BUSINESS BANKRUPTCY COMMITTEE NEWSLETTER

February 2018

In This Issue

Featured Articles

Useful Links

Important Dates

Business Law Section Spring Meeting
April 12-14, 2018
Orlando, FL

Business Law Section Annual Meeting
September 13-15, 2018
Austin, TX

Business Bankruptcy

"Business Bankruptcy Committee: The World's Largest Organization of Bankruptcy Restructuring Lawyers"

Business Law Section Spring Meeting

Business Law Section Spring Meeting
April 12-14, 2018
Orlando, Florida

Save the Date and Plan for Orlando: The ABA Business Law Section's Spring Meeting is in Orlando, Florida. We will be presenting several exciting programs, and providing various networking opportunities for you to enjoy with your colleagues. Our programs will cover a variety of topics to suit your interests, including, but not limited to: thorny franchise insolvency issues; the enforceability of pre-bankruptcy agreements; safety of personal consumer data information in a sale or crisis; family feuds in Chapter 11; and Bankruptcy Code puzzlers, anomalies, riddles and rhymes. We look forward to seeing you in Orlando!

Kathryn R. Heidt Memorial Award Goes To Eric Monzo

By Michael A. Sabella

At this year's Fall Meeting of the ABA Section of the Business Law Business Bankruptcy Committee in Las Vegas, Nevada, the annual Kathryn R. Heidt Memorial Award (the "Heidt Award") was presented to Eric Monzo. The Heidt Award honors the memory of Kathryn Heidt, who at the time of her passing was the chair of the ABA Section of the Business Law's Business Bankruptcy Committee. The Heidt Award recognizes those individuals who embody the qualities that Kathryn herself sought to instill in young lawyers.

In remarks prepared and read at the ceremony, Sandy Mayerson described to the audience all of the qualities that inspired her to nominate Mr. Monzo for this prestigious award. These thoughts were echoed in remarks delivered by Brett Fallon, one of Mr. Monzo's fellow partners at Morris James LLP, to the audience in attendance. Like the late Kathryn Heidt, Mr. Monzo has demonstrated a firm commitment to his family, his practice, his community, and the Business Bankruptcy Committee.

Mr. Monzo graduated with a juris doctorate from Widener University Delaware Law School, with honors in 2002. From there, he went on to clerk for the Honorable Mary Pat Thynge, U.S. Magistrate Judge for the U.S. District Court, District of Delaware. He built upon his education and clerkship with his business restructuring and insolvency practice as a partner at Morris James LLP. Mr. Monzo works with a variety of clients, such as stakeholders, creditors, creditors' committees, indenture trustees, and lender groups. His representation allows him to address restructuring issues that affect a broad range of industries including, but not limited to, construction, energy, finance, healthcare, and retail. In turn, these issues raise jurisdictional and international issues that Mr. Monzo works through in service of his clients.

Committee Meeting and National Conference of Bankruptcy Judges
October 28-31, 2018
San Antonio, TX

Susan Freeman
Chair, Committee on Business Bankruptcy
SFreeman@LRRC.com

Editorial Board

A prolific writer, Mr. Monzo has written articles for various organizations and groups, including the ABA, the ABI, the Business Bankruptcy Committee, Turnaround Management Association, and multiple Delaware bar publications. He is an active member of the Delaware bar, and is a regular speaker before many bar groups. Additionally, Mr. Monzo contributed to the ABA Business Bankruptcy Committee's seminal report on Best Practices on Electronic Discovery Issues in Bankruptcy Cases. It is his contributions to the profession that led to his recognition by both Delaware Today (as one of the state's Top Lawyers for 2016 and 2017), and Delaware Super Lawyers (as a Rising Star in the Business Bankruptcy field for 2013 through 2016).

Beyond the professional realm, Mr. Monzo's commitment to his wife Dana and their three children emulates qualities prized by Kathryn. Mr. Monzo's relationship with his children has led to his work as a guardian and child advocate, as well as his charitable work on behalf of child-centered organizations. Mr. Monzo also gives his time as the Chair of the Ethics Commission for New Castle County, and as the New Castle County Chair of the Combined Campaign for Justice, which assists low-income Delawareans with legal services.

During the award ceremony, Mr. Monzo spoke of his honor in receiving the Heidt Award, and his appreciation for the support from the ABA Business Bankruptcy Committee. Mr. Monzo will continue to assist and lead the ABA Business Bankruptcy Committee as he assumes the role of Vice Chair of the Trust Indentures Subcommittee.

The ABA Business Bankruptcy Committee looks forward to seeing Mr. Monzo's future contributions to the ABA Business Bankruptcy Committee and the broader legal community.

Pro Bono in the Digital Age

By Freddi Macki[i] and Jonathan Petts[ii]

Albert Einstein has been credited with saying: "It has become appallingly obvious that our technology has exceeded our humanity."[iii] Assuming *arguendo* this was true in Einstein's day, the authors posit this statement has not withstood the test of time. To the contrary, as shown below, some of the legal profession's brightest researchers and innovators have used technological advances to provide access to much-needed bankruptcy relief for countless Americans. Technology and humanity can-and must-evolve together.

On October 8, 2017, the Pro Bono Services Subcommittee of the ABA's Business Bankruptcy Committee presented a panel discussion titled *Pro Bono in the Digital Age: The Benefits of Technology and Ethical Issues Implicated By Its Use*. Moderated by the Hon. Elizabeth S. Stong of the U.S. Bankruptcy Court for the Eastern District of New York, the panel featured Warren E. Agin,[iv] Professor Lois R. Lupica,[v] Freddi Mack, and Jonathan Petts. This article recaps the panel's discussion.

Apps for Justice Project

One of the first topics discussed was the "Apps for Justice Project." The Apps for Justice Project, spearheaded by Professor Lupica, aims to disrupt the traditional delivery of legal services to low and moderate income individuals through technology-based tools that can be scaled to fit their needs. According to Professor Lupica, more than four-fifths of the individual legal needs of the poor and a majority of the needs of middle-income Americans remain unmet.

Many individuals are unaware that they even have a legal problem and,

consequently, fail to take any actions whatsoever to resolve those problems. For example, individuals may receive legal documents (such as a summons and complaint or a pre-suit notice) and not understand the jargon and concomitant legal implications.[vi] Even if the individuals realize they have some legal problem, there is still a need for easily accessible, easily digestible, no- or low-cost legal assistance.

The Apps for Justice Project seeks to develop apps that replicate the thinking and actions of an expert on a specific question or task. Machine learning can empower an app to ask questions of the user to collect facts and, using the app's logic, can drive the selection and sequence of further questions, adjusting to the user's answers and the intermediate conclusions already reached. As it collects facts and data, the app continuously and automatically applies all reasoning types to replicate the reasoning of the developer. Then, by applying reasoning to the facts and data, the app reaches intermediate and final conclusions, with explanations as to why it reached those conclusions, much like a human expert would. Based on those conclusions, the app provides customized outputs such as action plans or checklists, summaries, scripts, and customized letters or e-mails.

The Apps for Justice Project has put into practice two apps (the Maine Family Law Helper App and the Maine Tenant's Rights App) to assist Maine residents[vii] with basic landlord-tenant and family law issues. The feedback has been consistently positive, with users describing the apps as "easy," "useful," "simple," and "helpful."

Financial Distress Research Study

Professor Lupica, along with D. James Greiner of Harvard Law School and Dalié Jiménez of the University of Connecticut School of Law, has been gathering empirical data about what helps consumers in financial distress improve their financial lives, with a goal of improving overall consumer financial well-being. The study is the result of a unique partnership among academics, federal and state government liaisons, non-profit service providers and funders, and private sector participants. Consumers may face a vicious cycle of financial distress, which leads to stress, distraction, and low mental performance, which in turn leads to poor decision-making, which itself causes more financial distress. But the study has focused on a "treatment" of self-help: providing the consumer with access to basic information that will allow her to help herself to, for example, defend against collection lawsuits, negotiate with creditors out of court, obtain and correct credit reports, or file a no-asset Chapter 7 bankruptcy case.[viii]

Moreover, the study has found that "access" to resources such as legal counsel and written legal materials (treatises, websites, etc.) may not be the consumer's biggest challenge-rather, it is the "deployment" of the resources and knowledge that poses a significant obstacle for the lay consumer. The study hypothesizes that individuals in collections will have trouble deploying professional legal knowledge. A consumer proceeding *pro se* is expected to have sufficient legal knowledge to defend or bring the claims at issue. Written resources or one-time legal clinic consultations might suffice to provide the consumer with the requisite legal knowledge, but deployment obstacles could prevent the consumer from putting the legal knowledge she gained into practice. Deployment challenges arise as a result of a variety of barriers: cognitive, emotional, behavioral, and psychological; debilitating feelings of shame, guilt, or hopelessness; lack of self-agency; and/or failures in plan-making and plan-implementation. As a result, the study has focused on developing materials that break down these barriers to deployment. For example, consumers have responded positively to cartoons and other visuals that accompany written advice or instructions. Professor Lupica's team has created a go-to character named "Blob" to walk consumers through the presentation of evidence, formation of arguments, what to expect in court or mediation, and even non-legal affirmations, like self-esteem and confidence-boosting exercises to provide empowerment and a sense of agency. Through

these materials, consumers can help themselves both gain access to the legal system, and deploy the legal and financial knowledge in efforts toward a better life.

Upsolve

Millions of low-income Americans are buried in debt from sudden financial shocks like medical illness, job loss, and divorce. Chapter 7 bankruptcy is supposed to be a lifeline for them. Most bankruptcies result from medical illness, job loss, divorce, and small business failure. Our bankruptcy system was designed to give these Americans "a new opportunity in life and a clear field for future effort." *Local Loan Co. v. Hunt*, 292 U.S. 234, 244 (1934). In addition to erasing unsecured debt, Chapter 7 bankruptcy increases one's likelihood of employment by 12.3%, *see* Daphne Chen & Jake Zhao, *The Impact of Personal Bankruptcy on Labor Supply*, 26 Rev. of Econ. Dynamics 40, 40 (Oct. 2017), stops wage garnishment, increases access to banking, credit, and housing, and has low repeat-filing rates. *See* John Golmant & Tom Ulrich, *Repeat Bankruptcy Filings*, 14 Am. Bankr. Inst. L. Rev. 169, 180 (Spring 2006) (over 84% of filers nationwide had never filed before. This percentage is even higher when excluding repeat Chapter 13 filers not at issue here.) In short, it's a powerful poverty-fighting tool.

Unfortunately, this lifeline is broken. The bankruptcy forms contain 70-plus pages of questions using legalese like "unsecured nonpriority debt." They are too hard to complete without help and it costs $1,500 to hire a lawyer, which few Americans can afford. Thus, the only recourse for many is free legal aid from a legal service provider ("LSP"). Unfortunately, very few LSPs handle bankruptcy cases, including because they take so much attorney time -- about 10 hours per case.

It is estimated that more than 10 million American households would benefit from filing a Chapter 7 bankruptcy. *See* Stefania Albanesi & Jaromir Nosal, *Insolvency after the 2005 Bankruptcy Reform*, Fed. Res. Bank of N.Y. Staff Report No. 725 (Apr. 2015); Michelle J. White, *Why Don't More Households File for Bankruptcy?*, 14-2 J.L. Econ. & Org. 205 (1998). Yet, in the year 2016, under half a million did. *Report F-5A*. *U.S. Bankruptcy Courts*, (period ending December 31, 2016), U.S. Cts. (2017), http://www.uscourts.gov/sites/default/files/data_tables/bf_f5a_1231.2016.pdf. Millions are simply priced out of our bankruptcy courts and the chance for a fresh start.These Americans remain buried in debt and face reduced access to banking, credit, employment, and housing. For them, the cycle of poverty continues.

Jonathan Petts, the Executive Director of Upsolve, discussed a solution. Upsolve is a team of lawyers, judges, academics, and technologists founded out of Harvard Law School's Access to Justice Lab in 2016. Upsolve believes in a fresh start to fight poverty and is using academic research and technology to build the first "Turbotax" for Chapter 7.

Here's how it works: a client calls an LSP asking for bankruptcy help. The LSP staff will use Upsolve's screening tool (upsolve.org/intake), designed by leading bankruptcy scholar Henry Sommer, to determine if the client is a good bankruptcy candidate. The LSP staff will also check whether the client is reasonably comfortable using a computer (about half of LSP clients currently are). If so, the client is referred to Upsolve's website (upsolve.org/start) where the client creates an account.

On the website, the client is guided through a mandatory budgeting course. After that, the client answers a questionnaire using cartoons and design principles created by Professor Lupica (discussed above). The questionnaire asks the client everything he or she makes, spends, owes, and owns. The questions were designed with feedback from Chapter 7 trustee and Upsolve advisory board member, Warren Agin.

From those answers, Upsolve's software generates a draft of the required

bankruptcy forms, which are emailed to the LSP. The forms are then reviewed and revised by a pro bono attorney in about one hour. The client signs the forms and takes them to the local bankruptcy court to file. Then, Upsolve's website guides the client through the mandatory debtor education course that the client must complete to obtain a discharge, usually two months later.

In total, Upsolve achieves the same results as a 10-hour full-service representation in under two hours of attorney time. LSPs using Upsolve can multiply the clients they bring out of poverty with a fresh start each year. Since its founding in Harvard Law School's Access to Justice Lab last year, Upsolve has built and tested its prototype software on a shoestring budget. Nearly 1,000 Americans have used Upsolve's website to diagnose their consumer debt problems. And Upsolve's software has successfully filed over 50 test cases for low-income New Yorkers, erasing about $2 million in debt. A few of Upsolve's first users' experiences in New York can be reviewed at http://bit.ly/2tDoEgG.

Ethical Implications

As technology changes, so too does the application of our well-known ABA Model Rules of Professional Conduct. Per the comments to Model Rule 1.1, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Model Rules of Prof'l Conduct r. 1.1 (Am. Bar Ass'n 1983). This includes: (i) the duty to effectively protect privileged and confidential client information in the digital age (*see* Model Rules of Prof'l Conduct r. 1.6 (Am. Bar Ass'n 1983); *see also* ABA Comm'n on Ethics & Prof'l Responsibility, Formal Op. 477R (2017)); (ii) the duty to safeguard clients' digital property (*see* Model Rules of Prof'l Conduct R. 1.15 (Am. Bar Ass'n 1983); *see also* Kathryn A. Thompson, *You Have to Share*, 94 A.B.A. J. 30, 30-31 (Sept. 2008)); and (iii) the duty to preserve electronic data and communications, and to pursue the same through discovery as is required to vindicate a client's cause or endeavor (*see* Model Rules of Prof'l Conduct r. 1.3 & cmt. 1 (Am. Bar Ass'n 1983); *see also* Carol Owen, *The Duty to Preserve:* Victor Stanley *and Its Progeny*, 19 A.B.A. Trial Evidence no. 4 (Summer 2011), at 2-9). At the same time, the provision of limited scope representation, *i.e.*, the "un-bundling" of legal services, as contemplated by the Model Rules of Professional Conduct Rule 1.2(c) is more readily put into practice, as shown by projects like Apps for Justice and Upsolve.

Conclusion

Despite all of the exciting technological developments, practitioners need not fear that they will become redundant in the new legal world. As technology and self-help become more prevalent in no-asset, non-complex cases, LSPs will be able to focus on thornier bankruptcy issues. As a result, the bankruptcy bar will benefit from more robust jurisprudence and scholarship. Simultaneously, low-to-moderate income Americans will have increased access to the fresh start they need. At the risk of sounding overly optimistic, the authors believe that humanity will thrive as technology continues to expand. Einstein, we hope, would be proud.

i. Freddi Mack is an associate in the Miami, FL office of Jones Day. The views and opinions set forth herein are the personal views or opinions of the author; they do not necessarily reflect views or opinions of the law firm with which she is associated.

ii. Jonathan Petts is the co-founder and Executive Director of Upsolve, and is based in New York, NY.

iii. Wikiquote, https://en.wikiquote.org/wiki/Talk:Albert_Einstein (last visited on January 3, 2018).

iv. Warren E. Agin is the founder of Analytic Law, LLC and of counsel to Swiggart & Agin, LLC in Boston, MA. An overview of Mr. Agin's presentation materials can be found at A Simple Guide to Machine Learning in ABA's Business Law Today, February 2017 issue.

v. Lois R. Lupica is the Maine Law Foundation Professor of Law at the University of Maine School of Law.

vi. The Apps for Justice Program recognizes there are two distinct issues for lay persons: (1) access to legal information and (2) implementation of that information. The apps assist with both issues, but primarily with the second issue; knowledge of the apps' availability, and the individual's need therefor, would come from Legal Services organizations, word of mouth, and other sources. The apps' utility presupposes that individuals will first learn that the apps exist and would be helpful to them.

vii. As of the publication date of this article, the apps assume Maine law is the governing law. The Apps for Justice may expand the project in the future.

viii. The two-year-long study is ongoing, but the benefits of self-help treatment are already being seen. The study involves both identifying barriers to self-help and providing resources to facilitate self-help, and then measuring the success of those resources. As such, even before the study is concluded, test subjects are already benefitting from possible "treatments" for self-help.

Third Circuit Adopts Probability Standard In Evaluating Warn Act Unforeseen Business Circumstances Exception

By Patrick J. Reilley and J. Kate Stickles

The WARN Act requires employers to provide employees with 60 days' notice of a plant closing or mass layoff. *See* Worker Adjustment And Retraining Notification (WARN) Act, 29 U.S.C. §§ 2101-2109 (2018). The Act contains certain exceptions, including the "unforeseeable business circumstances" exception, which absolves an employer of liability when the layoff was "caused by business circumstances that were not reasonability foreseeable at the time that notice would have been required." *Id.* § 2102(b)(2)(A). In *Varela v. AE Liquidation, Inc.*, the U.S. Court of Appeals for the Third Circuit addressed the standard to be applied when assessing "reasonable foreseeability" and joined five other circuits in holding that WARN notice is triggered when a mass layoff becomes probable, not merely foreseeable. *Varela v. AE Liquidation, Inc. (In re AE Liquidation, Inc.)*, 866 F.3d 515 (3d Cir. 2017).

Facts of *AE Liquidation*

Chapter 11 debtor Eclipse Aviation Corporation ("Eclipse"), an aircraft manufacturer, agreed to sell the company as a going concern to its largest shareholder, European Technology and Investment Research Center ("ETIRC"). *Id.* at 518. The sale required funding from Vnesheconomban ("VEB"), a state-owned Russian Bank. *Id*. Following Bankruptcy Court approval of the sale on January 23, 2009, VEB became unexpectedly insolvent and required recapitalization by the Russian government. *Id.* at 519-20. In the month following the sale, Eclipse received assurances that funding was imminent. Despite "a roller coaster ride of promises and assurances," including representations from a Russian Governor, the financing never materialized. *Id.* at 520-21. A month after the Bankruptcy Court approved the sale, on February 24, 2009, Eclipse ceased operations, moved to convert the case to a chapter 7 liquidation, and emailed its employees advising that "closing of the sale transaction has stalled and our company is out of time and money," and also notifying them that "the prior furlough had been converted into a layoff, effective February 19th." *Id*. at 522.

Eclipse employees filed a class complaint in the Delaware Bankruptcy Court alleging a violation of the WARN Act for failure to give sixty days' notice prior to the layoff. *Id*. Eclipse asserted that the "unforeseeable business circumstances"

exception barred WARN Act liability. *Id.* The Bankruptcy Court granted summary judgment in Eclipse's favor. *Id*. The District Court affirmed. The decision was appealed to the Third Circuit. *Id*.

The Third Circuit Opinion

After determining that the content of the notice of termination and method of delivery were sufficient under the WARN Act, the Third Circuit considered whether Eclipse was entitled to rely on the unforeseeable business circumstances exception as an affirmative defense to WARN Act liability. *Id.* at 523-25. For the unforeseeable business circumstances exception to apply, an employer must demonstrate that (i) the business circumstances causing the layoff were not reasonably foreseeable; and (ii) those circumstances caused the layoff. *Id*. at 523 (*citing Calloway v. Caraco Pharm. Labs., Ltd.*, 800 F.3d 244, 251 (6th Cir. 2015)). Even if the unforeseeable business circumstances exception applies, the Act requires an employer "give as much notice as is practicable," including "notice after the fact." *Id.*; *see also* 29 U.S.C. § 2102(b)(3) (2018) and 20 C.F.R. § 639.9 (2018).

Addressing causation, the Court presumed when a business is being sold as a going concern, "the sale 'involves the hiring of the seller's employees unless something indicates otherwise,' regardless of whether the seller has expressly contracted for the retention of its employees.'" *Id*. at 526 (*citing Wilson v. Airtherm Prods., Inc*., 436 F.3d 906, 912 (8th Cir. 2006)). Applying this presumption, and considering other evidence, the Court found that "Eclipse's employees would have retained their jobs had the sale been finalized," and "the failure to obtaining financing for that sale was the cause of the layoff." *Id.* at 528.

The Court then considered whether the failure of the sale was reasonably foreseeable before the date Eclipse notified its employees of the layoff. The Court acknowledged that the Act does not define "what makes a business circumstance 'not reasonably foreseeable,'" but noted that the regulations require a "fact-specific inquiry to assess on a case-by-case basis whether, … the employer 'exercise[d] such commercially reasonable business judgment as would a similarly situated employer in predicting the demands of its particular market.'" *Id.* To assess such facts and circumstances, the Third Circuit adopted the probability standard set forth by the Fifth Circuit in *Halkias v. General Dynamics Corp.*, 137 F.3d 333, 336 (5th Cir. 1998)[1] and held that the WARN Act is triggered "when a mass layoff becomes probable-that is, when the objective facts reflect that the layoff was more likely than not. "*Id.* at 530. The Court reasoned that "[t]his standard strikes an appropriate balance in ensuring employees receive the protections the WARN Act was intended to provide without imposing an 'impracticable' burden on employers that could put both them and their employees in harm's way." *Id*. (*citing Halkias*, 137 F.3d at 336).

Applying the "reasonable foreseeability test" to the facts, the Court considered "whether a reasonable jury could find that the exercise of commercially reasonable business judgment required WARN Act notice to be given at some point in the month between the approval of the sale and its ultimate demise." *Id.* at 531. The Court noted funding from VEB never materialized, but recognized that Eclipse received constant assurances that funding was forthcoming. *Id*. at 532. It also noted that although "these assurances may look like empty promises in hindsight," the Court "must consider the decisions Eclipse made based on the information available to it at the time and 'in light of the history of the business and of the industry in which that business operated.'" *Id*. The Court found that Eclipse and ETIRC had a business relationship for many years, ETIRC took an active role in Eclipse's affairs and was committed to Eclipse's survival. *Id*. Considering this history, the Court focused on "the specific assurances Eclipse received regarding ETIRC's funding to assess whether the sale's failure ever crossed the line from possible to probable before February 24, 2009." *Id.* Eclipse received consistent positive reports from credible parties that VEB had been recapitalized, funds had been allocated to the sale, and funding would be

forthcoming in a matter of days and, based on these facts, the Court concluded that "Eclipse had a reliable basis to believe it was more likely than not the funding would receive Prime Minister Putin's final approval on February 21st and be dispersed shortly thereafter." *Id.* at 532-33. Once the February 24 deadline[2] passed with no positive report, Eclipse moved to convert the case and notified its employees. Based on these facts, and in light of the parties' historical relationship, the Court concluded that Eclipse met its burden of demonstrating that the eventual shutdown and layoff of its employees was not probable prior to February 24, 2009. *Id*. at 533. Consequently, Eclipse was entitled to invoke the WARN Act's unforeseeable business circumstances exception. *Id*. at 533-34.

Significance of *AE Liquidation* Opinion

Although the facts and circumstances of the *AE Liquidation* case are unique, and the Court's ruling is fact driven, the decision provides guidance to a company in financial distress facing WARN issues in the Third Circuit. First, the Third Circuit adopted the probability standard for assessing reasonable foreseeability and held that a WARN Act notice must be given when a mass layoff is probable, not foreseeable. The Court emphasized, however, that the probability test is an objective one and "even the most well-intentioned subjective beliefs will not excuse failure to comply with the WARN Act's notice requirement if they are not 'commercially reasonable' in light of the facts that were available to the company in the sixty-day period prior to the layoff." *Id.* at 30 n. 11. Second, the decision is noteworthy because the Court ruled that there is a presumption that a debtor's employees will retain their jobs as part of a sale under section 363 of the Bankruptcy Code. This provides comfort to a debtor employer subject to a going concern sale that it need not prematurely or conditionally issue a WARN Act notice if there is only a possibility of a layoff; rather, the obligation to provide notice is triggered when a layoff becomes more likely than not. Ultimately, the specific facts and circumstances will dictate when an employer is obligated to issue a notice under the WARN Act.

[1] The probability standard has also been adopted by the Sixth, Seventh, Eighth and Tenth Circuits. 866 F.3d at 528 (*citing United Steel Workers of Am. Local 2660 v. U.S. Steel Corp*., 683 F.3d 882, 887 (8th Cir. 2012): *Gross v. Hale-Halsell Co.,* 554 F.3d 870, 876 (10th Cir. 2009); *Roquet v. Arthur Anderson LLP*, 398 F.3d 585, 589 (7th Cir. 2005); *Watson v. Mich. Indus. Holdings, Inc.*, 311 F.3d 760, 765 (6th Cir. 2002)).

[2] A resolution directed Eclipse's management to file a motion to convert the bankruptcy to Chapter 7 liquidation proceedings on February 24 unless a "formal written commitment from the Russian Government" was received. Id. at 522.

Cyberattack: Zombies, Data and Hospitals

By Leslie A. Berkoff

On October 10, 2017, the Healthcare and Non-Profit Sub Committee of the Business Bankruptcy Committee presented a program entitled *Cyberattack: Zombies, Data and Hospitals*, which was co-chaired by Leslie Berkoff of Moritt Hock & Hamroff LLP and Andrew Troop of Pillsbury Winthrop Shaw Pittman LLP. The panel included Ms. Berkoff, Catherine Meyer of Pillsbury Winthrop Shaw Pittman LLP, and David Beltran of BMS, Inc. and was moderated by Natasha Songonuga of Gibbons P.C.

The panel originated from a consensus that it seems like almost every day we read news of hospitals and health care organization settling enforcement actions for potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by disclosing patient information.

According to a 2017 Healthcare Breach Report released by data protection company Bitglass, 328 U.S. health-care firms reported data breaches in 2016, up from 268. *Healthcare Breaches Reach High in 2016, Drop-off in Early* 2017, Bitglass (May 3, 2017, 5:00 AM), https://www.bitglass.com/press-releases/2016-healthcare-breaches-all-time-high. In 2016, HIPAA settlements totaled $22,855,300 from 13 separate healthcare systems across the country. *OCR HIPAA Enforcement: Summary of 2016 HIPAA Settlements*, HIPAA J. (Jan. 12, 2017), http://www.hipaajournal.com/ocr-hipaa-enforcement-summary-2016-hipaa-settlements-8646. During 2017, there were 10 HIPAA settlements totaling over $19 million. *HIPAA Fines Listed by Year*, Compliancy-Group.com, https://compliancy-group.com/hipaa-fines-directory-year/.

The actions giving rise to almost all of these settlements related to human errors: for example, employees clicking on infected links in emails or information being inadvertently uploaded to Google during a system upgrade, both of which introduced some form of hacker-derived malware to extract protected data. *See* Heather Landi, *Report: Healthcare Organizations Struggle with Human Error in Securing PHI*, Healthcare Informatics (Oct. 19, 2017), https://www.healthcare-informatics.com/news-item/cybersecurity/report-healthcare-organizations-struggle-human-error-securing-phi.

However, for those professionals who represent healthcare providers and their business associates in the healthcare data realm, there is a greater concern -- cybersecurity breaches, which can lead to a bankruptcy filing, or which occur during a healthcare bankruptcy or during the purchase of assets from a bankrupt healthcare debtor. According to the Ponemon Institute Cost of Data Breach Studies, healthcare has the highest cost per breach record *i.e.* $363 million in 2015 and $355 million in 2016. *2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute 9 (May 2015), https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF; *2016 Cost of Data Breach Study: Global Analysis*, Ponemon Institute 10 (June 2016), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094 WWEN.

The panel focused on the bankruptcy-related risks faced by hospitals and healthcare organizations from cyberattacks. While most practitioners understand that cybersecurity is an issue, many may not yet have fully focused on the fact that for healthcare organizations this is distinct from the organizations' obligation to protect HIPAA information and raises additional independent obligations and financial obligations.

Under HIPAA, organizations are accountable for the protection of medical and health information. Additional obligations arise under The American Recovery and Reinvestment Act and the Affordable Healthcare Act, which govern the protection of electronic personally identifiable information (" PII"). The Health Information Technology for Economic and Clinical Health Act (HITECH Act) was enacted as part of ARRA to provide incentives for the adoption of electronic health records. Norbert F. Kugele, *HIPAA Goes HITECH: How the HITECH Amendments to HIPAA Impact Employer-Sponsored Health Plans*, 35 MI Tax L. 19 (2009). HITECH also amends the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to include additional protections for individuals' electronic health records. *Id.* Specifically, HITECH: (i) extends the privacy and security provisions of HIPAA to business associates of covered entities; (ii) implements a tiered penalty structure for electronic, paper, and verbal breaches; and (iii) imposes new notification requirements on covered entities. *See* Ariele Yaffee, *Financing the Pulp to Digital Phenomenon*, 7 J. Health & Biomed. L. 325, 340 (2011). Further, the Affordable Care Act of 2010 requires the Secretary of Health and Human Services to ensure that all data collected are protected under privacy protections that as at least as broad as those protections under HITECH and HIPAA. *Id.*

Hospitals and healthcare related facilities possess forms of PII and other data far beyond that of other kinds of businesses including: (i) social security numbers of

patients and spouses or other family members who may be guarantors; (ii) banking information such as checking account numbers, credit card information of patients and spouses, or other family members who may also be guarantors; and (iii) tax returns and financial statements if patients have requested financial leniency. If hackers can obtain social security numbers, then they can obtain other information such as birth dates, spouse or parent names, and addresses all of which can be utilized to create fake identification documents. The hackers then can use these documents to obtain financial loans and incur other obligations in the name of their victims. Insurance information can also be used to procure treatment for unscrupulous third parties or obtain prescriptions, which can in turn be sold onto the black market. Further, healthcare facilities will have research studies and drug trials information, which may have tremendous value both nationally and abroad; this information can be sold on the black-market to blackmail companies or sell to competitors. According to the Medical Data Fraud Alliance, a stolen medical identity can be fifty times more valuable than a social security number alone. Gary R. Gordon, *The Growing Threat of Medical Identity Fraud: A Call to* Action, Medical Identity Fraud Alliance 5 (July 2013), http://medidfraud.org/wp-content/uploads/2013/07/MIFA-Growing-Threat-07232013.pdf. This can lead to a multitude of claims against the facility.

Further, beyond these claims for theft of PII and other data, there is also the significant potential for the direct disruption to the healthcare facilities operations and potential claims that may arise from the same. This past May international headlines were made when one of the largest "ransomware" attacks on records aptly named "WannaCry" "WCry" or "Wanna Decryptor" was transmitted via email targeting vulnerabilities in computer systems. Jeff Parsons, *What is 'Wanna Decryptor'? A Look at the Ransomware that Brought down the NHS*, Mirror (May 17, 2017), https://www.mirror.co.uk/tech/what-wanna-decryptor-look-ransomware-10410236. During this attack, cyber attackers took over computers, encrypted information, then demanded payment of $300 of Bitcoin per machine to unlock the devices. *Id*. The attack impacted seventy-four countries and a wide variety of industries. Lily Hay Newman, *The Ransomware Meltdown*, Wired (May 12, 2017, 2:03 PM), https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/. WannaCry affected some of the world's largest institutions and government agencies, including the United Kingdom's National Health Service, where sixteen hospitals were hit. Russell Brandom, *UK Hospitals Hit with Massive Ransomware Attack*, The Verge (May 12, 2017, 11:36 AM), https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin. Since many of the European hospital systems are centralized, the result was crippling. *See* Nico Hines & Kevin Poulsen, *Hackers Cripple Hospitals with Stolen NSA Malware*, Daily Beast (May 12, 2017, 9:40 PM), https://www.thedailybeast.com/stolen-nsa-tech-shuts-down-hospitals. For some reason, perhaps because the hospital systems in the United States are less centralized, hospitals in the United States were not significantly impacted by this attack. Greg Slabodkin, *Few U.S. Healthcare Organizations Affected by WannaCry*, Health Data Management (May 16, 2017, 7:09 AM), https://www.healthdatamanagement.com/news/us-healthcare-organizations-appear-to-dodge-wannacry-bullet. These attacks impacted healthcare systems in a variety of ways, resulting in the inability of hospitals to provide healthcare to the patients. Russell Brandom, *UK Hospitals Hit with Massive Ransomware Attack*, The Verge (May 12, 2017, 11:36 AM), https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin.

Among other things, the attacks disabled the facilities and inhibited the ability for doctors to access medical records. *Id.* Without access to medical records, hospitals could not access health insurance records to confirm coverage, and, more importantly, medical history could not be obtained, so doctors could not prescribe new scripts or render services because they could not check for contraindications for adverse interactions or allergies. Steven Erlanger, *et al.*, *U.K. Health Service Ignored Warnings for Months*, N.Y. Times (May 12, 2017),

https://www.nytimes.com/2017/05/12/world/europe/nhs-cyberattack-warnings.html. More minor complications resulted in the doctors' inability to update records or communicate with other doctors.

The healthcare industry presents unique opportunities for hackers to access information that is not available in other industries or businesses. For example: (i) medical diagnostic devices provide access across the internet to send out vital statistics to electronic health records in real-time both encrypted and unencrypted; (ii) billing systems utilize electronic transfer systems (iii) hospitals allow patients and visitors to access hospital Wi-Fi as a courtesy so both patients and visitors are putting their data at risk and gaining access to the intranet of the healthcare facility; (iv) hospital email systems are easily susceptible to common threats such as "spear-phishing", which is an email spoofing attack targeting a specific organization or individual which obtains sensitive information; and (v) unsecure employee internet access is often unregulated and poorly monitored such that employees are accessing external sites. *See* Steve Ranger, *The Internet of Things is Making Hospitals More Vulnerable to Hackers* , ZDNet (Nov. 25, 2016), http://www.zdnet.com/article/the-internet-of-things-is-making-hospitals-more-vulnerable-to-hackers/; *Cyber Security Services: Spear-Phishing and Health Care Organizations*, Symantec, https://www.symantec.com/content/dam/symantec/docs/white-papers/cyber-security-services-spear-phishing-and-health-care-organizations-en.pdf. The more medical devices connect to a hospital's internet, the more the risk of attacks increases. *Id*.

Last year, ForeScout Technologies surveyed IT professionals worldwide who are responsible for enterprise communication's networks regarding their individual view as to security issues and the key takeaways were: (i) only thirty percent are confident that they really know what is on their network; (ii) many who initially thought they had no devices which were connected to the internet and which would then be at risk for attack discovered that they had Internet of Things ("IOT") devices; and (iii) only forty-four percent of the respondents to the survey had a known policy for addressing IOT. Steven Taylor, *The Internet of Things Isn't Coming. It's Here.*, ForeScout (2016), https://www.forescout.com/wp-content/uploads/2016/06/ForeScout-Webtorials-IoT-Security-Survey-Results-June-2016.pdf.

In preparing security plans to address cyber security threats, most measures appear to be aimed at protecting HIPAA, not at device security. Many mission critical systems are out of date. In fact, hospitals tend to spend less than 6% percent of their budget on cybersecurity. See *Cybersecurity in Healthcare: Why It's Not Enough, Why It Can't Wait,* Symantec, https://www.symantec.com/content/dam/symantec/docs/infographics/symantec-healthcare-it-security-risk-management-study-en.pdf. In 2015, nearly half of the hospitals surveyed stated that their fiscal budget for cybersecurity threats was less than $500,000. *46% of Hospitals Spend Less than $500k on Cybersecurity: 3 Things to Know,* Becker's Health IT & CIO Review (Nov. 24, 2015), https://www.beckershospitalreview.com/healthcare-information-technology/46-of-hospitals-spend-less-than-500k-on-cybersecurity-3-things-to-know.html. There is also little attention being paid to updating software or implementing simple patches.

The breaches identified above could force an entity to contemplate or file for bankruptcy because of an influx of claims. *See* Arianna Etemadieh, *HIPAA Violations Can Bankrupt Your Business- Learning from 21CO's $2.3M Fine*, Paubox (Jan. 4, 2018), https://www.paubox.com/blog/hipaa-violations-can-bankrupt-business-learning-21cos-2-3m-fine. For example, WannaCry was the indirect result of a failure to perform certain upgrades and implement patches. *See* Russell Brandom, *Is Microsoft to Blame for the Largest Ransomware Attacks in Internet History?* The Verge (May 15, 2017), https://www.theverge.com/2017/5/15/15641198/microsoft-ransomware-wannacry-

security-patch-upgrade-wannacrypt. Individuals who have had their privacy breached, or their personal data hacked, or utilized by third parties may have a basis to sue the medical facilities, or their officers or directors, for failing to take proper precautions. Patient injury or death due to compromised devices, systems or technology could lead to a potential rise in class actions and claims against the facilities. There can also be significant fines levied by HIPAA and other regulatory statutes. *See*, *e.g.*, *New York Hospital Fined $2.2 Million for Unauthorized Filming of* Patients, HIPAA J. (Apr. 22, 2016), https://www.hipaajournal.com/new-york-hospital-fined-2-2-million-for-unauthorized-filming-of-patients-3402/. Thus, healthcare facilities that suffer from cyberattacks have an increased chance to file for bankruptcy. The financial and operational risks from a cyberattack would also be exacerbated in bankruptcy, although to date so far none have occurred post-petition.

The concomitant loss of public confidence and trust when these kinds of attacks occur often result in the loss of revenue from the public who will seek alternative venues for treatment. Moreover, insurance companies may consider the failure to protect this data a basis to stop reimbursements. Loss of revenue may lead to loss of independent funding. Lenders to the facility may consider any or all of these to be a breach of an underlying loan covenant as a result of disruption of operations and loss of patient information. All of these events may stress an already financially stressed healthcare provider.

The cost of these suits can be enormous. For example, in the U.S., HIPAA settlements totaled over $19 million from breaches of confidential information in 2017. Ed Cicerone, *Stay Safe: Keeping Your Practice Resistant to Cyber* Attacks, Nextech (Nov. 29, 2017), http://www.nextech.com/blog/keeping-your-practice-resistant-to-cyber-attacks. In June, Anthem, the largest U.S. health insurance company, settled a multi-district lawsuit after the personal information of 78.8 million people was stolen during a 2015 cyberattack for $115 million. In the bankruptcy case *21st Oncology Holdings, Inc.*, pending in the Southern District of New York, 17-22770 (RDD), a class action was filed on behalf of over two million current and former patients of the debtor who had their personal information compromised while undergoing cancer treatment at the facility. The claims assert that the loss was due to the company's failure to enforce sufficient security protocols and procedures and that the company did not discover the breach, but rather the FBI informed the company that the information was posted on the Dark Web. In December 2017, 21st Century Oncology, Inc. agreed to pay approximately $2.3 million in lieu of civil penalties for HIPAA violations, which was approved by a bankruptcy court. Erin Dietsche, 21st Century Oncology Agrees to Pay $2.3M as Part of Latest HIPAA Settlement, MEDCITYNEWS (Jan. 2, 2018, 1:44 PM), https://medcitynews.com/2018/01/21st-century-oncology.

Healthcare systems have an obligation to take reasonable care to protect private customer information. Focusing on these issues is also part of the responsibility of the officers and directors of a facility. Yet the cybersecurity protections do not seem to be in place. While healthcare providers are universally switching over to electronic data, the security of this information has not matched its growth. Financial services industries devote in excess of ten percent of their annual IT budgets to cybersecurity while the health care industry is less than five percent. Given that these facilities often have outdated IT systems and a wealth of confidential patient data, hospitals remain a particularly tempting target. As healthcare budgets shrink, healthcare providers must focus on preparing and protecting against further attacks. While it may not be possible to replace all outdated equipment, some steps can be taken. One thing is clear, as these attacks continue to increase; the concomitant risk grows, leading a shaky industry to perhaps tip more into the insolvency zone.

In conclusion, the panel recommended some steps to take which included ensuring that cash collateral and debtor-in-possession financing orders: (i) provide funds to protect client information and/or to address an attack; (ii) provide

funds perhaps in a carve-out in event of liquidation or conversion; (iii) a Patient Care Ombudsman who can work with a debtor to firm up protocols for these issues and secure funds; and (iv) secure payment for insurance to cover these issues to perhaps avoid claims for post-petition concerns, should be considered as part of any bankruptcy planning or budgeting.

Submit Article for the Business Bankruptcy Newsletter

The Business Bankruptcy Committee invites you to submit articles for possible publication in future issues. The articles do not need to be long or in-depth, and it is a great way to get involved in the Business Bankruptcy Committee. Articles can survey the law nationally or locally, discuss particular business bankruptcy issues, or examine a specific case. If you are interested in submitting an article, please contact Newsletter Editor-in-Chief, Krista L. Kulp at KKulp@moritthock.com, or Co-Editor-In-Chief, Michael A. Sabella at MSabella@bakerlaw.com.