Privacy in an Open Forum: Managing Sensitive Information in Bankruptcy Cases

Authors: Brad Knapp, Abigail Ryan, Elise Frejka

National Conference of Bankruptcy Judges Annual Meeting, October 9, 2026

Bankruptcy is, by design, a transparent process. Debtors are expected to provide full and accurate disclosure to allow courts, creditors, and other stakeholders to evaluate assets and liabilities and participate fully in the reorganization or liquidation. That transparency, however, often collides with legitimate concerns about privacy and data protection. Debtors may hold vast quantities of personally identifiable information ("PII") and highly sensitive commercial data. Creditors and other parties in interest may also be exposed when their information surfaces in schedules, claims, or sale processes.

This paper addresses four key topics at the intersection of bankruptcy and privacy:

- What private information is "out there?"
- What protection does the Bankruptcy Code provide in an otherwise transparent process?
- What are the best practices in selecting and involving Consumer Privacy Ombudsmen?
- What should practitioners consider regarding handling sensitive information during sales processes?

The paper concludes with a summary chart that distills the core issues, applicable protections, and practical takeaways from the perspective of key participants in the bankruptcy process.

1. What Private Information Is "Out There?"

A. The Golden Age of Data Collection

At no time in the history of the world has more data been freely offered, collected, and stored than the present. Everyone carries around devices in which they constantly transmit information about their location, preferences, finances, contacts, and habits. The abundance of data collection and substantial value attributable to data makes an understanding of privacy protections essential.

B. Sensitive Information in the Bankruptcy Process

Bankruptcy cases and mandatory bankruptcy filings routinely involve sensitive information involving the debtor itself, the debtor's customers, or the debtor's employees. In certain industries—such as health care—this information can extend to very personal patient information. Types of information include:

- **Consumer data**. Debtors maintain, or control through a third-party payment processor, significant consumer information as far ranging as consumer bank

251677253v1

account and financial information to, in the case of 23andMe, genetic information. In the healthcare space, consumer data includes patient information and medical records. Additionally, state law, such as the California Consumer Privacy Act of 2018, may require additional protections. Consumer identities and other private information can be exposed in creditor matrices and data rooms related to sale processes.

- **Employee data.** Employees are almost always creditors. Disclosure of employee identity and contact information may expose employees to any number of harmful communications. In an extreme example, a domestic abuse survivor was allegedly identified by her abuser when her address appeared in a creditor matrix. *See In re Charming Charlie Holdings, Inc.*, No. 19-11534 (Bankr. D. Del. Jul. 11, 2019) [Doc. No. 4].

- **Commercially sensitive information.** Particularly in sale situations, debtors often produce extremely sensitive information regarding their assets, trade secrets, customer list, and other proprietary information that is relevant for potential buyers.

- **Litigation materials.** The increased frequency of bankruptcy filings by debtors addressing substantial tort claims has heightened concerns regarding litigation materials and disclosure of creditors who hold litigation claims. Particularly in bankruptcies involving sexual abuse claims, debtors may hold extremely sensitive information regarding claimants' abuse allegations of confidential prepetition claims. Debtor information regarding perpetrators and internal investigations may also contain information regarding details of sexual abuse and the identity of claimants.

2. What Protections the Bankruptcy Code Provides for Information in an Otherwise Open Process

A. Transparency as the Baseline: Section 107(a)

The Bankruptcy Code contains provisions providing a presumption of openness. Section 107(a) provides: "Except as provided in subsections (b) and (c) and subject to section 112, a paper filed in a case under this title and the dockets of a bankruptcy court are public records and open to examination by an entity at reasonable times without charge." 11 U.S.C. § 107(a). Openness is assumed, and a party trying to protect documents must demonstrate "that the interest in secrecy outweighs the presumption in favor of access." *See In re Continental Airlines*, 150 B.R. 334, 340 (D. Del. 1993) (internal citation omitted). The presumption of open records "is of special importance in the bankruptcy arena, as unrestricted access to judicial records offers confidence among creditors regarding the fairness of the bankruptcy system." *In re Gitto Global Corp.*, 422, F.3d 1, 7 (1st Cir. 2005) (quoting *In re Crawford*, 194 F.3d 954, 960 (9th Cir. 1999)). In addition to these policy considerations, "on a purely practical level, the sealing of court records inflicts a costly nuisance on the judicial system," due to the "[m]echanical and logistical problems of sealing the files, finding extra space in the vault, satisfying all the handling requirements, plus the related direct and indirect costs . . ." *In re Orion Pictures Corp.*, 21 F.3d 24, 26 (2d Cir. 1994). For all these reasons, practitioners seeking to protect information face a burden to demonstrate that matter should be protected.

B. Protections under Section 107(b) and (c)

Section 107(b) carves out narrow but mandatory exceptions to the general rule of access: "On request of a party in interest, the bankruptcy court shall, and on the bankruptcy court's own motion, the bankruptcy court may (1) protect an entity with respect to a trade secret or confidential research, development, or commercial information; or (2) protect a person with respect to scandalous or defamatory matter contained in a paper filed in a case under this title." 11 U.S.C. § 107(b).

Section 107(c) provides further protection for certain "means of identification" and personal data if the court finds that disclosure of the personal information "would create undue risk of identity theft or other unlawful injury to the individual or the individual's property." Bankruptcy Courts have used this section to expand personal protections now that "[w]e live in a new age in which the theft of personal identification is a real risk, as is injury to persons who, for personal reasons, seek to have their addresses withheld." Hr'g Tr. at 60:22-25, *In re Forever 21, Inc.*, No. 19-12122 (KG) (Bankr. D. Del. Dec. 19, 2019). As a result of these risks, allowing broad redactions has become a nearly standard approach to protect individuals from potential harm. *See, e.g.*, *In re Anthology, Inc.*, Case No. 25-90498 (Bankr. S.D. Tex. Sept. 30, 2025); *In re F21 Opco, LLC*, Case No. 25-10469 (Bankr. D. Del. Mar. 18, 2025).

i. Confidential Commercial Information

Section 107(b)(1) provides for the protection of "trade secret or confidential research, development, or commercial information." This protection is mandatory: in other words, "if information fits any of the specified categories, the court is *required* to protect a requesting interested party and has no discretion to deny the application." *Orion Pictures*, 21 F.3d at 27.

Confidential commercial information means information that "would cause an unfair advantage to competitors by providing them information as to the commercial operations of the debtor." *Orion Pictures*, 21 F.3d at 27. This information is distinct from the concept of a "trade secret" by protecting information that "does not rise to the level of a trade secret but that is so critical to the operations of the entity seeking the protective order that its disclosure will unfairly benefit that entity's competitors." *In re Barney's Inc.*, 201 B.R. 703, 708-09 (Bankr. S.D.N.Y. 1996). The overall purpose is to prevent a "commercial injury." *In re Global Crossing, Ltd.*, 295 B.R. 720, 725 (Bankr. S.D.N.Y. 2003).

ii. "Scandalous or Defamatory Matter"

The limited circuit case law on section 107(b)(2) illustrates different approaches to how "scandalous or defamatory" should be understood and applied. The leading authorities are *In re Neal*, 461 F.3d 1048 (8th Cir. 2006) and *In re Roman Catholic Archbishop of Portland in Oregon*, 661 F.3d 417 (9th Cir. 2011). This section will discuss each in turn.

The *Neal* bankruptcy case began in controversy. The debtor was a former municipal court judge very much in the public spotlight due to a gambling addiction fueled by loans from the local bar. The scandal resulted in criminal prosecutions and state bar investigations. Of course, the debtor ultimately had to file the required creditor matrix, which included the names of several attorneys who had loaned her money while she was on the bench. The debtor moved to seal the names of the attorney-creditors under section 107(b)(2), arguing that disclosing them was "scandalous" and "defamatory." The bankruptcy court agreed and sealed the names. A local newspaper challenged the sealing, and the district court ultimately agreed with the newspaper. On appeal, the Eighth Circuit held that the creditor list was **not** "scandalous" for purposes of section 107(b)(2).

Much as section 107 itself begins with the presumption of openness, the *Neal* court began with a discussion of the common-law right to inspect judicial records and the principle that courts must prevent their files from being used to "gratify public spite or promote public scandal" or serve as "reservoirs of libelous statements for press consumption." *Neal*, 461 F.3d at 1053 (quoting *Nixon v. Warner Communications, Inc.* 435 U.S. 589, 598 (1978)). Only "the most compelling reasons" justify hiding judicial records. *Id.* at 1053 (quoting *Gitto Global*, 422 F.3d at 6). Therefore, the Eighth Circuit determined, based on common law principles, that the context of the filing matters in determining whether a matter should be protected. In other words, reputational harm alone is not sufficient, but "[t]he purpose of including material in a paper filed with the court" informs whether it falls within section 107(b)(2). *Neal* 461 F.3d at 1053-54.

Applying that test to the creditor list, the Eighth Circuit observed that the filing itself was simply a list of people the debtor owed money with no additional accusations or commentary. Moreover, the only reason for filing the list was to comply with bankruptcy filing requirements. Any "scandal" required information "'outside the lines' of the bankruptcy proceeding," such as media coverage, had nothing to do with the filing itself. *Neal*, 461 F.3d at 1054. Therefore, the Eighth Circuit concluded that the creditor list did not contain "scandalous" matter within the meaning of section 107(b)(2). The potential for negative media coverage was "regrettable" but not a basis to seal an otherwise routine, statutorily required filing. *Neal*, 461 F.3d at 1054.

The Ninth Circuit took a different approach in *In re Roman Catholic Archbishop of Portland in Oregon*, 661 F.3d 417 (9th Cir. 2011), which arose from sexual-abuse claims against a Catholic archdiocese. That case concerned two categories of materials: discovery materials produced under an agreed protective order and a punitive damages estimation memorandum and attachments filed in the bankruptcy court, which included detailed allegations of child sexual abuse by those priests.

For filed materials, the Court turned to section 107 and made two important rulings. First, the Ninth Circuit compared section 107 with common-law access doctrine and held that section 107 "speaks directly to and diverges from" the common law. *Archbishop of Portland*, 661 F.3d at 430. Addressing some of these key differences, the Ninth Circuit noted that the common law distinguishes between dispositive and non-dispositive motions while section 107(a) applies to all papers filed in a bankruptcy case. Additionally, the common law allows courts broad discretion to craft exceptions, but section 107(b) and (c) provide only three statutory exceptions. Finally, the common law invites balancing of public and private interests, but section 107(b) uses mandatory language ("the bankruptcy court shall"), leaving no room for balancing once an exception applies. On this basis, the court held that section 107 preempts the common-law right of access in bankruptcy proceedings. Courts are not to import "compelling reasons" tests or improper-purpose inquiries when they are applying section 107(b).

Turning to whether material was "scandalous or defamatory," the Ninth Circuit rejected the context-based approach of *Neal*. Instead, the court held that courts must start with the plain meaning of the text. Because Congress did not define "scandalous," courts should use its ordinary dictionary meaning—"disgraceful, offensive, shameful and the like." *Archbishop of Portland*, 661 F.3d at 432. The court further observed there is no basis in section 107(b)(2) to require proof of falsity, irrelevance, or improper motive. *Id.*

Applying that plain language standard, allegations that a priest had sexually abused children were "most assuredly 'scandalous' because they bring discredit onto the alleged perpetrators." *Archbishop of Portland*, 661 F.3d at 433. Once the priests invoked section 107(b)(2), the bankruptcy court was required to protect them "with respect to scandalous or defamatory matter" contained in the filed memorandum and attachments. The Ninth Circuit ultimately held that the bankruptcy court erred in unsealing those materials.

C. Federal Rule of Civil Procedure 26

Outside of section 107, Federal Rule of Civil Procedure 26 provides mechanisms to protect materials during discovery. While ultimately those materials may need to satisfy a section 107 standard before being filed with a court, a protective order under Rule 26 can facilitate information and document exchanges allowing for open negotiations while limiting potential exposures.

As with materials filed with the court, "as a general rule, the public is permitted 'access to litigation documents and information produced during discovery.'" *Archbishop of Portland*, 661 F.3d at 424 (quoting *Phillips v. Gen. Motors Corp.*, 307 F.3d 1206, 1210 (9th Cir. 2002)). However, under Federal Rule of Civil Procedure 26(c)(1), a party from whom discovery is sought may move for a protective order, and "[t]he court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." Fed. R. Civ. P. 26(c)(1). While a "good cause" requirement is set forth in the statute, courts typically do not require a showing of "good cause" for stipulated protective orders. *See Archbishop of Portland*, 661 F.3d at 424. However, if a party seeks a release of material subject to a protective order, the court must consider whether to keep the protection in place by determining whether "particularized harm" will result from the disclosure, and, if harm will result, then the court must balance public and private interests regarding protecting the material. *Id.* Applying this law to the question of whether priest personnel files produced in discovery should be removed from protection under a stipulated protective order, the Ninth Circuit ruled that the public interest in knowing about credible accusations against a priest in active ministry outweighed the priest's private interests in privacy. *Id.* at 428. However, with respect to a retired priest, the private interest in privacy outweighed any public need for disclosure. *Id.*

Of course, the power of a protective order lies in its enforcement. Federal Rule of Civil Procedure 37(b)(2) provides courts with authority to impose sanctions for failure to comply with discovery orders, including protective orders. Moreover, courts have "broad discretion under Rule 37(b) to fashion remedies suited to the misconduct." *In re Roman Catholic Church of the Archdiocese of New Orleans*, No. 23-30466, 2026 WL 18901, at *10 (5th Cir. 2026) (internal citations omitted). These remedies often include imposing reasonable expenses and attorneys' fees related to the violation. *Id.*

D. Federal Rule of Bankruptcy Procedure 9037

Federal Rule of Bankruptcy Procedure 9037 also provides certain privacy protections. Rule 9037(a) requires filers to redact social security numbers, dates of birth, minor names, and financial account numbers, subject to certain exceptions. Rule 9037 also provides the court with latitude to require additional redaction or to restrict access to documents. Additionally, Rule 9037 provides that an institution waives the protections of the rule by failing to redact.

E. Interaction with Non-Bankruptcy Privacy Regimes

Bankruptcy law is not the only law that merits consideration by bankruptcy courts and practitioners. After all, trustees and debtors in possession must operate "according to the requirements of the valid laws of the State in which such property is situated . . ." 28 U.S.C. § 959. These requirements arguably also include international privacy regimes. Key statutes to consider include:

- **Sector-specific laws.** Statutes with privacy components such as HIPAA, GLBA, and FERPA continue to apply to covered entities and information.

- **State privacy and data-breach statutes**. State statutes, such as the California Consumer Privacy Act of 2018, create obligations to protect certain consumer information. Additionally, many states have laws requiring notification of consumers in the event of data breaches. These obligations become particularly important if information is jeopardized during a bankruptcy proceeding.

- **Foreign privacy laws.** With the increase in cross-border insolvencies and cross-border online information exchange, foreign privacy statutes may apply, such as the EU's General Data Protection Regulation (GDPR). The GDPR is a particularly tough privacy law with substantial potential penalties for violations (maxing out at €20 million or 4% of global revenue, whichever is higher) plus compensatory damages.

Practitioners need to be careful to address required disclosure requirements in bankruptcy with their obligations under these statutes.

3. Issues Regarding Consumer Privacy Ombudsmen

A. Statutory Role and Triggering Conditions

Bankruptcy Code section 332 requires the appointment of a Consumer Privacy Ombudsmen ("CPOs") to address the sale or transfer of consumer information in bankruptcy cases if the privacy policy in effect on the Petition Date otherwise prohibits such sale or transfer.

Key components:

- **When a CPO is required**
  - Cases involving the proposed sale or transfer of consumer PII by a debtor in the business of collecting and storing such information.
  - Focus on situations where the proposed use or transfer may be inconsistent with the debtor's existing privacy policy.
  - Scrutinize possible sources of PII as policy may be broader and more detailed than what the debtor collects.
- **Appointment and scope**
  - Appointment by the U.S. Trustee or the court prior to approval of the sale.
  - Mandated to advise the court on the facts, circumstances, and privacy implications of the proposed transaction.
- **Advisory role**
  - The CPO makes recommendations; the court retains ultimate authority.

B. Practical Challenges in CPO Engagements

Common issues:

- **Defining the "consumer database"**
  Ascertain what information is collected by a debtor from a consumer that meets the definition of Personally Identifiable Information in section 101(41)(A) of the Bankruptcy Code.
- **Access to and understanding of systems**
  Rapidly mapping complex IT environments and legacy data stores.
- **Time pressure**
  Sale timelines often compress diligence and analysis.

- **Scope of recommendations**
  Balancing meaningful privacy protections with preservation of transaction value.

- **Coordination with stakeholders**
  Working with the debtor, buyers, and regulators with varying risk tolerances.

C. Themes in CPO Reports and Court Responses

Patterns that commonly emerge:

- **Alignment with privacy policies**
  Focus on whether the sale is consistent with or reasonably aligned to the debtor's prior privacy commitments.

- **Conditions and safeguards**
  Courts may impose:
  - Use restrictions;
  - Confirmation that prior opt-outs/deletion requests have been honored;
  - Limits on transfers to certain buyer categories (e.g., data brokers).

- **Notice to consumers**
  Additional notice may be required where the new use materially deviates from the original policy.

- **Residual data and deletion**
  Treatment of data that is not sold, including deletion protocols.

D. Strategic Considerations for Practitioners

For debtors, committees, and buyers

:

- **Early assessment** of whether a CPO is likely and how it may affect timeline and structure including knowledge of historical policies.

- **Data hygiene** to minimize unnecessary or obsolete PII before sale.

- **Transaction structuring** (e.g., anonymized data sets, licenses rather than outright sales).

- **Regulatory engagement** where attorney generals, consumer advocates, or regulators are likely to be active.

4. Sales of Sensitive Information

A. The Role of § 363 Sales in Data-Rich Bankruptcies

Section 363 sales often transfer substantial data assets:

- Customer databases and profiles
- Marketing analytics
- Usage and behavior logs

Issues arise around:

- **Data as a core asset**
  The database may be among the most valuable assets.

- **Speed vs. scrutiny**
  Fast sale timelines complicate careful privacy review.

- **Risk allocation**
  Negotiated allocation of privacy, regulatory, and litigation risk between estate and buyer.

B. Consistency with Privacy Policies

A central inquiry is whether the transfer is **consistent** with the debtor's privacy policy in effect on the Petition Date:

- **Legacy policies** may limit or condition transfers in mergers, acquisitions, or bankruptcy. Permissive language ordinarily found in the section "When we Disclose Information" or similar language.

- **If a legacy policy prohibited the transfer of PII, was adequate notice of the change given at the time of the modification?** Review section "Changes to Privacy Policy" or similar language.

- Whether this is a **material deviation**:

  - Appointment of a CPO is more likely;

  - Courts may require additional notice or opt-out opportunities;

  - Courts may impose restrictions on permissible use.

- **Buyer's commitments**
  Buyers may agree to adopt the debtor's existing policy, a more restrictive policy, or a comparable regime as a condition of sale approval.

C. Structuring Sales to Address Privacy Concerns

Tools include:

- **Data minimization**
  Transfer only what the buyer truly needs.

- **Anonymization/pseudonymization**
  Remove or mask direct identifiers where feasible.

- **Segmented transactions**
  Separate especially sensitive cohorts (e.g., minors, health-related data, video titles) for tailored treatment.

- **Use restrictions and covenants**
  Embed privacy covenants in the APA and sale order (no resale to data brokers, compliance with applicable privacy laws, security requirements).

D. Sale Orders and Enforcement

Sale orders can serve as quasi-regulatory instruments:

- **Incorporation of terms**
  Detailed privacy and data-use conditions embedded in both the APA and sale order.

- **Retained jurisdiction**
  Courts may retain jurisdiction to resolve disputes over compliance with privacy conditions.

- **Post-closing oversight**
  In some cases, reporting or certification obligations to demonstrate ongoing compliance.

Summary Chart: Key Privacy Concerns by Stakeholder

Stakeholder	Key Privacy Concerns	Typical Tools / Responses
Bankruptcy Court	• Implementing section 107 correctly • Preventing unnecessary disclosure of PII (SSNs, full account numbers, minors' names) and highly sensitive information • Handling sealing/redaction requests without undermining confidence in the openness of the process • Avoiding misuse of the docket as a vehicle for scandal or harassment	•Approving and enforcing protective orders for discovery •Conditioning sale/plan approval on privacy covenants and CPO recommendations •Adapting statutory requirements for particular facts
Debtor	• Satisfying disclosure obligations while minimizing unnecessary exposure of PII and confidential commercial information • Managing legacy and unstructured data sets with mixed or unknown content • Aligning bankruptcy disclosures with contractual privacy policies and applicable law • Liability and reputational risk from breaches, misuse, or perceived betrayal of privacy expectations	• Early data inventory and classification (PII vs. non PII; sensitive vs. routine) • Use of redactions, sealing motions, and limited disclosures where justified •Historical privacy policy diligence to verify changes were communicated in accordance with policy in effect when consumer consented and that the data inventory excludes consumers who opted-out of receiving marketing communications • Seeking appointment of a CPO when required or strategically useful and engaging with UST in a thoughtful and well-informed manner • Negotiating plan/sale terms that allocate and mitigate privacy and data security risk

Creditors	• Exposure of their own PII or confidential commercial information in proofs of claim, discovery, or public filings • Impact of privacy driven conditions on estate value and recoveries (limits on monetizing data assets) • Potential liability if they receive or use data inconsistent with law or prior privacy commitments	• Filing claims and exhibits with appropriate redactions; seeking leave to file sensitive material under seal • Committee or individual objections to inadequate protections • Negotiating plan/sale terms that balance data monetization with compliance and reputational concerns • Requesting targeted protective orders for trade secrets and competitively sensitive information
Buyers	• Ensuring acquired consumer and employee data can be used as anticipated without violating privacy policies or law • Regulatory and litigation risk from inheriting improperly collected, insecure, or over-shared data • Integration risk when combining acquired data with existing datasets • Obtaining open access to records in compliance with any protective orders in place	• Robust privacy and cybersecurity due diligence on data assets and historic practices, including respecting prior opt-outs and how notices of changes to privacy policies were conveyed • Negotiating representations, warranties, indemnities, use restrictions, and data security covenants • Agreeing to honor or exceed debtor's prior privacy policies; committing to deletion/anonymization of certain data • Seeking clear sale order language defining permissible uses and mitigating successor liability arguments

Consumer Privacy Ombudsman (CPO)	• Understanding what consumer data the debtor holds, how it was collected, and what privacy policies promised • Assessing whether proposed sales/uses are consistent with prior policies and applicable law • Identifying risks of re identification, function creep, and secondary uses by buyers • Balancing consumer expectations and regulatory risk against transaction value	• Rapid diligence on data practices, systems, and policies as usually appointed very late in the sale process • Recommending conditions: use restrictions, deletion/anonymization protocols, opt-out mechanisms, limits on onward transfer • Advising the court on whether to approve a sale and on what terms • Coordinating with state AGs and regulators in high-risk or high-profile cases
State Attorney General	• Sale/transfer of consumer data inconsistent with privacy policies or state law • Use of § 363 sales or plans to sidestep state privacy or data security regimes • Inadequate notice to consumers about new uses/buyers • Downstream misuse of sensitive categories (minors, health, financial, location) • Breaches or lax security during and after the case	• Objections to § 363 sales and plans; appearances as party or amicus • Negotiated sale conditions (use limits, deletion, opt-out rights, restrictions on downstream transfers) • Enforcement actions under state privacy and consumer-protection statutes • Coordination with Consumer Privacy Ombudsman and U.S. Trustee