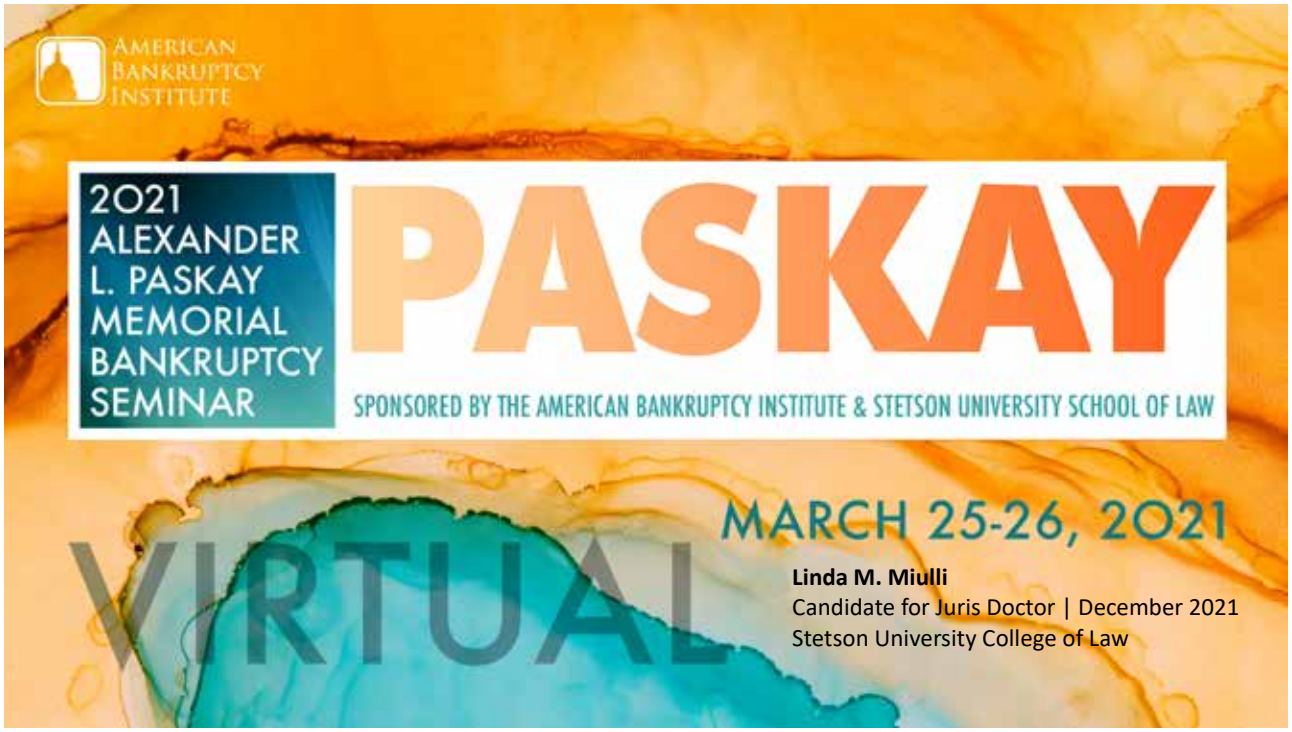
AMERICAN BANKRUPTCY INSTITUTE

2021 Alexander L. Paskay Memorial Virtual Bankruptcy Seminar

Annual Alexander L. Paskay Keynote

Sponsored by Stichter, Riedel, Blain & Postler, PA

James Fama
Former Vice President
Energy Delivery for the Edison Electric Institute (EEI)



Cybersecurity Issues Firms Face

Florida Statutes requiring disclosure of data breaches by businesses in Florida, including law firms, as "Covered Entities":

Florida Information Protection Act (F.S. 501.171) or ("FIPA")

http://www.leg.state.fl.us/statutes/index.cfm?mode=View%20Statutes&SubMenu=1&App_mode=Display_Statute&Search_String=501.171&URL=0500-0599/0501/Sections/0501.171.html

Covered Entities include not just law firms located in Florida, but also any companies, regardless of where they are located or incorporated, that acquire, use, store or maintain the personally identifiable information (PII) of Floridians, as being required to comply.

Florida Information Protection Act (F.S. 501.171) or ("FIPA") cont'd

Law firms are required to notify the Dept. of Legal Affairs for the State of Florida within 30 days from the date the breach of its data is discovered with a detailed list of required information to be disclosed. If the breach affects the personal data of more than 500 Floridians, then those individuals must be notified 'as soon as reasonably practical.'

FIPA also imposes obligations on law firms regardless of whether they suffer a breach or not. Law firms must take reasonable measures to protect and secure data personal information in electronic form and dispose or arrange for the disposal of customer records containing personal information. Such disposal must involve shredding, erasing or otherwise modifying the personal information in the records to make it unreadable or undecipherable.

Florida Information Protection Act (F.S. 501.171) or ("FIPA") cont'd

Law firms who fail to provide required notices under FIPA violate Florida Deceptive and Unfair Trade Practices Act (FDUTPA) and are subject to civil penalties of $1,000 per day for the first 30 days, $50,000 for each 30-day period up to 180 days, and a maximum penalty of $500,000 for violations exceeding 180 days.

ABA Rules

ABA Model Rule 1.6(c) requires that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

ABA Rules

The Florida Bar has several similar ethical provisions in place. The Florida Bar Board of Governors voted in July 2015 to approve the addition of the following language to the comment of Florida Bar Rules of Professional Conduct 4-1.1:

"Competent representation may also involve the association or retention of a non-lawyer advisor of established technological competence in the field in question. Competent representation also involves safeguarding confidential information relating to the representation, including, but not limited to, electronic transmissions and communications."

ABA Rules

Ethics Opinion 00-4 notes that lawyers may practice over the internet if they can do so competently. Ethics Opinion 12-3 allows lawyers to use cloud computing provided they follow the guidelines set forth in the opinion. Lawyers should make sure the technology they use to practice remotely is secure and protects confidential information.

See: https://www.floridabar.org/the-florida-bar-news/ethics-during-covid-19/

Shore v. Johnson & Bell

Clients of the law firm of Johnson & Bell sued the firm claiming its confidential information was at risk because of Defendant's IT security failures. A breach had not actually occurred – the lawsuit related to the firm's negligence in protecting client's confidential information, putting it at risk of exposure.

https://www.westlaw.com/Document/I512d5110fa7911e69f02f3f03f61dd4d/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0

An October American Bar Association report found 29% of law firms reported a security breach, with 1 in 5 saying they weren't sure if there had ever been a breach and 36% reporting past malware infections in their systems. 43% of respondents use file encryption; less than 40% use email encryption, two-factor authentication and intrusion prevention; and less than 30% use full disk encryption and intrusion detection.

https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/

Ransomware Attack: TLA Piper, June, 2017

DLA Piper LLP, one of the largest law firms in the world, had a ransomware attack that infected hundreds of thousands of computers across their platform. The global cyber event encrypted all affected files and requested a ransom of $300 in bitcoin to regain access or avoid threat of deletion. The costs associated with getting its computers back on line and secure ran into the millions.

Ransomware Attack: Grubman Shire Meiselas & Sacks, May, 2020

Grubman Shire Meiselas & Sacks Law firm which offers specialized legal services to people involved in the entertainment and media industry became a victim of a file-encrypting malware where hackers have stolen confidential documents and are threatening to leak those files on the dark web if the victim fails to pay them their demanded ransom. The data stolen allegedly includes contracts, nondisclosure agreements, phone numbers and email addresses, and private correspondence.

A report released in May by security firm BlueVoyant found that 15% of a global sample of thousands of law firms showed signs of compromised networks, and all firms were subject to targeted threat activity.

https://www.prnewswire.com/news-releases/over-15-of-a-global-sample-of-law-firms-show-signs-of-compromise-according-to-bluevoyant-sector-17-report-301065918.html

A LogicForce report surveying 200 firms has found that all firms were subject to hacking attacks. The report also found that only 23% of firms polled had cybersecurity insurance policies.

Insurance Protection

Cybersecurity policies covered direct costs associated with the hack, such as ransom costs, hiring investigators and a legal team to advise in the event.

Personal indemnity policies are designed to protect client data and money – loss of revenue due to business interruption is not always covered. Even the "business interruption" component of a firm's insurance policy would not remediate long-term losses of the hack.

Takeaways:

Employee Training: mandatory seminars, regular training, and phishing test emails are effective in mitigating the risk. Florida has required, since 2014, 3 hours of CLE technology credits for a reason. It's important for law firms (and lawyers) to familiar with how cyberattacks happen.

Incident Response Readiness: Firms should create specific procedures for handling cyberattacks to minimize business interruption and limit potential damages.

Takeaways:

Review Your Cyber Insurance Policy with Your Broker: Most traditional insurance products include some cyber coverage. However, in most instances, the coverage provided in those products is very narrow in scope. Stand-alone cyber insurance policies offer a broad range of first and third-party coverages intended to protect an organization in the event of a ransomware attack. A comprehensive cyber insurance policy is a key element of any cyber risk management program.

Faculty

James Fama is a consultant specializing in electric utility cyber and physical security, business continuity, resilience, reliability, and related federal and state matters. He currently serves on the advisory board of Protect Our Power, a nonprofit supporting electric utility cybersecurity. Previously, Mr. Fama served as vice president of Energy Delivery for the Edison Electric Institute (EEI), the national trade association for investor-owned electric utilities. In this capacity, he was responsible for supporting EEI and its members on electric system reliability, security, business continuity, regulatory and compliance matters. During his 14-year tenure with EEI, Mr. Fama led the industry's efforts to create three nationwide resilience programs: Cyber Mutual Assistance, the National Response Event storm restoration program and the Spare Transformer Equipment Program. Prior to joining EEI, for three years Mr. Fama was Senior Counsel with the Washington, D.C., office of LeBoeuf, Lamb, Greene and MacRae, where he represented various energy companies in mergers, litigation, regulation and other matters. For two years, Mr. Fama was vice president and general counsel for ECWerks, Inc., a Tampa, Fla., IT company specializing in electronic commerce and software development, which is now part of CGI Group, the largest IT company in Canada. He also has served as deputy general counsel for Florida Power Corp. (now Duke Florida) in St. Petersburg, Fla., where he was the officer in charge of Florida Power's legal department. Prior to joining Florida Power, Mr. Fama was assistant general counsel for the Bonneville Power Administration in Portland, Ore., where he was responsible for rate regulation and litigation. He began his career as a trial attorney in the Federal Energy Regulatory Commission's Office of General Counsel. Mr. Fama received his B.A. from the University of Virginia and his J.D. from the University of Baltimore.