AMERICAN BANKRUPTCY INSTITUTE

2021 Winter Leadership Conference

Cybersecurity and Being Secure in Your Practice: How Confident Are You in Your Competency?

Hosted by the Ethics & Professional Compensation and Emerging Industries & Technology Committees

Karim A. Guirguis, Moderator
American Bankruptcy Institute; Alexandria, Va.

Manoj Tandon
Dark Rhino Security; Harrison City, Pa.

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

CONCURRENT SESSION

2021

Cyberethics and Best Practices

ABI Winter Leadership Conference

Dec. 10, 2021

Elizabeth Vandesteeg, Partner at Levenfeld Pearlstein

Ethical Obligations: Sources of Duties and Guidance

- ABA MRPC 1.1 Competence (Cmt. 8)
- ABA MRPC 1.6 Confidentiality of Information
- ABA MRPC 1.15 Safekeeping Property
- ABA MRPC 5.3 (Cmt. 3) Responsibilities Regarding Nonlawyer Assistants
- ABA Formal Opinion 477
- ABA Formal Opinion 483
- ABA Formal Opinion 498

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
- Practically speaking, "[t]his provision will require lawyers to better understand any advances in technology that genuinely relate to competent performance of the lawyer's duties to a client."

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)

The Scope of the Duty of Confidentiality

- The duty of confidentiality is far broader than the narrow duty underpinning the attorney-client privilege
  - A lawyer owes a duty of care in protecting the confidences of a client, even those of a prospective client with whom no attorney-client relationship is formed. See ABA Comm. on Ethics and Professional Responsibility, Formal Op. No. 90-358, Sept. 13, 1990.
    - *United States v. Morrell-Corrada, 343 F Supp 2nd 80, 88 (2004)*

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 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 477

- Seven factors to consider when determining the appropriate level of cybersecurity:
  1. The nature of the threat.
  2. How client confidential info is stored and sent
  3. The use of reasonable electronic security measures.
  4. How electronic communications should be protected.
  5. The need to label client information as privileged and confidential.
  6. The need to train lawyers and nonlawyer assistants.
  7. The need to conduct due diligence on vendors who provide technology services. Guidance in this regard can be found in ABA Formal Opinion 08-451.

ABA Formal Opinion 477
https://www.americanbar.org/content/dam/aba/images/abanews/FormalOpinion477.pdf

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

ABA Formal Opinion 483

- Generally outlines "reasonable" steps the ABA believes lawyers should take in a data breach to meet the obligations set forth in the ABA's Model Rules of Professional Conduct
- Identifies 6 ABA Model Rules that might be implicated in an event of a data breach

1. Model Rule 1.1: Requires lawyers to "provide competent representation to a client," including exercising the requisite "legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."
2. Model Rule 1.4: Requires, among other things, that lawyers "keep the client reasonably informed about the status of the matter" and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation."
3. Model Rule 1.6: Requires that lawyers "not reveal information relating to the representation of a client unless the client gives informed consent" and "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."
4. Model Rule 1.15: Requires lawyers to "appropriately safeguard" clients' documents and property.
5. Model Rule 5.1: Requires that lawyers with "managerial authority in a law firm . . . make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct."
6. Model Rule 5.3: requires that lawyers in supervisory capacities "make reasonable efforts to ensure that [any non-lawyer's] conduct is compatible with the professional obligations of the lawyer."

ABA Formal Opinion 483, cont.

- Key points from the Opinion –
  - Defines "*Data Breach*" - "a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode."
  - broad definition than state and federal breach notification laws
  - *Duty of Competence* – obligation to monitor for a data breach
    - monitoring for incidents, taking appropriate containment and remediation steps, and appropriately investigating the incident.
  - Incident Response Plan – when a breach is detected or suspected, lawyers must act reasonably and promptly to stop the breach and mitigate any damage that may have resulted, an incident response plan should –
    - maintain at least a basic understanding of changes in the law and its practice
    - prepare an incident response plan which addresses how the lawyer or firm will promptly
    - implement internal policies and procedures designed to safeguard confidential client information and critical business systems
    - provide appropriate oversight for any lawyers and non-lawyers

ABA Formal Opinion 483, cont.

- *Duty of Confidentiality* – the unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. several factors to be used in assessing the reasonableness of the lawyer's efforts, include –
    - The sensitivity of the information;
    - cost of employing additional safeguards
    - difficulty of implementing the safeguards
- Notification obligations - obligation to provide notice of an incident in two contexts –
    1. notification to current clients, and
    2. notification to former clients whose data is being maintained in accordance with record retention requirements

ABA formal opinion:
https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf

ABA Formal Opinion 498

- Ethics rules apply regardless of where an attorney practices, whether virtually or not.
    - "A lawyer's virtual practice often occurs when a lawyer at home or on-the-go is working from a location outside the office, but a lawyer's practice may be entirely virtual because there is no requirement in the Model Rules that a lawyer have a brick-and-mortar office. Virtual practice began years ago but has accelerated recently, both because of enhanced technology (and enhanced technology usage by both clients and lawyers) and increased need."

ABA Formal Opinion 498, cont.

- "[w] hether interacting face-to-face or through technology, lawyers must:
  - reasonably consult with the client about the means by which the client's objectives are to be accomplished; ...
  - keep the client reasonably informed about the status of the matter;
  - promptly comply with reasonable requests for information....
- "[L]awyers should have plans in place to ensure responsibilities regarding competence, diligence, and communication are being fulfilled when practicing virtually."

ABA Formal Opinion 498, cont.

- Specifically reminds lawyers to take steps to prevent unauthorized access to confidential information, advising lawyers to "be diligent in installing any security-related updates and using strong passwords, antivirus software, and encryption."
  - In a remote-work environment, lawyers need to be more vigilant about risks in their home/work environment.
  - Home routers should be secured, and lawyers should consider using VPNs when outside the office network.
  - As technology evolves, updates to these systems might be necessary as well.

ABA Formal Opinion 498, cont.

- Accessing Client Files
  - Take care to use systems that allow them to remotely access client files and protect this information from possible data loss.
- Virtual Meetings
  - Opinion 498 reminds lawyers that access to accounts and meetings should only be through strong passwords, and all recordings and transcripts should be secured and only used with client consent.
- Smart Speakers
  - Attorneys should disable the listening capability of devices or services in the home office, such as smart speakers, virtual assistants and other listening-enabled devices (e.g., Siri and Alexa), while communicating about client matters.

ABA Formal Opinion 498, cont.

- Supervision of Technology Use
  - Formal Opinion 498 noted that supervision of the firm's bring-your-own-device policy is particularly important.
- Technology Vendors and 3rd Parties
  - Use a confidentiality agreement with technology vendors and other third-party providers to protect client information.

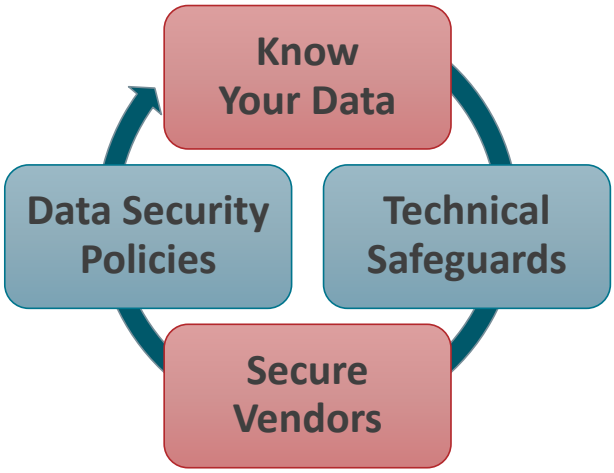
It's Not Just the Law Firm Anymore

- "To reflect the scope of the nonlawyer services now being provided outside of firms," Model Rule 5.3's commentary now references "cloud computing" as an example of modern outside help.

Supervising Third Parties

- A law firm's data security practices are only as strong as its weakest link
- Lawyers must make sure that law firm staff and external business partners understand necessary data security practices and the critical role all parties play in ensuring the protection of client information

Protecting Valuable Client Information



Why We Should Be Careful Using the Word "Breach"

- Using "breach" to describe a data-privacy related incident assumes the incident meets the definition of a security breach which triggers various notification requirements
- An "incident" does not always rise to the level of "breach" (i.e., encryption safe harbor)
- "Incident" is better received by the public than "breach"

Breach & Breach Reporting

What is a breach?	How does a breach occur?	Now what?
• Hacking • Phishing • Malware • Theft • Misuse	• Motive • Opportunity • Weak security • Weak policies	• Respond quickly • Respond appropriately • Preserve evidence

Who Should Be On Your Incident Response Team?

- Because the issue impacts almost every component of the organization, and failure to properly manage can result in both long and short term consequences, the team should include "C" level decision makers in the following areas:
  - Legal
  - IT
  - Risk management/insurance
  - HR
  - Marketing
  - Public relations
  - Compliance & internal audit
  - Physical security
  - Other executive, as appropriate
  - Third party response services (e.g., forensics, privacy counsel, notification)

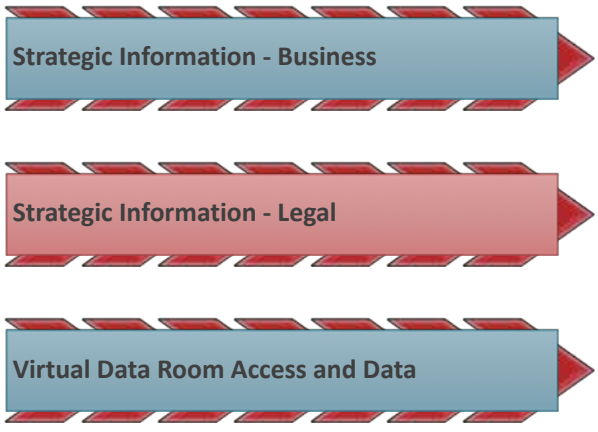
Steps in a Breach Response

Discovery & Reporting	• Identify the incident or potential incident. • Immediately report the incident or threat to the proper party.
Initial Response	• Secure and isolate affected systems to limit further data loss. • Preserve evidence. Convene the Incident Response Team in accordance with this Plan. • Know your role. Coordinate investigation and remediation.
Investigation	• Gather information on the incident. • Consider involving forensics team and outside counsel. • Analyze the cause of the incident and the affected systems. • Analyze legal requirements and liabilities going forward.
Remediation	• Comply with legal requirements including breach notification. • Remove known vulnerabilities; repairing systems. • Respond to third party inquiries. Consider contacting law enforcement.
Post-Incident Review	• Review analysis and notes regarding the incident. • Improve practices as necessary. • Improve policies as necessary.

LEVENFELD PEARLSTEIN, LLC

33

Risky Business for Bankruptcy Counsel



LEVENFELD PEARLSTEIN, LLC

34

Property of the Estate I

- Upon the filing of a bankruptcy petition, the bankruptcy estate is created from the Debtor's property
- Section 541 of the Bankruptcy Code defines what property is included in and excluded from a debtor's bankruptcy estate. See 11 U.S.C. § 541(a)-(f)

Property of the Estate II

- The bankruptcy estate is the pool of assets that is subject to the jurisdiction of the bankruptcy court and from which creditors' claims are paid
- Electronically stored proprietary information can be the most valuable "property of the estate" in many bankruptcy cases

The United States Trustee's Handbook Requirements– Guidance For All of Us

- Chapter 7 trustees must comply with guidelines:
  - imposing specific restrictions on the use of wire transfers
  - requiring specific computer security measures
  - requiring trustees to develop and maintain a business interruption plan
  - requiring 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)

Client Counseling Issues

- The Chapter 7 Trustee or the DIP have fiduciary duties to creditors and other parties in interest
- As a lawyer – what are you client counseling obligations?
- Breach insurance
- Employee policies
- ESI preservation in contemplation of litigation

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

Information Security Program (ISP)

Developing an Information Security Program (ISP)

- What is information security?
  - Refers to processes and methodologies designed and implemented to protect print, electronic, or any other form of information or data, including –
    - Confidential, private, and sensitive information; or
    - Data derived from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption

Developing an Information Security Program (ISP), cont.

- What is an Information Security Program (ISP)?
  - A memorialized set of the company's information security policies, guidelines and procedures
  - Objective is to assess risk, monitor threats, and mitigate cyber security attacks

Developing an Information Security Program (ISP), cont.

- Who needs an ISP?
  - Every company regardless of size
  - Whether or not you deal with PII, your data could still be the target of an attack
    - Your own financial records, key information, or other confidential information could be an attractive target for attackers as they could potentially sell or manipulate in other ways to make a profit

3 Key Components of an Effective ISP

- Threat and vulnerability management
  - Designed to mitigate the risk of an information security breach and meet compliance with regulatory requirements
  - Should cover -
    1. Program governance
    2. Threat management
    3. Vulnerability management

Elements of an Effective ISP

- Purpose
- Scope
- Information security objectives
- Confidentiality, accessibility, and integrity of data
- Authority and access control policy
- Classification of data
- Data support and operations
- Security awareness sessions
- Responsibilities and duties of personnel
- Relevant laws

ISP Purpose

- Establish a general approach to information security
- Detect and forestall the compromise of information security
  - i.e. misuse of data, networks, computer systems and applications
- Protect reputation of the company with respect to its ethical and legal obligations
- Recognize the rights of customers
  - i.e. providing effective mechanism for responding to complaints

ISP Scope

- An effective ISP will cover –
  - All data
  - Programs
  - Systems
  - Facilities
  - Personnel, and
  - Other tech infrastructure

ISP Objectives/Goals

- Companies should have a defined ISP objective(s)
  - Helps measure success and failure of ISP
- Information security systems are deemed to safeguard 3 main objectives –
  - Confidentiality
  - Integrity
  - Availability

ISP Objectives/Goals, cont.

- A well-defined ISP mission statement will include -
  - Company's main function
    - What is it that your security team does for the company?
  - Your primary customers
    - Who is it that your team primarily serves?
  - Protecting the products and services that make up the revenue of your business
  - The geographic location in which you operate, if relevant

ISP Authority and Access Control Policy

- Typically, a security policy has a hierarchical pattern -
  - Senior staff - may have enough authority to decide on what data can be shared and with whom
  - Junior staff - usually bound not to share the little amount of information they have unless explicitly authorized
    - Policies governing senior employees may not be the same policy governing junior employees
  - ISP should address every basic position in the organization with specifications that will clarify their authoritative status

ISP Classification of Data

- Data can have different value and thus may impose separation and specific handling regimes/procedures for each kind of data
- Information classification system is commonly sorted as:
  - High risk class
  - Confidential class
  - Public class

ISP Classification of Data, cont.

- High risk class - generally data protected by state and federal legislation
  - Information covered under The Data Protection Act, HIPAA, FERPA
  - Financial;
  - Payroll; and
  - Personnel (privacy requirements).
- Confidential class - not protected under law, but should be protected against unauthorized disclosure
- Public class - information freely distributed

ISP Security Awareness

- The knowledge and attitude members of the company possess for protection of the information assets of a company
- Providing employees training could help provide employees with information regarding how to collect/use/delete data, maintain data quality, records management, confidentiality, privacy, appropriate utilization of IT systems, correct usage social networking, etc.

ISP Policies & Procedures

- Overall, a company should focus on creating policies and procedures relating to:
  - Data governance and classification
  - Access controls
  - Capacity and performance planning
  - Systems and network security
  - Systems and network monitoring
  - Systems and application development
  - Physical security and environmental controls
  - Risk assessment
  - Incident response
  - Personnel training

LEVENFELD PEARLSTEIN, LLC

55

LEVENFELD PEARLSTEIN, LLC

Elizabeth (Lisa) Vandesteeg

Partner, Financial Services & Restructuring
Email evandesteeg@lplegal.com
Phone 312.476.7650

Lisa Vandesteeg is a Partner in the Financial Services & Restructuring Group at Levenfeld Pearlstein. She focuses on identifying risk exposure and mitigating liability for clients, with a concentration in the areas of bankruptcy, creditors' rights, commercial litigation, and data security and privacy. She represents secured creditors, debtors, unsecured creditors, creditors' committees, landlords, and shareholders in bankruptcy courts throughout U.S, as well as representing clients in civil litigation in federal and state courts.

Her passion is helping clients identify and resolve potential problems related to creditors' rights, troubled businesses, bankruptcy and workouts, and business disputes. She strives to resolve disputes without litigation, but when necessary, she will litigate cases logically and efficiently. She prioritizes client communication and an ongoing understanding of the clients' objectives and what "success" in a particular case looks like so she can create a customized plan of action. Lisa is also qualified as a Certified Information Privacy Professional for the U.S. Private Sector by the International Association of Privacy Professionals, the world's largest information privacy organization. She advises clients on cybersecurity and privacy compliance and regulatory issues. She also guides clients in developing and implementing information security programs that are reasonable and appropriate for their specific business needs and risks, as well as advising them in responding to data breaches.

In addition to her robust legal practice, Lisa is also on the Board of Directors of Chicago Run, an organization that promotes the health and wellness of Chicago children through innovative, engaging, and sustainable youth running programs.

LEVENFELD PEARLSTEIN, LLC

Faculty

Karim A. Guirguis, PMP, CAE is chief operating officer of the American Bankruptcy Institute in Alexandria, Va., the nation's largest association of bankruptcy professionals, comprised of 11,000 members in multidisciplinary roles, including attorneys, bankers, judges, lenders, turnaround specialists and others. Mr. Guirguis provides vision and leadership in transforming and conducting the company's internal and external IT plans. He joined the ABI staff in 2002 after several positions in website architecture and computer animation, most recently with Disney MGM Studios in Florida. Mr. Guirguis's work has earned several awards from his peers, including an Oscar for his work on Finding Nemo, the prestigious Horizon Award for ABI's video honoring its founders, as well as the Webby Award for his work with Tiffany Inc. and Polo.com. He is a regular presenter on cutting-edge technology issues for professional educators such as the American Society of Association Executives, for which he serves on its technology board. Mr. Guirguis received his B.S. in electrical engineering from Cambridge University in England, his Master's in multimedia and animation from George Mason University, and his M.B.A. from Harvard Business School.

Manoj Tandon is currently an equity partner and COO for Dark Rhino Security, Inc. in Harrison City, Pa., which is his fifth involvement with a startup. After spending time helping companies with manufacturing process improvements, in the late 90s he moved to the world of startups and has been involved with five technology and services startups since then. At Dark Rhino Security, Mr. Tandon is responsible for creating value innovation to deliver defense in depth to customers ranging in size from Main Street to Wall Street. He runs a weekly cybersecurity podcast, Security Confidential, which covers broad topics with industry-leading professionals in cybersecurity, including career development, professional best practices, risk-reduction, cyberinsurance, and governance and compliance. Mr. Tandon graduated from The Ohio State University with a degree in aeronautical and astronautical engineering.

Elizabeth B. Vandesteeg, CIPP is a partner in the Financial Services & Restructuring Group at Levenfeld Pearlstein, LLC in Chicago, where she focuses on identifying risk exposure and mitigating liability for clients, with a concentration in the areas of bankruptcy, creditors' rights, commercial litigation, and data security and privacy. She represents secured creditors, debtors, unsecured creditors, creditors' committees, landlords and shareholders in bankruptcy courts throughout U.S., as well as clients in civil litigation in federal and state courts. Her passion is helping clients identify and resolve potential problems related to creditors' rights, troubled businesses, bankruptcy and workouts, and business disputes. Ms. Vandesteeg advises clients on cybersecurity and privacy compliance and regulatory issues. She also guides clients in developing and implementing information security programs that are reasonable and appropriate for their specific business needs and risks, as well as advising them in responding to data breaches, and was instrumental in launching the *ABI Journal*'s Cyber U column. Previously, Ms. Vandesteeg was with Sugar Felsenthal Grais & Helsinger LLP, where she was a partner and member of the firm's Executive Committee. She received her B.A. from Columbia University and her J.D. from Boston College.