INSTITUTE
ALVAREZ & MARSAL

## Noteworthy Takeaways



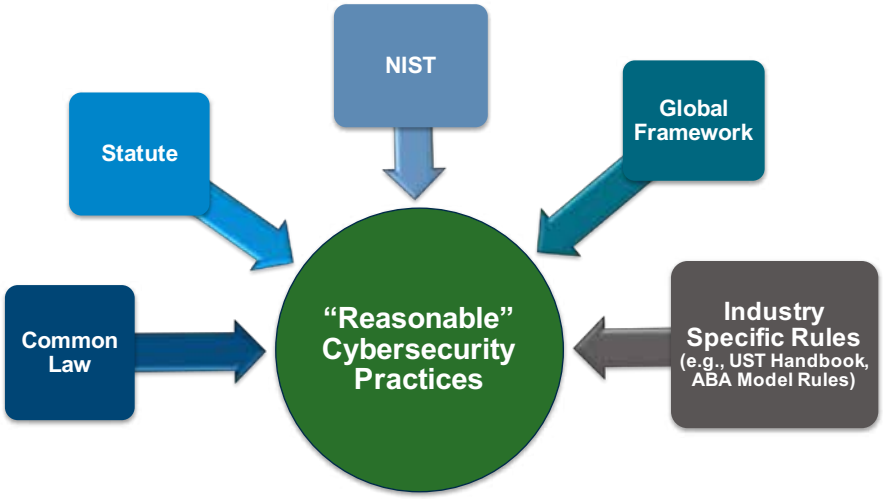

Alvarez & Marsal Disputes and Investigations 95

AMERICAN BANKRUPTCY INSTITUTE
ALVAREZ & MARSAL

# Social Engineering….are you safe?

- At it's heart, social engineering is all about using our willingness to trust against us.
- Social engineering attacks seem intentionally innocent.
- Social media and the internet in general have made social engineering attacks incredibly effective. We freely give up information on a regular basis. Birthday, anniversaries, family and pet names. Think how many password "reminders" ask you questions based upon information easily available from the internet.
- Bad actors seek to gather information that can be used in further attacks, *e.g.* employee names and job titles, e-mail addresses, phone numbers, account or social security numbers, logins.
- Bankruptcy courts, insolvency professionals, creditors and debtors (consumer and business) are easy targets. Much of our information is public via PACER, court and company websites. Be extremely vigilant with any attachments or links sent to your e-mail.
- Can be combined with e-mail "spear phishing" attacks by using the information gained to send malicious e-mail with a virus payload from what appears a legitimate account or to make phone or e-mail contact, such as to redirect a known forthcoming document, check or wire transfer.

What are the Standards of Care for Insuring Data Security?




# Vendor best practices

**What you should know about your vendor**

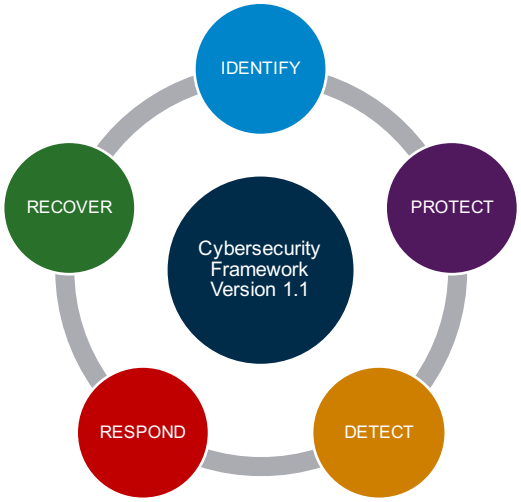
- Who is responsible if information is breached due to vendor action or inaction?
- Who is financially liable?
- Can you shift vendors/resources and recover quickly?

**Best Practices**

- Perform site review; leverage security and process experts in your company
- Allow vendor access only to required data
- Limit and segregate log-ins to mitigate potential breaches
- Address responsibilities and liability if your vendor becomes compromised and impacts your business
- Understand vendor's loss recovery processes and service level agreements currently in place
- Do your homework – check references, awards, company standards regarding product, data security processes, procedures to ensure balanced risk-reward decision
- Hold your vendor to the same "Best Practice" standards you adopt internally

# Protecting Data – Best Practices

- NIST Framework -- voluntary standards, guidelines, and best practices to manage cybersecurity-related risk.




## Best Practices: Basic Information Security Tips

- Have a plan. Regardless if you're part of a large firm or a solo practice, take time to either create or understand how you'll respond to an IT security issue. If you know information was compromised, speed and timeliness is everything in mitigating risk.
- Know your SLA (Service Level Agreement). Software you purchase, IT contractors, data service providers, *etc.* should all be providing you with some form of agreement, even if it's simply terms of service. Understand where your risk lies. A free e-mail account may not provide you with the security that a paid-for account might, for example. In the event that provider has a security compromise, are you protected by this agreement?
- Be extremely careful with using personal equipment for case work. Try to keep your work computer and any home computer tasks on separate devices. Many malware attacks are initiated by simple browsing or opening infected e-mail files. Keeping your personal e-mail, social media, and general web browsing as far away from any work files as feasible.
- Make sure everyone that has access to your privileged information is on the same page with training and understanding of risk. Your bankruptcy court logins and passwords link to your account and reflect as such. It's vital to ensure your whole team knows and understands the importance of data security.

# THANK YOU!

## Moderator:

**Hon. Mary Ann Whipple**
United States Bankruptcy Judge
Northern District of Ohio

## Panelists:

**Elizabeth Vandesteeg**

SFGH
Sugar Felsenthal Grais & Helsinger LLP

**Mark Kindy**

A&M

**Megan McKnight**

TEALSTONE LAW


## Presenters

### Moderator:

**Hon. Mary Ann Whipple**
United States Bankruptcy Judge
Northern District of Ohio

### Panelists:

**Elizabeth Vandesteeg**
SFGH
Sugar Felsenthal Grais & Helsinger LLP

**Mark Kindy**
A&M

**Megan McKnight**
TEALSTONE LAW

## Program Overview



3

AMERICAN BANKRUPTCY INSTITUTE

# 01 Era of Big Data and Communication Overload

ALVAREZ & MARSAL


## Poll Everywhere

**1. Text TEALSTONE to 22333**

**2. Wait for confirmation.**

**3. Text the letter associated with your response.**

Notes: Standard text messaging rates apply. All responses are private.

We are not able to link back to anyone's responses.

## Which flavor of ice cream best represents you?

Start the presentation to see live content. Still no live content? Install the app or get help at PollEv.com/app



AMERICAN BANKRUPTCY INSTITUTE

## How have you communicated during the past seven (7) days? With colleagues, clients, friends, family. . . .

Start the presentation to see live content. Still no live content? Install the app or get help at PollEv.com/app



AMERICAN BANKRUPTCY INSTITUTE

## Results

### Michigan State Law Students March 2019

**What means have you used to communicate with others since last Friday morning?**

Poll is full and no longer accepting responses




AMERICAN BANKRUPTCY INSTITUTE

**How many means have you used to communicate since last Friday?**




AMERICAN BANKRUPTCY INSTITUTE

## Big Data & the Communication Explosion

Big Data & the Communication Explosion


*Permission to use infographic in this slide deck only rec'd via twitter to @megpmck from @LoriLewis & @OfficiallyChadd on 4/23/19.*



AMERICAN BANKRUPTCY INSTITUTE

# 02 Lawyers' Duty of Technological Competency: Ethical Obligations

ALVAREZ & MARSAL

## Ethical Obligations: Sources of Duties and Guidance

- ABA MRPC 1.1 Competence (Cmt. 8)
- ABA MRPC 1.6 Confidentiality of Information
- ABA Formal Opinion 477
- ABA MRPC 1.15 Safekeeping Property
- ABA MRPC 5.3 (Cmt. 3) Responsibilities Regarding Nonlawyer Assistants
- ABA Formal Opinion 483





## ABA MRPC 1.1: Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation necessary for the representation.

Cmt [8]

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…

Language added in 2012

## State Specific Analogs to MRPC 1.1 [Cmt. 8]

| ILLINOIS | INDIANA | MICHIGAN | OHIO | WISCONSIN |
|---|---|---|---|---|
| Amended its Cmt 8 to Rule 1.1 to add the "including the benefits and risks associated with relevant technology language," eff. January 1, 2016 | Amended its Cmt 6 to Rule 1.1 to add the "including the benefits and risks associated with relevant technology language," eff. January 1, 2018 | Has not amended its Rule 1.1 or the comments to add the ABA comment language, nor is there such a duty expressly appearing in or connection with any other rules | Amended its then Cmt 6 now Cmt 8 to Rule 1.1 to add the "including the benefits and risks associated with relevant technology language," eff. April 1, 2015 | *See* its Cmt 6, amended and renumbered as Cmt 8 to Rule 20:1.1 to add the "including the benefits and risks associated with relevant technology language," eff. January 1, 2017 (comments not adopted but published and available for guidance) |

15

AMERICAN BANKRUPTCY INSTITUTE

## ABA Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach (October 17, 2018)

Data breach defined: "a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform legal services for which the lawyer is hired is significantly impaired by the episode."

- Lawyers must take steps to proactively monitor for data breaches and cyber attacks
- If a breach occurs, lawyers must take steps to stop it, restore affected systems and notify current and former clients about the breach and any damage
- Adopt bests practices, including proactively developing an incident response plan and procedures for data breach response

16

AMERICAN BANKRUPTCY INSTITUTE

## ABA Formal Opinion 477: Securing Communication of Protected Client Information (May 4, 2017)

Pointing to Model Rule 1.6(c), cmt [18], Opinion 477 does not mandate specific cybersecurity measures but instead requires "reasonable efforts" to ensure client confidentiality when using any form of electronic communications, including email, text messaging, and cloud based document sharing. It sets out seven factors to consider when determining the appropriate level of cybersecurity:

- The nature of the threat
- How client confidential information is stored and sent
- The use of reasonable electronic security measures
- How electronic communications should be protected
- Need to label client information as privileged and confidential
- Need to train lawyers and nonlawyer assistants
- Need to conduct due diligence on vendors who provide technology services (for guidance, see ABA formal Opinion 08-451)





# 03 Privacy for Bankruptcy Professionals

## What Types of Information and Data Do All Companies Need to Protect?

- **Personally identifiable information (PII): information that can be linked to a specific individual**
  - Includes name, birthdate, social security number, driver's license number, account numbers
- **Non-personally identifiable information: cannot by itself be used to identify a specific individual**
  - Aggregate data, zip code, area code, city, state, gender, age
- **Gray area – "anomyzed data"**
  - Non-PII that, when linked with other data, can effectively identify a person
  - Includes geolocation data, site history, and viewing patterns from IP addresses

19

AMERICAN BANKRUPTCY INSTITUTE

## PII Must Be Protected

**Personally Identifiable Information (PII)**

- Social Security number
- Drivers license number
- Credit/debit card numbers
- Passport number
- Bank Account Information
- Date of Birth
- Medical Information
- Mother's maiden name
- Biometric data (i.e., fingerprint)
- E-mail/username in combination with password/security question & answer

20

AMERICAN BANKRUPTCY INSTITUTE

## Consumer Data Issues in Bankruptcy

- How does a business deal with sale of consumer data?
- Can it be sold?
- What about data collected with the express promise of "we will not sell your data"?
  - 11 U.S.C. § 363(b)(1) requirements for a hearing regarding sale of PII
- Government (FTC) intervention/involvement
- Federal Rule of Bankruptcy Procedure 9037 – Privacy Protection for Filings Made with the Court





## Consumer Data Issues in Bankruptcy (Continued)

- Section 341 notice – SSN listed and sent to all creditors
- HIPAA – patient records
- UST involvement and oversight

## Compliance Problems and Issues: Personally Identifiable Information ("PII")

**(1) Noncompliance with Bankruptcy Rule 9037: Privacy Protection for Filings Made With the Court**

Examples of problem filings: schedules, pay advices, claims, motions for relief from stay, reaffirmation agreements (especially supporting documentation), motions to redeem, trial exhibits

Under Bankruptcy Rule 9037(a), unless the court orders otherwise, special treatment and redaction is required in an electronic or paper filing for:

- Individual social security numbers (include only last 4 digits)(but see petition preparer disclosure form))
- Taxpayer-identification numbers (include only last 4 digits)
- Birth dates and names of minors (year of birth and initials only)
- Financial-account numbers (include only last 4 digits)





## Compliance Problems and Issues (Continued)

2) Free communication of client social security numbers by lawyers and staff to court staff to obtain case information—who are you really talking to?
3) CM/ECF User password problems: Local Automation Specialists cannot retrieve a lost password or change it because they don't know who the requester is
4) Malware and phishing emails sent to judge and likewise also clients from attorney e-mail addresses
5) Other bankruptcy courts: reports of fake communications to clients purporting to be from lawyer, court or case trustee and directing turnover of personal information or money allegedly required as part of the bankruptcy case and requirements for discharge
6) Other bankruptcy courts: reports of fake communications to lawyers purporting to be from clients or third parties directing turnover of personal information or money as part of an ongoing transaction or case
7) Other courts: redacting pdfs incorrectly to disclose protected information (Manafort case)

## Privacy Ombudsmen

Section 332(a):If a hearing is required under section 363(b)(1)(B), the court shall order the United States trustee to appoint, not later than 7 days before the commencement of the hearing, 1 disinterested person (other than the United States trustee) to serve as the consumer privacy ombudsman in the case and shall require that notice of such hearing be timely given to such ombudsman.



AMERICAN BANKRUPTCY INSTITUTE

# 04 Electronic Discovery for Insolvency Professionals

ALVAREZ & MARSAL


## Civil Rules Amendments That Became Effective on December 1, 2015: Case Management and Discovery Rules

- Amended rules recognize the exponential growth of ESI
- New rules addressing the timing, sequencing and scope of discovery
- The importance of proportionality in discovery has been magnified
- Changes in how to respond to discovery requests
- Changes to rules related to spoliation of ESI
- "Corrective measures" for loss of ESI and how applied

These amendments became effective in bankruptcy practice through incorporation into the analogous Part VII Adversary Proceeding rules and in turn to contested matters, in part (not Rule 16 and the Rule 26(f) amendments), through Rule 9014(c).

*See also* Rule 9016 incorporating Rule 45 governing subpoenas and commands to produce ESI.

## Amended Rule 37(e): ESI and Spoliation

**FAILURE TO PRESERVE ELECTRONICALLY STORED INFORMATION.** If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

- (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
- (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
  - (A) presume that the lost information was unfavorable to the party;
  - (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
  - (C) dismiss the action or enter a default judgment.

29

AMERICAN BANKRUPTCY INSTITUTE

## Why Do We Care About Rule 37(e)?

**Guess what?** Bankruptcy debtors (individuals and entities alike) and creditors have abundant ESI

**Examples of Individual Types of ESI:**

- Text messages
- Social media posting/social networks
- Email accounts
- Photo storage sites
- Online banking and credit card records
- Online access to payroll info, retirement accounts, insurance policies

**Examples of Where It Is Stored:**

- Cell / smart phones
- Computers: work and home
- Tablets / iPads
- External storage: hard drives, flash drives, the cloud
- Smart TVs

30

AMERICAN BANKRUPTCY INSTITUTE


## Client Perspective

*What to preserve?* **Balancing cost / spoliation concerns**

**Judgement is Required**

While the amended rules seek to clarify what triggers exposure for spoliation, sound judgment is still required.

A company must balance the need to delete ESI and manage data storage costs with:

1. The need to retain information for corporate and legal use and;
2. The need to continually evaluate this tension as the business and legal needs/obligations change over time.

# Client Perspective

## *What to preserve?* **Balancing cost / spoliation concerns**

**Exposure:**

- Given number and scope of claims, obligation to preserve data and documents can be extraordinarily broad
- Shared access to documents and data with 3rd parties can further complicate the preservation/retrieval process
- Systems may be sold or decommissioned given ongoing business needs
- Cost of preservation for bankrupt and/or insolvent entity a serious concern

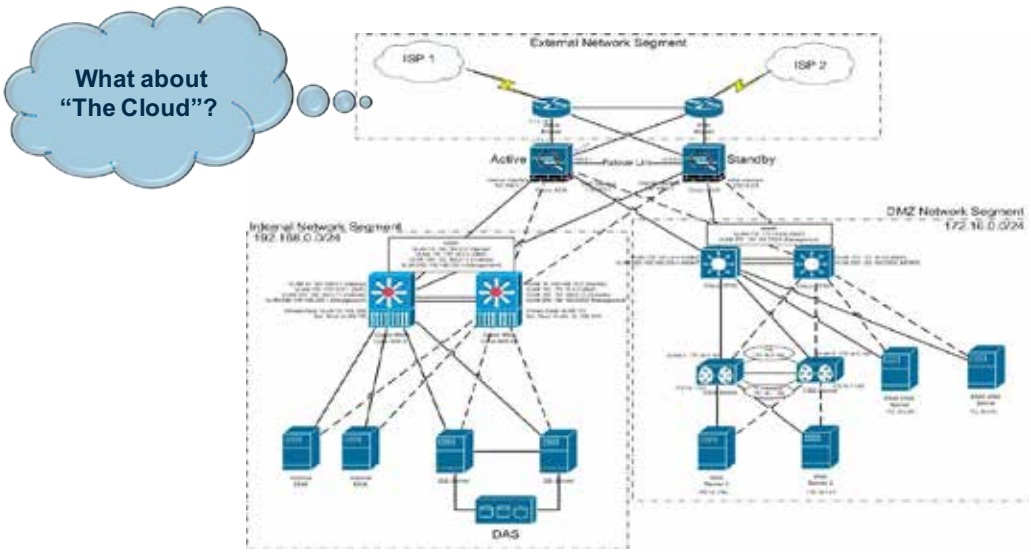
**Clients should have a deletion policy:**

- Big data initiatives often mean that we're saving everything we can – email, text message, social media - about our customers in the remote chance it may be useful later
- Saving data, especially email and informal chats, is a liability and a security risk
  - The best security against potential data theft is not to have the data in the first place
- Customer data should be deleted as soon as it is no longer useful
- Unless there are laws requiring an organization to save a particular type of data for a prescribed length of time, deletion should be the norm

AMERICAN BANKRUPTCY INSTITUTE

33

# Do You Know Where Your ESI Is?




AMERICAN BANKRUPTCY INSTITUTE

34

## Technologist / Consultant Perspective

1. **Technology – Pre-Bankruptcy**
   - IT Resources
   - # of Servers
   - # of Data Centers
   - # of Devices
   - # of Applications
   - IT budget

2. **Identify, Interview, Catalogue & Preserve**
   - Volume of data supporting applications
   - Volume of communication data
   - Volume of messages
   - Volume of files
   - Volume of contracts/reports/agreements
   - Volume of boxes
   - Volume of backup tapes

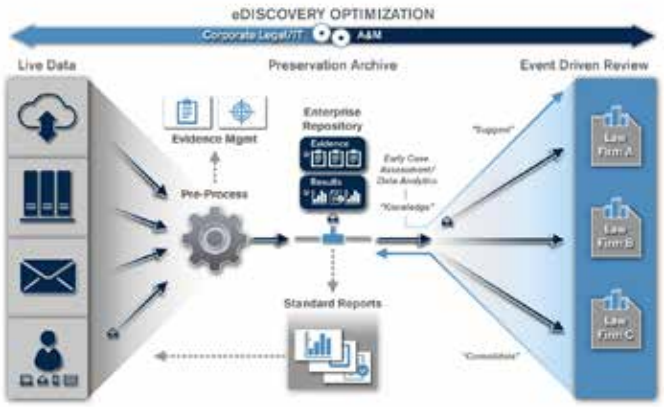




## Technologist / Consultant Perspective (Continued)

3. **Preservation**
   - Identification
   - Interviews with owners – business, IT & SME's
   - Catalogue
   - Preserve
   - Collection
   - Extraction
   - Migration

4. **Operationalize**
   - People
   - Process
   - Technology



## Don't Be Afraid to Go to the Judge

- The amended rules contemplate cooperation and early resolution of discovery disputes, but that's no reason to capitulate on important issues
- Expect to be tested and prepared to call a bluff
- Stand by your best judgement of what's justified / proportional
- Don't assume technical expertise – present in laymen's terms – keep it as simple and straightforward as possible





## Lessons Learned

1. Encourage your client to get organized and understand their IT environment
2. Identify technology SME's or consultants who can be spokespersons
3. Develop a standard, repeatable and defensible process
4. Early on and continuously throughout the matter have IT, business and legal at the table
5. Be specific about cost and burden and request your adversary to be specific as well
6. Defend and challenge "burden"
7. Don't be afraid to go to the judge



AMERICAN BANKRUPTCY INSTITUTE

# 05 Cybersecurity Risks for Insolvency Professionals

ALVAREZ & MARSAL

## Understanding Cybersecurity Risk Pillars

'threat' = capability ⨯ intent | 'risk' = probability ⨯ harm

**Threat**

An action, potential action, or inaction, likely to cause damage, harm or loss.

**Vulnerability**

Specific gaps in the protection of assets that can be exploited by Threats in order to compromise the asset and realize a Risk.

**Risk**

The resulting damage, harm or loss of unmitigated Vulnerability to Threats

## Breach Causality

The number one driver in most cybersecurity breaches is ineffective leadership and culture

**Contributing factors:**

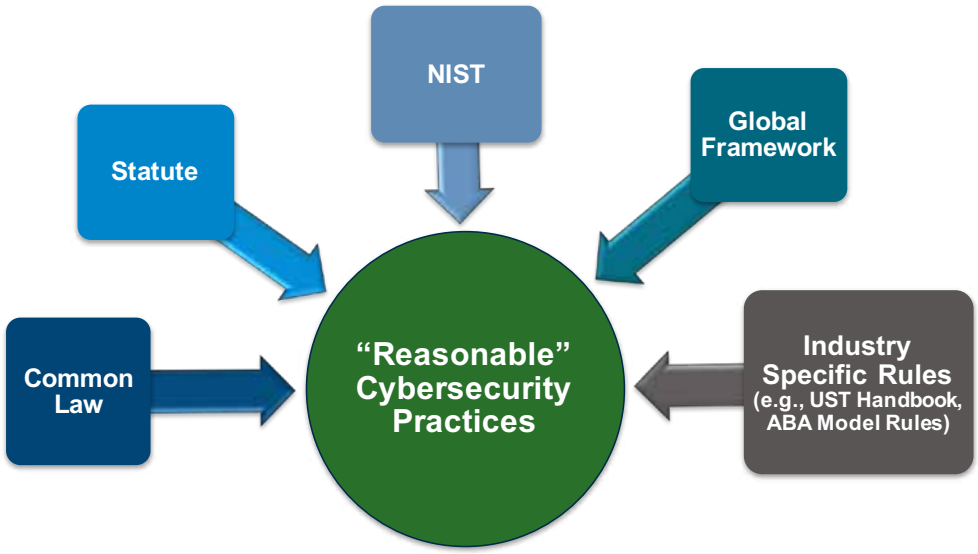
- Cybersecurity awareness that is lacking or under informed
- Refusal to acknowledge threats
- Culture of ignoring risks and vulnerabilities over revenue
- Inexperience
- Hubris

*"Risk comes from not knowing what you are doing."*
– Warren Buffet

41

AMERICAN BANKRUPTCY INSTITUTE

## What are the Standards of Care for Insuring Data Security?

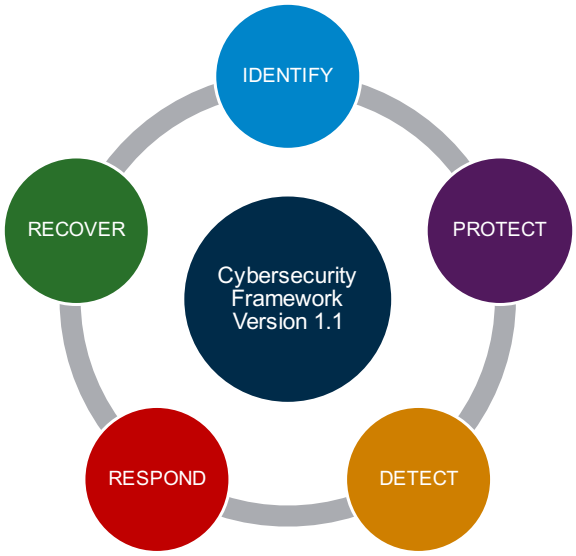



42

AMERICAN BANKRUPTCY INSTITUTE

## Protecting Data – Best Practices

NIST Framework – voluntary standards, guidelines, and best practices to manage cybersecurity-related risk.




43

AMERICAN BANKRUPTCY INSTITUTE

# 06 Tales from the Trenches – Bankruptcy Courts & Technology

ALVAREZ & MARSAL

## Thank You!

### Moderator:

**Hon. Mary Ann Whipple**
United States Bankruptcy Judge
Northern District of Ohio

### Panelists:

**Elizabeth Vandesteeg**

SFGH
Sugar Felsenthal Grais & Helsinger LLP

**Mark Kindy**

A&M

**Megan McKnight**

TEALSTONE LAW



AMERICAN BANKRUPTCY INSTITUTE