AMERICAN BANKRUPTCY INSTITUTE
JOURNAL
The Essential Resource for Today's Busy Insolvency Professional

Beyond the Quill

By Eric Kurtzman and Samuel R. Maizel

Challenges in Protecting Confidential Data in Bankruptcy

Eric Kurtzman
Stretto; Irvine, Calif.

Samuel R. Maizel
Dentons US LLP
Los Angeles

Eric Kurtzman is CEO of Stretto and is based in Irvine, Calif. Samuel Maizel is a partner in Dentons US LLP's Restructuring, Insolvency and Bankruptcy Group in Los Angeles.

Editor's Note: *To stay up to date on the COVID-19 pandemic, be sure to bookmark ABI's Coronavirus Resources for Bankruptcy Professionals website (abi.org/covid19).*

As the global COVID-19 pandemic continues its significant impact on the U.S. economy, many restructuring experts expect a significant increase in consumer and corporate restructurings and bankruptcies, commencing over the last quarter of 2020 and through the end of 2021. The bankruptcy system's capacity to manage the expected inflow relies, in part, on public access to court documents, ensuring transparency and accountability for all involved parties.

In no small part due to the widespread use of commercial noticing agents (which make all documents filed in a case available over the internet at no cost), the public's access to court documents has never been better, even if the physical access to courthouses has never been worse. Unfortunately, there's a balance required between providing sufficient public access to information via the internet and maintaining data security to prevent bad actors from accessing personally identifiable information (PII), as defined by § 101(41A) of the Bankruptcy Code,[1] or other sensitive case data.

As the restructuring community prepares for a period of intense activity, restructuring professionals need to take a step back and audit internal systems to ensure that attorneys, financial advisors and other professionals take the appropriate steps to safeguard sensitive information. The threats are ever-present and evolve every day; well-positioned professionals must continuously evaluate the risks to remain one step ahead, as the security of clients' data is paramount. For example, claims agents should employ a comprehensive and multi-layered approach to data security under the auspices of a chief information security officer who continuously monitors and hardens the environment and controls to continuously mitigate the threat of a system penetration or breach. Even with such heightened security standards, professionals holding PII should engage in annual audits from third parties to review and validate their programmatic approach to data security.

Proper preparation includes comparing data-security platforms to the relevant state, federal and (where applicable) international privacy laws. This article limits its discussion to laws impacting bankruptcy cases and provides a brief overview of the industries most often impacted by data-security violations.

Laws Governing Bankruptcy Cases and PII

Section 107(a) states that papers filed in a bankruptcy proceeding are "public records" that may be examined by anyone. However, pursuant to § 107(c)(1), certain types of information might be protected if the bankruptcy court finds that disclosure would unduly risk a person to identity theft[2] or other unlawful injury. In addition, § 363(b)(1) provides that the sale of PII can only occur under two distinct circumstances: (1) if the proposed sale of PII is consistent with the debtor's pre-existing policies on the sale of PII; or (2) the bankruptcy court appoints a consumer privacy ombudsman

1 All references to sections herein are to sections of the Bankruptcy Code, 11 U.S.C. § 101-1532, as amended.

2 "Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain." "Identity Theft," U.S. Dep't of Justice, *available at* justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud (unless otherwise specified, all links in this article were last visited on Dec. 1, 2020).

(CPO),[3] and the court approves the sale of the PII after "(i) giving due consideration to the facts, circumstances, and conditions of such sale or such lease; and (ii) finding that no showing was made that such sale or such lease would violate applicable nonbankruptcy law."

Rule 9037 of the Federal Rules of Bankruptcy Procedure requires certain redactions on filing documents — whether electronic or paper — containing an individual's Social Security number or birth date; the name of an individual, other than the debtor, known to be and identified as a minor; a taxpayer-identification number; or a financial account number. When documents include this specific type of PII, the filing may include only limited portions of this data as follows: the last four digits of the Social Security number, taxpayer-identification number or financial account number; the year of the individual's birth; and the minor's initials.

Along with the aforementioned protections, certain local laws create an additional layer of enforcement and responsibility when it comes to protecting PII. For example, the Local Bankruptcy Rules of the Eastern District of Texas state that the debtor and debtor's counsel are solely responsible for redacting personal identifiers, that the court will not review documents for compliance with this particular rule, and that parties who fail to redact these personal identifiers might be subjected to disciplinary acts by the court.[4]

Various privacy statutes are commonly raised in connection with the collection and use of PII in the bankruptcy process. For example, the Federal Trade Commission Act prohibits unfair or deceptive acts or practices in or affecting commerce.[5] If a debtor seeks to sell its PII in a manner inconsistent with its pre-existing information privacy policies, the Federal Trade Commission (FTC) will likely treat that as a violation of the FTC Act as a deceptive practice.

Perhaps one of the most impactful privacy regulations that arises in bankruptcy cases is the Health Insurance Portability and Accountability Act (HIPAA).[6] There are two basic rules under HIPAA concerning the security and privacy of "protected health information" (PHI). The "Privacy Rule" sets standards for when PHI may be used and disclosed. The "Security Rule" specifies safeguards and processes with which covered entities must comply in order to protect and safeguard their PHI. HIPAA must be considered in preparing and executing every health care bankruptcy case. For example, information identifying patients is considered PHI, so including patients in the list of 20 largest creditors required at the commencement of the bankruptcy case, or in the matrix of creditors, likely violates HIPAA. In addition, HIPAA considerations arise in the context of a sale of a health care industry entity, because inevitably PHI will be conveyed to the buyer of any operating health care entity.

On the international stage, the General Data Protection Regulation (GDPR) impacts organizations if those entities target or collect the personal data of European Union (EU) citizens.[7] Regardless of whether a company has offices or employees located in the EU, or transacts in the EU, companies must be compliant. "Personal data" under the GDPR includes an individual's name, address, bank details, religion, race, mental or physical characteristics, a person's IP address, web cookies, and contacts if they identify an individual.

The GDPR also places equal liability on organizations that own the data and external service providers that help manage individuals' data; thus, a third party whose practices do not comply with GDPR results in the organization not being compliant as well. Organizations and third-party contractors can effectively comply with the GDPR by implementing technical and operational protocols to protect PII, which include — but are not limited to — encrypting or anonymizing personal data whenever possible; developing and implementing data-protection impact assessments; and having a process in place to notify authorities and data subjects in the event of a security breach.

A debtor who ignores these privacy rules risks creating administrative expenses for its estate. For example, a health care industry debtor that improperly disposes of PHI can be subject to significant fines by the U.S. Department of Health and Human Services Office of Civil Rights. In addition, many states have similar laws, and attorneys general can bring actions against violators of state laws protecting PHI.[8] The fines can be in the millions of dollars,[9] and if the breach occurs post-petition, it might be treated as an expense of the administration of the case, which would have to be paid in full to confirm a reorganization plan.[10]

Industries Impacted Most by Privacy Breaches

The existence of PII and the difficulties in protecting it appear more often in certain types of bankruptcy cases. Perhaps at the top of the list are health care bankruptcy filings, which often include a significant amount of PII in the form of patients' medical records. In addition to personal medical files, other records such as billing statements can include the patient's name and address and a summary of the medical services that the patient received, as well as the name of the patient's insurance company and the patient-subscriber number.

While less common, bankruptcy cases that include sexual abuse claims give rise to a tremendous responsibility to protect relevant parties' PII from public access. The Diocese of Rockville Centre on Long Island recently became the largest American diocese to file for chapter 11 after being named in more than 200 sexual abuse lawsuits,[11] and the Catholic Diocese of Buffalo filed for bankruptcy protection in 2020.[12] In each of these cases, the bankruptcy professionals and related third parties involved are required to exercise an

3 A CPO is appointed pursuant to § 332, and must be appointed at least seven days prior to any hearing on the sale of PII. The CPO also has standing to appear at the hearing and provide information on the proposed sale.

4 Local Bankruptcy Rule of the Eastern District of Texas Rule 1007-1(c).

5 15 U.S.C. § 45.

6 Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191.

7 For more information, visit gdpr-info.eu.

8 *See, e.g.*, "Texas Seeks Civil Penalties for Improper Disposal of PHI," NetSec (Nov. 25, 2015), *available at* netsec.news/civil-penalties-for-improper-disposal-of-phi.

9 *See, e.g.*, "HIPAA Violation Fines," HIPAA Guide (March 14, 2019), *available at* hipaaguide.net/hipaa-violation-fines.

10 *Compare Cumberland Farms Inc. v. Fla. Dept. of Env'tl Prot.*, 116 F.3d 16, 21 (1st Cir. 1997) (holding that penalty imposed by government agency for failure to follow Florida's environmental laws was accorded administrative expense status), *with In re Allen Care Centers Inc.*, 96 F.3d 1328, 1330-31 (9th Cir. 1996) (holding that costs incurred by state agency in course of transferring residents to another facility were not incurred to remedy a violation of health or safety laws and, therefore, not administrative expense).

11 *In re The Roman Catholic Diocese of Rockville Centre, New York*, Case No. 20-10322 (Bankr. S.D.N.Y.), *available at* dm.epiq11.com/case/rdrockville/info.

12 *In re The Diocese of Buffalo, N.Y.*, Case No. 20-10322 (Bankr. W.D.N.Y.), *available at* case.stretto.com/dioceseofbuffalo.

abundance of caution to protect the PII of the sexual-abuse victims. The PII of minors in bankruptcy cases involving similar issues, including the Boy Scouts of America[13] and USA Gymnastics,[14] require heightened protection as well.

Retail companies also collect an enormous amount of data. They track individuals' names and addresses, credit card information, purchase histories and a variety of other information. This data represents a valuable asset, therefore many retail debtors may seek to sell their customers' PII as part of their liquidation process. Debtors may attempt to do this without the customers' knowledge and/or consent and often in direct violation of the retailer's own privacy policy, which can specifically state that the retailer will not sell such information to a third party.

When Toysmart.com filed for chapter 11 protection in 2000 and attempted to sell its customer data during the process, the FTC sought to block Toysmart.com's sale and eventually reached a settlement that provided a framework for future sales of PII. That settlement allowed the sale, provided that the PII (1) was not sold as a stand-alone asset; (2) was only sold to a purchaser engaged in substantially the same lines of business as Toysmart.com; and (3) was only sold to a purchaser who agreed to be bound by and adhere to the terms of Toysmart.com's existing privacy policy and to obtain affirmative (opt-in) consent from consumers for any material changes to the policy that affect information collected under the existing Toysmart.com policy.[15]

More recently, RadioShack Corp. routinely collected customers' names, physical and email addresses, payment card numbers, purchase history and other PII. This information was collected under its privacy policy, which indicated that it would not sell its mailing list or sell any of its consumer information "to anyone at any time." Notwithstanding that policy, after filing for chapter 11 protection in 2015, RadioShack offered to auction off its consumer information (in addition to its trademarks, patents and leases).

The FTC and multiple state attorneys general intervened to block the sale of consumer PII by RadioShack.[16] In this case, the CPO recommended that the sale proceed with limited conditions. In part, the CPO recommended that the sale not include customers' credit or debit card numbers, Social Security numbers, telephone numbers or dates of birth. The CPO suggested, and the sale was ultimately approved on those terms, that RadioShack: (1) only include email addresses from customers active within two years prior to the sale; (2) with respect to whom RadioShack had provided an opt-out option prior to the transfer; and (3) even then only if the buyer agreed not to sell the email addresses to or share them with any third party, and to otherwise abide by RadioShack's privacy policy.

Conclusion

In the normal course of business, individuals and companies face increased pressure to protect PII from increasingly nefarious characters. When insolvency proceedings introduce bankruptcy-related stresses to these data-security protocols, the mixture of international, federal and local laws can give rise to administrative headaches as professionals seek to ensure compliance. Simply put, the underlying bankruptcy principle of facilitating debtor reorganization or rehabilitation does not necessarily outweigh a consumer's implicit right to privacy.

Claims agents, at the front line of notice, should work with debtor's counsel to flag HIPAA, GDPR and other PII concerns on a case-by-case basis, and should have systems in place to navigate data-privacy issues as they are identified. In sexual abuse cases, health care cases and otherwise, upon the request of the debtor, claims agents should redact personal information from claims and other potentially public-facing documents; it is incumbent upon claims agents to have systems capable of efficiently doing so. More importantly, claims agent systems should be integrated to prevent unintended exposure when creditor data is propagated throughout other case activities (*e.g.*, the claims agent's system should redact the creditor matrix to prevent displaying PII in the claims register, and subsequently affidavits of service).

Further, if patients are going to be listed as potential creditors and included in the matrix of creditors, those names and addresses are usually filed under seal to preserve their privacy and comply with HIPAA. In addition, in the instructions provided to creditors for filing claims, it might be useful to include a reminder that if they are submitting a claim that would otherwise be supported by HIPAA-protected materials, they should not file those publicly but rather arrange with the debtor to provide that information separately. Finally, in objecting to claims, debtors must be mindful not to include HIPAA-protected materials in any filings; rather, such material should be filed, if at all, under seal.

Although court documents are public record and facilitate transparency and accountability for all related parties, PII (when included in bankruptcy filings) requires specific protections to combat instances of identity theft and/or individual injury due to its sensitive nature. While bankruptcy-related PII is more commonly seen in certain market-sector cases, best practices across the restructuring industry include internally maintaining constant vigilance in data security and externally holding up professionals' advice to restructuring clients against the backdrop of data-security laws to ensure that such professionals appropriately navigate multiple governing regulations. With the anticipated uptick in both consumer and corporate filings on the horizon, bankruptcy professionals should be familiar with all of the laws pertaining to protecting PII in bankruptcy matters so they have adequate resources to ensure compliance while adhering to competing administrative requirements. abi

Reprinted with permission from the ABI Journal, Vol. XL, No. 1, January 2021.

13 *In re The Boy Scouts of Am.*, Case No. 20-10343 (Bankr. D. Del.), *available at* cases.omniagentsolutions.com/bsa.

14 *In re USA Gymnastics*, Case No. 18-09108 (Bankr. S.D. Ind.),*available at* cases.omniagentsolutions.com/usagymnastics.

15 Stipulation and Order Establishing Conditions for the Sale of Customer Information in the *Toysmart.com* case, *available at* ftc.gov/sites/default/files/documents/cases/toysmarttbankruptcy.1.htm.

16 *See* Letter from FTC to Elise Frejka, dated May 16, 2015, *available at* ftc.gov/system/files/documents/public_statements/643291/150518radioshackletter.pdf.