

**UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK**

-----X	
	:
<i>In re</i>	:
	:
SPIRIT AVIATION HOLDINGS, INC., <i>et al.</i> ,	:
	:
Debtors. ¹	:
-----X	

Chapter 11
Case No. 25-11897-SHL
(Jointly Administered)

**CONSUMER PRIVACY OMBUDSMAN
REPORT TO THE COURT**

September 8, 2026

Lucy L. Thomson
Consumer Privacy Ombudsman

The Willard, Suite 400
1455 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
(703) 212-8770
lucythomson_cpo@earthlink.net

¹ The Debtors' names and last four digits of their respective employer identification numbers are as follows: Spirit Aviation Holdings, Inc. (1797); Spirit Airlines, LLC (7023); Spirit Finance Cayman 1 Ltd. (7020); Spirit Finance Cayman 2 Ltd. (7362); Spirit IP Cayman Ltd. (4732); and Spirit Loyalty Cayman Ltd. (4752). The Debtors' mailing address is 1731 Radiant Drive, Dania Beach, FL 33004.

I. Bankruptcy Code Privacy Framework

Pursuant to Bankruptcy Code section 332(b), Lucy L. Thomson, the Consumer Privacy Ombudsman (“CPO” or “Ombudsman”) appointed in this case,² submits this Report to advise the Court on the issues related to privacy and the protection of personally identifiable information (PII)³ of the consumers/ passengers of Spirit Aviation Holdings, Inc. d/b/a Spirit Airlines, LLC (“Debtors” or “Spirit”).

Sections 332 and 363 provide a framework for evaluating the sale of personally identifiable consumer records in the context of a bankruptcy case. 11 U.S.C. §§ 101 *et. seq.* The Bankruptcy Code creates certain privacy protections for personal information that consumers provided to a company in connection with obtaining a product or service, *i.e.* airline transportation. Section 363(b)(1) of the Bankruptcy Code provides that the sale may not violate non-bankruptcy laws.

The Debtors have divided their digital assets into three groups: (1) Intellectual Property, (2) Personal Data, and (3) Deidentified Data. Through an initial auction completed on Friday, August 13, 2026, the Debtors propose to sell enterprise data derived from the company’s

² Pursuant to the Order approving the Stipulation and Agreed Order Directing the United States Trustee to Appoint a Consumer Privacy Ombudsman (Doc. No. 1332, filed July 15, 2026), the United States Trustee appointed Lucy L. Thomson as the Consumer Privacy Ombudsman in this case. (Doc. Nos. 1350 and 1351, filed 7/17/26) The Court approved this appointment on July 23, 2026 (Doc. No. 1380).

³ Section 101 (41A) of the Bankruptcy Code defines the term "personally identifiable information" to mean –

(A) if provided by an individual to the debtor in connection with obtaining a product or a service from the debtor primarily for personal, family, or household purposes –

- (i) the first name (or initial) and last name of such individual, whether given at birth or time of adoption, or resulting from a lawful change of name;
- (ii) the geographical address of a physical place of residence of such individual;
- (iii) an electronic address (including an e-mail address) of such individual;
- (iv) a telephone number dedicated to contacting such individual at such physical place of residence;
- (v) a social security account number issued to such individual; or
- (vi) the account number of a credit card issued to such individual; or

(B) if identified in connection with 1 or more of the items of information specified in subparagraph (A) –

- (i) a birth date, the number of a certificate of birth or adoption, or a place of birth; or
- (ii) any other information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically.

operations that includes “deidentified data” pertaining to approximately 190 million airline flights taken by Spirit passengers. A subsequent auction to sell the personal data of the 97.5 million passengers will be conducted at a later date.

Because of the data requirements of modern day air travel, the personal passenger data collected by Spirit is extensive and highly sensitive. While this sale transaction purports to exclude “personal data,” the sale of deidentified consumer information presents challenging and novel issues for the Court’s consideration.

The Debtors have articulated their position that the sale of deidentified data of Spirit passengers to the successful bidder, a technology company that intends to use the data for training AI models,⁴ is permissible under current applicable law and the Spirit privacy policy.

This bankruptcy sale illustrates that with respect to the protection of personal data and deidentification, technology has far outpaced the law, potentially putting consumers at risk of significant harm if their deidentified personal data is reidentified and misused or stolen, or if AI makes inferences about individuals based on combining deidentified data with data from other sources, and that information is disclosed without authorization.

⁴ Notice of Auction Results and Scheduled Hearing for the Deidentified Data (Doc. No. 1463, filed 8/14/26). The Debtors selected Google LLC (the “Successful Bidder”) as the highest and best bid (the “Successful Bid”) and Mercor.io Corporation (the “Alternate Bidder”) as the Alternate Bid.

Google LLC is a multi-national technology company that offers hundreds of products and services spanning search, consumer software, enterprise cloud, mobile operating systems, and hardware.

Mercor.io is an AI data and recruiting startup founded in 2023 that connects specialized human experts with top AI labs and enterprises to train advanced AI models. In early 2026, the company experienced a supply chain security incident. If the Court decides to consider the company as the successful bidder, the CPO requests an opportunity to conduct further research into the circumstances of this data breach. <https://www.mercor.com/blog/update-on-mercior-security-incident/>.

micro1, a human-data and intelligence platform for AI training, filed a Notice of Intent to Submit a competing and superior bid for the deidentified data. (Doc. No. 1556, filed 9/3/26). If the Court decides to consider the company as the successful bidder, the CPO requests an opportunity to conduct further research into their proposal.

The CPO believes it is helpful to address the significant impact the sale will have on the consumers who provided their personal data to Spirit for airline bookings, as well as recent legal requirements and technology developments with respect to deidentification that the Court may wish to take into consideration in making its decision regarding approval of the sale. Specifically, this CPO Report focuses on these factors set forth in the Bankruptcy Code that the Ombudsman may address, including information relating to:

- The Debtors' Privacy Policy;
- Potential losses or gains of privacy to consumers if the sale is approved;
- Potential costs or benefits to consumers if the sale is approved; and
- Possible alternatives that would mitigate potential privacy losses or costs to consumers.

11 U.S.C. § 332.

Summary of Recommendations

The Debtors and the successful bidder have voluntarily agreed to follow the up-to-date deidentification standard adopted within the California Consumer Privacy Act ("CCPA") (Cal. Civ. Code § 1798.140(m)) for the deidentification process for this sale.

The parties have made voluntary commitments on important issues related to the deidentification process; these are good first steps.

This report recommends adoption of several conditions related to the following issues to mitigate the potential harm to the more than 97 million Spirit passengers that may result from this proposed sale:

- Verification of Deidentification and Certification
- Transparency
- Protection of Children and Teens
- Restrictions on Reidentification of the Deidentified Data
- Reasonable and Appropriate Security in the AI Training Environment

To ensure that this report is submitted on a timely basis, this CPO Report will be filed on Tuesday, September 8, 2026. Discussions with the CPO and counsel for the Debtors and the successful bidder about the recommendations are underway. Google, the successful bidder, has offered to narrow the types of personal data items to be included in the sale to reduce the likelihood that the data can be reidentified. This is a positive step and may lead to a successful sale. The risks to consumers discussed in this report should be read in light of Google's proposal to remove data items from the sale. The final list of recommended conditions will be filed promptly.

II. Assets to Be Sold – Deidentified Spirit Passenger Data

Over the decades of its operations since 1992, Spirit has collected PII and other personal data of its passengers as follows:

- Customer database and profiles (approximately 97.5 million passengers)
- Customer email list (approximately 13.7 million active addresses)
- Loyalty and co-brand cardholder lists (including Free Spirit portfolio and Savers Club)

Spirit collected personal data from passengers for the purpose of booking airline flights and with the understanding that, as the privacy policy states: “We do not sell personal information.”⁵ A sale such as this, in which Spirit proposes to sell data to Google or the backup bidder for an entirely different purpose – the training of AI models – requires close scrutiny.

This sale primarily includes enterprise data derived from the Company's operations, including productivity and collaboration data, core business systems, and workflow and process data.⁶ Debtors' counsel has advised the CPO that the categories of enterprise data in this sale

⁵ Further, the Sharing of Information, section 1 “Affiliates and Acquisitions,” states that “If another company acquires, or plans to acquire, our company, business, or assets, we will also share information with that company, including at the negotiation stage.” The debtors position is that this section 1 supports the sale of all the deidentified personal data to the successful bidder.

⁶ A complete list of the assets included within the Deidentified Data can be found in the Asset Schedule attached to the Notice of Auction Results and Scheduled Hearing for the Deidentified Data. Sale Agreement between Google

include eight systems that had multiple processing purposes, some of which may have involved the processing of personal data, but others did not. Some of the databases contain identity-related information dating back to 2018.⁷

Of these eight systems, the flight reservations database and Revenue Transactions / PNR Data⁸ currently contain voluminous amounts of personal data collected by Spirit in connection with the booking of airline flights by and travel to the destinations of the more than 97 million passengers.

With respect to consumer PII of Spirit passengers, the Sale Agreement states “Personal Data” is excluded from the sale as follows:

“Assets shall not include information that relates to, describes, or is reasonably capable of being associated with a consumer or is otherwise considered ‘personal data’, ‘personal information’, ‘nonpublic personal information’ or other similar term under applicable data protection laws.” Sale Agreement § 1(a)(i).

LLC and Spirit Airlines, LLC, Section 1(c) (attached as Exhibit A, Docket No. 1463 at 18) (note Deidentified Data excludes those rows marked “not included” and includes only those marked “included”).

⁷ The enterprise data assets encompass the following types of information:

- **Productivity & collaboration data**, including email and calendar data, document repositories (e.g., SharePoint/ OneDrive), chat and collaboration messages, and wikis/ knowledge base.
- **Core business systems**, including customer behavior (CRM), employee behavior and productivity data, revenue and yield management (inventory) data, and aircraft operation and logistics data.
- **Workflow & process data**, including finance, marketing, support/HR/ legacy, strategy and operations, and project management data.

Eight systems that might include customer data:

- Revenue Transactions / PNR Data (confirmation numbers), Refunds, Inflight Purchases, Timecard information, WiFi Sales, Corporate emails (includes employee data and possibly marginal consumer data).

Systems that would include employee data: Concur, Employee business travel records.

⁸ A PNR (Passenger Name Record) is a unique six-character code that acts as the digital booking reference for a flight. It is also known as a record locator or booking code. <https://www.cbp.gov/travel/clearing-cbp/passenger-name-record>.

Debtors structured the bid process so that pursuant to the Successful Bid these systems will be subject to a deidentification process designed to remove personal data *prior to* transmission to the winning bidder.

What is Deidentification?

Deidentification is a process used to remove the link between a set of identifying data and a specific individual. It strips personal identifiers from a dataset so the remaining information cannot be easily tracked back to a real person. Source: NIST

The exclusion of “personal data” from this sale is premised on the theory that “deidentified data” under certain federal and state privacy laws is not considered “personal data.” A close look at the details of the sale process and the data to be sold illustrated in the table below suggests that until such time as any of the personal data is deidentified, it is the PII of Spirit passengers and requires strong protection for the future, particularly since the data will be used by the successful bidder for a different purpose than for which it was collected. Counsel for Google LLC, the successful bidder, advised the CPO that the deidentified data will be used for the training of artificial intelligence (AI) models.

With the sale provisions in mind, the following table outlines the sale process to be followed in deidentifying the data. It identifies actions that will be taken and decisions to be made so the Court can assess the privacy issues at each point on the timeline. Protection of consumers at the deidentification planning stage is particularly important when decisions will be made about what consumer passenger data items to include in the deidentified data to be provided to the successful bidder.

Lifecycle of Sale Process – Spirit Consumer PII to be Deidentified				
Spirit Airlines owns the consumer PII			Court approves the sale	Successful bidder owns the deidentified consumer PII
Consumer PII requires strong protection				
Consumer personal data (PII) collected for airline bookings; included in 8 enterprise systems that may contain consumer data to be sold	Spirit proposes to hire third party expert to deidentify the consumer data (PII)	Third party will follow generally accepted standards that provide strong protection for consumers; Court to evaluate and approve.	Spirit transfers the deidentified data to the successful bidder Data to be used to train AI models	Privacy laws provide that the deidentified data is no longer considered PII
97+ million consumers 190 million flights	Deidentification planning process – identify direct and indirect identifiers to remove from data systems <i>and</i> other processes to specify	Personal identifiers removed and other deidentification steps/ processes specified and applied		

III. Technology Landscape and Consumer Risks – Deidentification Limitations

Deidentification is particularly problematic in the age of AI, when AI and machine learning can easily reidentify deidentified or anonymized data by matching patterns, behavioral tracks, or auxiliary datasets. A decade ago, the National Institute Standards and Technology (NIST) explained the purpose and risks of deidentification of personal data:

De-identification removes identifying information from a dataset so that individual data cannot be linked with specific individuals. De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing or publishing information. De-identification thus attempts to balance the contradictory goals of using and sharing personal information while protecting privacy. Several U.S laws, regulations and policies specify that data should be de-identified prior to sharing. In recent years researchers have shown that some de-identified data can sometimes be re-identified. Many different kinds of information can be de-identified, including structured information, free format text, multimedia, and medical imagery.⁹

⁹ National Institute Standards and Technology (NIST), *De-Identification of Personal Information*, NISTIR 8053 (2025), <https://www.nist.gov/publications/de-identification-personal-information>

In a July 2026 publication by Gartner, a business and technology insights company, researchers predicted that “[p]rivacy risks are increasingly emerging from what AI algorithms infer about individuals rather than what data is directly exposed.”¹⁰ Gartner concluded that by 2029, most privacy incidents will result not from the direct exposure of personally identifiable information (PII), but from AI-generated inferences about individuals. This Gartner update on the AI privacy and cybersecurity risks follows a decade of scholarly research that illustrates how machine-driven cross-database linking exposes unique individual combinations and can lead to identifying a specific individual.¹¹

FBI Warns America’s airlines are under attack – AI exacerbates cybersecurity risks and facilitates the types of attacks that can undermine the deidentification of personal data. The aviation sector includes many industries ranging from airlines, airports, technology providers, subcontractors – all of which are prime targets for cyberattacks. The FBI has observed a shift in cyberattacks from isolated data theft to coordinated campaigns targeting the airline industry using social engineering techniques.¹² In numerous breaches that exposed millions of passenger records, airlines suffered systemwide outages that grounded fleets and critical systems became unavailable, ransomware extortion demands were delivered, and client confidences undermined when stolen

¹⁰ *AI Privacy Risks Push CISOs Beyond Traditional Data Protection to Include Inference Governance*, GARTNER (July 30, 2026), <https://www.gartner.com/en/newsroom/press-releases/2026-07-30-gartner-predicts-most-privacy-incidents-will-stem-from-artificial-intelligence-generated-inferences-by-2029>

¹¹ *Anonymity, De-Identification, and the Accuracy of Data*, HARVARDONLINE (Aug 28, 2023) <https://harvardonline.harvard.edu/blog/anonymity-de-identification-accuracy-data>

¹² Cybersecurity & Infrastructure Security Agency (CISA), FBI, Canada, Australia and U.K. law enforcement, joint Cybersecurity Advisory, Scattered Spider, Alert Code AA23-320A (July 29, 2025), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a>.

sensitive passenger data and contact details were published on the dark web (an underground marketplace on a “dark” part of the Internet where cyber criminals post stolen data).¹³

The threat landscape for reidentification of personal data is diverse and evolving. Inference, linkage, and reconstruction attacks are sophisticated data privacy exploits used to deanonymize data or reverse-engineer sensitive AI training models. While linkage attacks relying on external data remain a primary concern, inference and reconstruction attacks pose growing risks even to datasets processed with sophisticated methods.¹⁴ This necessitates robust privacy protections that anticipate a wide range of potential attack vectors.¹⁵

The Debtors emphasize that notwithstanding the potential risks in the broader technology landscape, this sale is appropriate because it is grounded in the “reasonableness” standard in U.S. and state privacy laws and reflected in the Sale Agreement. Specifically, the Debtor intends to –

- (1) take reasonable measures to ensure that data cannot be associated with a natural person,
- (2) require a purchaser to publicly commit to maintaining and using deidentified data without attempting reidentification, and
- (3) prohibit a purchaser from onward transferring deidentified data to a third party unless the third party enters into a similar public commitment.

¹³ A website that goes by the name “Information is Beautiful” provides a visualization of hundreds of the massive data breaches that have affected the private sector and government, *World’s Biggest Data Breaches & Hacks* (Sep. 2025), <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>.

¹⁴ *Data Privacy Attacks: The Alarming Risk of Reconstruction Attacks on Seemingly Anonymous Data*, MEDIUM, (Jan. 12, 2024) <https://medium.com/@oblv/data-privacy-attacks-the-alarming-risk-of-reconstruction-attacks-on-seemingly-anonymous-data-ddf68c3764d6>.

¹⁵ Jules Polonetsky, *The Curse of Dimensionality: De-identification Challenges in the Sharing of Highly Dimensional Datasets*, FUTURE OF PRIVACY FORUM (May 5, 2025), <https://fpf.org/blog/the-curse-of-dimensionality-de-identification-challenges-in-the-sharing-of-highly-dimensional-datasets/>.

IV. Spirit Airlines Privacy Policy

The Bankruptcy Code creates certain privacy protections for personal information that consumers provide to a company in connection with obtaining a product or service, primarily for personal, family, or household purposes – in this case, airline transportation. In enacting the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), Congress balanced the interest in the sale of assets of the bankruptcy estate with protection of consumer privacy by creating a duty to ensure that the promises made in the Debtors’ privacy policy are honored. 11 U.S.C. §363(b)(1)(B)(ii).

Spirit Airlines published a privacy policy on its website to address the collection and handling of its consumer PII.¹⁶ It describes “how Spirit Airlines collects, uses, shares, and safeguards personal information.” It also tells consumers about their rights and choices with respect to their personal information, and how they can reach the company to get answers to questions.

In the **Sharing of Information** section, the privacy policy specifies eight circumstances in which “we disclose information in the following situations.” Of particular relevance to this sale are the following provisions:

1. **Affiliates and Acquisitions.** We may share information with any corporate affiliates (e.g., parent company, sister companies, subsidiaries, joint ventures, or other companies under common control). If another company acquires, or plans to acquire, our company, business, or our assets, we will also share information with that company, including at the negotiation stage.

7. **Sale of Information.** We do not sell personal information.

¹⁶ The privacy policy was effective on December 22, 2022 and last updated on January 14, 2026 and was in effect on the filing date of this case.

Debtors rely on Section 1, “Affiliates and Acquisitions,” to justify this sale. While the Debtors take the position that this sentence authorizes the transfer of all of its assets to the successful bidder, the meaning of the sentence is not entirely clear. This sentence does not address the sale of personal data or specify in any way what information is to be “shared.” When read in the context of “including the negotiation stage,” a reasonable interpretation of the sentence does not appear to authorize the sharing (or sale) of all the company’s personal data.

The privacy policy describes in detail the specific purposes for the collection of PII and the uses Spirit makes of the personal data. All of these purposes and uses relate to providing airline travel for the Spirit customers and offering related services that may be of interest to them (*i.e.*, through targeted advertising and offerings). It does not suggest the sale of personal data for a different purpose other than airline travel.

Sensitive personal data is a special subset of personal information that needs extra protection. If leaked or stolen, it can cause severe harm, fraud, or discrimination to the individuals who provided the information. The privacy policy contains a “Sensitive Information Disclosure” and states that the company collects the following sensitive information:

- social security number
- passport number, or other form of state or federal identification
- account number
- log-in information (to your Spirit account)
- credit or debit card-related information
- precise geolocation
- biometric information (when consumer chooses to use self-serve bag drop kiosks)

Sensitive data about children and teens who flew on Spirit Airlines is also included in the PII.

V. Potential losses or gains of privacy and potential costs or benefits to consumers if the sale is approved.

A. Potential Gains and Benefits to Consumers – Non-Personal Data / Deidentified Data

An auction for this first sale of the digital assets was conducted on August 13, 2026. This category of assets, labeled “de-identified data,” consists of “certain deidentified enterprise data derived from the Company’s operations, including productivity and collaboration data, core business systems, and workflow and process data.”

No one as yet has articulated a personal or cognizable benefit to consumers from this sale of their personal data. In a statement following announcement of the auction results, a Google spokesperson said the Spirit data “can be helpful in improving our products and AI models.”

For the protection of the consumers who provided their personal data to Spirit for airline travel, this sale must minimize the risk that personal data, and particularly sensitive data, and inferences that AI might subsequently make, might be unlawfully accessed or disclosed.

Excluded Databases – The deidentified data will not include, and is not being derived from, databases relating to customer insights, customer profiles, Free Spirit member data, savers club data, social media data, and survey data. No biometric or geolocation data will be included.

B. Potential losses of privacy and costs to consumers if the sale is approved.

The privacy policy does not contemplate the transfer of the personal consumer data or e-mails of Spirit consumers to a technology company for the development and/or training of AI models.

In the “Sharing of Information” section, the Debtors’ privacy policy describes the categories of personal information Spirit collects, discloses for a business purpose, and shares with third parties. While the policy provides for the sharing of consumer personal data in some

instances,¹⁷ in this sale the Debtors are seeking to sell significant amounts of deidentified personal data to a company for the purpose of training AI models.

C. Possible alternatives that would mitigate potential privacy losses or costs to consumers.

In a letter dated August 5, 2026, Debtors' counsel advised the CPO that in the interest of protecting consumer privacy, Spirit Airlines intends to voluntarily apply "the deidentification standards enunciated by the modern state privacy laws and the FTC." Specifically, it intends to –

(1) take reasonable measures to ensure that data cannot be associated with a natural person,
(2) require a purchaser to publicly commit to maintaining and using deidentified data without attempting reidentification, and

(3) prohibit a purchaser from onward transferring deidentified data to a third party unless the third party enters into a similar public commitment.

The Debtors and the successful bidder have voluntarily agreed to follow the up-to-date deidentification standard adopted in the California Consumer Privacy Act ("CCPA") (Cal. Civ. Code § 1798.140(m)) for the deidentification process for this sale. The parties have made voluntary commitments on important issues related to the deidentification process; these are good first steps.

For the protection of the consumers who provided their personal data to Spirit for airline travel, this sale must minimize the risk that personal data, and inferences that AI might subsequently make, could be unlawfully accessed or disclosed.

To approve this sale, the CPO recommends that the Court adopt the proposed conditions to be provided as Attachment A to this CPO Report.

¹⁷ For example, Paragraph 1 of the privacy policy authorizes sharing of "information" with entities that have a defined legal or contractual relationship with the Debtors. As such, the entities receive information subject to Spirit's privacy policy and other contractual requirements. In the course of negotiations with prospective bidders in this case, Debtor has shared "information" – not personal data – in a "data room" as part of generally accepted business practices to inform prospective buyers of the categories of data available for sale.

VI. Law

A. Evolution of Laws Regarding Privacy and Deidentification of Personal Data

This bankruptcy sale presents challenging issues in which law and technology are interrelated. It illustrates that with respect to the protection of personal data and deidentification, technology has far outpaced the law, potentially putting consumers at risk of significant harm if their deidentified personal data is reidentified and misused or stolen, or if AI makes inferences about individuals based on combining deidentified data with data from other sources, and that information is disclosed without authorization. While properly deidentified data has a very low risk of re-identification, combining it with external datasets or using insufficient deidentification methods can potentially reveal individual identities.

There is no comprehensive data privacy law in America – privacy is regulated on an ad-hoc industry-by-industry basis. Several privacy laws and regulations currently in effect were enacted over a decade ago and they have not been updated to address the privacy risks presented by emerging technologies such as AI. None of these laws – or the definition of “deidentified data” – take into account the risks of reidentification that are growing as the power of AI increases.

With respect to federal privacy regulation, while the Federal Trade Commission (FTC) has been the primary federal agency providing guidance to the public and the business community on data privacy issues, the Federal Trade Commission Act (“FTCA”) excludes “air carriers” from the agency’s jurisdiction. 15 U.S.C. 45(a)(2). As an airline carrier, Spirit Airlines is covered by requirements promulgated by the U.S. Department of Transportation (DOT). The DOT portal provides the following summary of the applicable privacy rules and requirements.¹⁸

¹⁸ <https://www.transportation.gov/individuals/aviation-consumer-protection/privacy>
See also, e.g., *Airline Deregulation Act of 1978: Preemption of State Consumer Protection Laws*, Congressional Research Service (March 1, 2023), <https://www.congress.gov/crs-product/LSB10925>.

Air Consumer Privacy

Airlines and ticket agents regularly collect personal information from passengers in the course of business that may not be otherwise publicly available such as name, date of birth, and frequent flyer number. It is important for this information to be collected and maintained responsibly.

Mishandling the private information of consumers may be considered an unfair or deceptive practice. The U.S. Department of Transportation (DOT) has the authority to investigate complaints and take action against airlines and ticket agents for unfair or deceptive practices. This authority includes imposing civil penalties where appropriate.

It is an unfair or deceptive practice for an airline or ticket agent to violate the privacy of airline passengers by:

- violating the terms of its privacy policy.
- violating a rule issued by the DOT identifying specific privacy practices to be unfair or deceptive.
- violating the Children's Online Privacy Protection Act (COPPA) or Federal Trade Commission (FTC) rules implementing COPPA.
- failing, as a participant in the Data Privacy Framework (DPF) Program, to comply with DPF Principles.¹⁹
- engaging in an “unfair” practice. In general, a practice is unfair if it causes or is likely to cause substantial injury, which is not reasonably avoidable, and the harm is not outweighed by benefits to consumers or competition.
- engaging in a “deceptive” practice. A practice is deceptive if it is likely to mislead a consumer, acting reasonably under the circumstances, regarding a material matter. A matter is material if it is likely to have affected the consumer’s conduct or decision with respect to a product or service.

In August 2022 the DOT issued guidance on these definitions in response to Executive Order 14036, *Promoting Competition in the American Economy*. In the guidance, the DOT explicitly explained that the definitions are modeled after the FTC’s authority.²⁰

The Children’s Online Privacy Protection Act (COPPA) addresses the need to protect children when they provide their personal data to a company covered by the statute. If an airline’s

¹⁹ The EU-U.S. Data Privacy Framework (DPF) is a method by which companies may transfer consumers’ personal data to the United States from the European Union (EU) without violating EU privacy laws.

²⁰ The FTC has adopted widely-accepted fair information practice principles and enforces laws prohibiting unfair and deceptive practices. The Consumer Financial Protection Board (CFPB) found that inadequate security for the sensitive consumer information collected, processed, maintained, or stored by a company can constitute an unfair practice in violation of 12 U.S.C. 5536(a)(1)(B).

digital platform targets children under 13—or has actual knowledge it is collecting data from children under 13—it must get verifiable parental consent. While the COPPA rules do not apply to Spirit because the company collects personal data *about* children, not *from* children, nor do the rules apply to deidentified data, the statute focuses on children as a special category of individuals whose data require special protection.

Again addressing the personal data of children – not deidentified data – the FTC updated COPPA (effective April 22, 2026) with a particular focus on the AI environment. The FTC ruled that disclosing or using a child's data to train or develop AI technologies is not integral to providing an online service. Companies must secure distinct, standalone, verifiable parental consent explicitly for AI model training or sharing data with third-party AI vendors.²¹

Ban on Indefinite Data Retention – AI systems rely heavily on massive historical datasets to optimize algorithms over time. The updated COPPA rule strictly prohibits the indefinite retention of children's personal information. Operators must establish and maintain a strict written data retention policy. Once data is no longer necessary for the specific, non-AI function it was originally collected for, it must be permanently deleted rather than archived to train future algorithms.

Many children fly with family or friends or unaccompanied, and their personal data may be included in the assets to be sold. The risk of reidentification is particularly problematic when the deidentified data pertains to children. Consideration should be given to excluding the data of children from this sale.

²¹ FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data: Agency's final rule expands protections for children's data and requires that operators provide more information to parents (Jan. 16, 2025), <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data>.

Recent Congressional Action on Deidentification

Legislators’ and regulators’ assessments about deidentification are changing and in connection with the “bulk data transfer rule” have concluded in the context of national security that deidentification standards may no longer be adequate to protect the rights of individuals. The Justice Department’s Data Security Program (DSP) is a regulatory framework that restricts or prohibits U.S. entities from transferring large quantities of sensitive personal data and U.S. government-related data to specific "countries of concern" or by classes of covered persons.²² Unlike most privacy and data broker laws, in the context of national security, the DSP does *not* exclude anonymized, pseudonymized, or deidentified data but rather expressly includes the foregoing within the definition of certain covered data. 90 Fed Reg. 1636, 1650) (Jan 8, 2025).

Pursuant to the rule-making process, the commentary to a proposed DSP regulation makes significant findings that seriously undercut reliance on traditional definitions of “deidentification” as a means to protect the privacy interests of consumers. 28 C.F.R. § 202.206, 90 Fed Reg. 1706 (Jan. 8, 2025). The final rule, referencing the Notice of Proposed rulemaking, found that “advances in technology, combined with access by countries of concern to large datasets, increasingly enable countries of concern that access this data to re-identify or de-anonymize data,” allowing them to “reveal exploitable sensitive personal information on U.S. persons.” *Id.* at 1653.

With respect to healthcare data, the Department reported that it agreed that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) de-identification standard no longer protects individuals, 90 Fed Reg 1636, 1666 (Jan. 8, 2026), and that human genomic data,

²² U.S. Department of Justice, National Security Division, Data Security Program (eff. April 8, 2025), <https://www.justice.gov/nsd/data-security>. See Executive Order 14117, *Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government Data by Countries of Concern*, 89 Fed. Reg. 15421 (Feb. 28, 2024). The program addresses the sale of bulk data to foreign countries. While the regulation does not specifically apply to this type of case, the factual findings regarding the failure of current deidentification tools/models are informative.

even when deidentified, can still be reidentified. *Id.* at 1653. Finally, as the Justice Department has recently explained, “[o]pen-source reporting has repeatedly raised concern[s] that supposedly anonymized data is rarely, if ever, truly anonymous.” Notice of Proposed Rule Making, 89 Fed. Reg. 86116, 86126 (Oct. 29, 2024). The point is that many of the current deidentification tools are no longer a reliable means of protecting data, including the deidentified sensitive personal data.

B. Limitations on Secondary Uses

Passenger Name Record (PNR)

Following the 9/11 attacks on the World Trade Center, Congress passed the Aviation and Transportation Security Act that established enhanced airline security screening measures. Pub.L. 107-71 (Nov. 19, 2001). The law requires air carriers operating passenger flights in foreign air transportation to, from, or through the United States to make Passenger Name Record (PNR) information available to U.S. Customs and Border Protection (CBP) upon request.²³ Passengers are required to submit this information to the airline as a condition of boarding. Privacy protections for the government’s use and handling of PNR data are governed by the Privacy Act of 1974.

Restrictions on the use and retention of PNR data have been mandated globally. Bilateral international agreements govern the international collection and transfer of PNR data. For example, the U.S.-EU PNR Agreement (2011) establishes privacy guardrails such as a strict purpose limitation that the data may only be used to prevent, detect, investigate, and prosecute terrorist offenses and transnational crimes. It cannot be repurposed for general surveillance.

In 2022 the EU Court of Justice imposed strict new boundaries for PNR data retention at six months for general travelers unless there is objective evidence linking a specific passenger to

²³ 49 U.S.C. § 44909(c)(3) requires airlines to provide the government with the full name of each passenger and crew member, date of birth and citizenship, sex, passport number and country of issuance, U.S. visa or resident alien number, and other information.

a genuine, present, or foreseeable threat of terrorism or serious transnational crime. The U.S. framework relies on keeping data active for five years (and dormant for up to 15 years). The Court also created a ban on general predictive modeling, ruling that law enforcement cannot store historical PNR data indefinitely just to "feed" or train machine-learning algorithms and predictive databases. Security agencies are prohibited from keeping records just to look for future, unconfirmed patterns. *Ligue des droits humains v. Conseil des ministres*, Case C-817/19, ECLI:EU:C:2022:491 (21 June 2022).

The strict purpose limitation that the PNR data may only be used to prevent, detect, investigate, and prosecute terrorist offenses and transnational crimes suggests that it may not be appropriate to retain and use PNR data that was provided by Spirit passengers as a condition of boarding airline flights for a different purpose, namely, to train AI models.

C. Deidentification Framework

It is the Debtors' position that "modern privacy laws" do not apply to data that has been deidentified. In a memorandum to the CPO dated August 16, 2026, Debtors' counsel points to a Federal Trade Commission (FTC) report titled "*Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*," that "articulate[d] best practice[s] for companies that collect and use consumer data."²⁴ Among other things, the FTC discussed what data should be, and should not be, considered personal data. This deidentification standard has been uniformly adopted by the 26 states that have enacted modern privacy legislation.²⁵ Those

²⁴ See FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers* (March 2012) at 21.

²⁵ Many of the modern State privacy laws provide that any information "collected, processed, sold, or disclosed in relation to price, route, or service" by an airline are further exempted from any state laws limiting the sale of such data. See, e.g., Fla. Stat. § 501.704 (2025). While some State laws do not contain such an express carve-out, any prohibition contained within those states' laws concerning the sale of data would arguably be preempted by the Airline Deregulation Act. See 49 U.S.C. § 41713.

laws universally codified the FTC's "reasonable linkability" standard for determining when data has been deidentified.

Thus, the Debtors propose to follow the codified definition of deidentification adopted within the California Consumer Privacy Act ("CCPA") for the deidentification process for this sale:

(m) "Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:

- (1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.
- (2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.
- (3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision.

...

(v)(3) "Personal information" does not include consumer information that is deidentified..."

The Successful Bid expressly incorporates the three requirements set forth under that standard for deidentification, and will require an independent third party to conduct the deidentification based upon industry standards and practice.

The Debtors believe that by following this "reasonableness" standard in the U.S. and state privacy laws, they meet the legal requirements for this sale. The process for deidentification the Debtors have adopted is thoughtful and designed to meet the latest professional standards available. The Debtors are in the process of identifying a vendor to conduct the data deidentification. The CPO requests an opportunity to learn more about the standards the vendor plans to follow once the vendor is selected.

Because organizations can technically comply with statutory deidentification standards, harmed individuals have little legal recourse or avenue for recovery when reidentification occurs. There is no duty for a company to report to a federal or state regulator or affected individual if deidentified personal data has been reidentified. There is no external way to verify if a private entity has privately deidentified “anonymized” data. Thus individuals whose personal data has been deidentified are at a serious disadvantage because of this lack of transparency.

The Sale Agreement requires the successful bidder publicly to commit to maintaining and using deidentified data without attempting reidentification. This prong of the “reasonableness” standard that requires such a public statement is intended to provide a means of redress for any consumer whose data was reidentified by the successful bidder.

Further, the successful bidder must provide reasonable and appropriate security for the deidentified personal data it receives. The DOT has found that mishandling the private information of consumers may be considered an unfair or deceptive practice. Google published the following paper titled *Our Approach to Protecting AI Training Data* that outlines its approach to cybersecurity for AI training data.

Best Practices for Protecting AI Training Data

Google has published *Our Approach to Protecting AI Training Data* that highlights best practices in data protection and describes how Google applies them in its systems.²⁶

Protecting data requires both technical controls to enable safe data use at scale, and governance processes to ensure that companies have visibility and control over how their data is used. This fundamentally requires: understanding data and ensuring it has sufficient metadata in the form of attributes, controlling the data and implementing policies to allow (or disallow) certain usage based on those attributes, transforming data to enable its usage in policy compliant ways, and human oversight and governance.

²⁶ *Our Approach to Protecting AI Training Data*, GOOGLE, <https://research.google/pubs/our-approach-to-protecting-ai-training-data/>

Protecting data in AI inherits these requirements and introduces new requirements to account for unique AI-specific risks including memorization/recitation and the costs of training foundational models. Meeting these new risks requires new capabilities including enhanced understanding of data and model lineage as well as an increased ability to control data usage through checks on data for policy compliance at the time a training job is configured before it is run.

This white paper offers an in-depth look at data protection best practices and Google's data protection capabilities, and is one of a series of publications about Google's Secure AI Framework (SAIF).

Conclusion

The issues related to the sale of the deidentified data of the more than 97 million Spirit passengers required under sections 332 and 363 of the Bankruptcy Code have been addressed for consideration by the Court, including compliance with the privacy policy, the application of non-bankruptcy laws, and the losses or gains, and costs or benefits to consumers, if the sale is approved.

The CPO has provided an analysis of the laws and privacy principles relevant to the proposed sale, and preliminary recommendations regarding practical steps the parties can take to protect the privacy of the Spirit consumers. The CPO believes the Recommendations in this CPO Report strike an appropriate balance between the privacy rights of consumers and practical considerations associated with this bankruptcy sale. She stands ready to provide whatever further analysis or recommendations the Court deems appropriate.

Respectfully submitted,

Lucy L. Thomson

Consumer Privacy Ombudsman