Privacy Impact Assessment
for
Relativity

September 24, 2025

Point of Contact
Gregory Jones

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer

OVERVIEW

Relativity is a web-based document review platform (application) that supports the management and review of coded data, full text, scanned images, and native files. It can process electronic files, employ data-analytic tools to conduct analysis, integrate with other CFTC applications, and generate documentation for information sharing. Relativity organizes documents based on concepts enabling users to find and group similar documents, train the system to analyze documents based on key terms, and run advanced keyword analysis. The Division of Administration Information Technology Legal Technology (eLaw) operates and manages Relativity for the CFTC. Litigation Support Specialists (LSSs), Subject Matter Experts (SMEs) and Electronic Document Discovery (EDD) staff support Relativity from front to back ends.

The majority of the information in Relativity comes from the CFTC's Division of Enforcement's (DOE) activities, but other divisions and sources also provide information, including the Market Participants Division (MPD), Division of Market Oversight (DMO),Office of the General Counsel (OGC), Division of Clearing and Risk (OCR), Office of the Executive Director (OED), Office of Legislative Affairs (OLA), and the Office of the Inspector General (OIG). Relativity is used for a variety of purposes, including to support CFTC litigation and other enforcement actions from discovery through case resolution; to maintain and manage records of enduring value, related to significant events, milestones, or decision-making by individuals in executive leadership; to capture departing employees' email and other work-product to preserve for knowledge transfer; and to facilitate responding to Freedom of Information Act and other external information requests.

The sources of information in Relativity are both external and internal. External sources can include third parties, opposing parties in litigation, or other government agencies. Internal sources can include the CFTC's forensics team, emails, departed employees' files, and the FOIA team. All information, regardless of source, is received by CFTC's Central Processing Intake Team and then processed and loaded into Relativity for analysis. This can include legacy system case documentation, audio-visual files and recordings, and extracts from files to be incorporated into case-management functions. After undergoing centralized scanning for viruses and malware, data is moved into litigation support network share drives in preparation for ingestion into Relativity. Partner systems, such as CloudNine, Nexidia, and CaseMap process and provide analytic products and data such as legacy data organization, audio-video transcription, text analysis, and complex case management to Relativity. While this information is ultimately housed in Relativity, it may be sent to other CFTC applications for additional processing and analysis, such as CloudNine, Nexidia, and CaseMap.

1. AUTHORITIES AND OTHER REQUIREMENTS

1.1 What legal authority(ies) permit or require the CFTC to collect, use, maintain, or disseminate the information in the system, project, or program?

The Commodity Exchange Act, 7 U.S.C. § 1 et seq., and the rules and regulations promulgated thereunder, establishes the CFTC and provides the authority for the CFTC's regulatory, enforcement, and market oversight activities as well as the authority for general operations of the CFTC, all of which may lead to the collection, maintenance, use, and dissemination of information in Relativity. The Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act of 1974, 5 U.S.C. § 552a establish the authority and requirements for providing to members of the public and to individuals information that may also be contained in Relativity. In addition, the Administrative Procedure Act, 5 U.S.C. §§ 551-559, Federal Rules of Civil Procedure, and state and federal statutes and case law govern the preservation, collection, and production of information in connection with regulatory activities, actual or anticipated litigation, and responses to subpoenas, all of which may lead to the collection, maintenance, use, and dissemination of information in Relativity.

1.2 Is there a Privacy Act System of Records Notice(s) (SORN(s)) that applies to the information in the system, project, or program? If yes, please identify it. If no, please explain why not.

Yes. The CFTC-3, Docket Files for Reparations and Administrative Adjudication, CFTC-10, Investigatory Records, CFTC-16, Enforcement Case Files, CFTC-17, Litigation Files – OGC, CFTC-29, Reparations Cases Closed in the Complaints Section, CFTC-39, Freedom of Information Act Requests, CFTC-45, Comments Online, and CFTC-49, Whistleblower Records, SORNs may apply to certain records in Relativity. The CFTC's SORNs are available at CFTC.gov/privacy.

1.3 Please identify the applicable accreditation boundary evaluated during the Authority to Operate (ATO) process. If the system is hosted by a Cloud Service Provider (CSP), please identify the CSP and state whether the system has Federal Risk and Authorization Management Program (FedRAMP) authorization.

The applicable accreditation boundary is Legal Technology Services – Relativity, which was issued an ATO on May 22, 2023, and placed into continuous monitoring.

1.4 Is there a records retention schedule(s) approved by the National Archives and Records Administration (NARA) that governs the retention of the records maintained in the system, project, or program? If yes, please identify the schedule. If not, please explain.

Yes. The records in Relativity vary in type and are subject to different retention schedules. These include General Records Schedule (GRS) 4.2, Item 020, Access and disclosure request files (DAA-GRS-2016-0002-0001) and GRS 6.1, Item 010, Email and other electronic messages of Capstone officials (DAA-GRS-2022-0006-0001). They also include CFTC Mission Schedules 301, Legal Representation and

Advice (DAA-0180-2018-0006-0003); 401, Customer and Official Inquiry Files (DAA-0180-2012-0003-0001); 402, Investigations Closed without Litigation (DAA-0180-2012-0003-0003); 403, Enforcement Case Files (DAA-0180-2012-0003-0006); 404, Closed Matter Summaries (DAA-0180-2021-0002-0001); 405, Whistleblower Submission Files (N1.180.12.2); 407, Non-records from Record Codes 401, 402, and 403 (CFTC Filing Instruction); 411, Docket Files - Cases filed from October 2010 to present, Permanent records in each docket file (DAA-0180-2013-0005-0004); 412, All other Docket Files - Cases filed from October 2010 to present, All other Records (DM-0180-2013-0005-0005); 414, Docket File Tracking Systems (DAA-0180-2015-0001-0003); 423, Administrative Wage Garnishment Case Files (DAA-0180-2015-0001-0004); and 431, Landmark Inquiries, audits, investigations, litigations and similar events (DAA-0180-2021-0001-0001).

1.5 Please list all forms or other information collection instruments that are used to collect the information in the system. If the information collected is subject to the Paperwork Reduction Act, provide the name of the form or information collection and the applicable OMB control number.

Not applicable.

2. INFORMATION

2.1 Identify the information that the system, project, or program collects, maintains, uses, or disseminates.

Relativity includes a variety of information gathered in the course of investigating and litigating matters under the CFTC's jurisdiction, responding to subpoenas, responding to FOIA and Congressional requests, processing the CFTC's regulatory activities such as rulemakings, and maintaining as needed emails, guidance, and work product.

This various information may contain information about individuals who, for example, are the subject of an investigation or information request to the CFTC, involved in litigation or enforcement action as a witness, defendant, complainant, or otherwise, or who have otherwise been engaged with the CFTC, such as through providing comment in a rulemaking proceeding. The information in Relativity also includes information about current and departed employees and contractors.

Elements of PII in Relativity may contain personal and financial identifying numbers (e.g., social security number, driver's license number, and employee ID), biographical and appearance information (e.g., name, date of birth, citizenship, height, weight, and race), contact and employment information (e.g., phone number, email, address, and employer).

2.2 Is the information collected directly from the individual and, if not, what are the sources of information collected. How is the information obtained?

Relativity does not collect information directly from the individual. However, information is obtained by the CFTC from parties to litigation, sources in an investigation, individuals seeking information from or providing information to the CFTC, and other third parties and government agencies, who may provide information about themselves and/or others and which may ultimately be placed into Relativity. The CFTC may receive information from these external sources via encrypted media, secure file transfer protocol (SFTP), email, or other electronic means and by regular mail or other non-electronic delivery mechanisms. The CFTC also collects and maintains in Relativity information from other CFTC internal systems, such as email servers, shared drives, SharePoint sites, and Comments Online for purposes of litigation holds, internal investigations (including Whistleblower data), to respond to FOIA, Privacy Act, or Congressional requests, or to process public comments related to regulatory activity.

Regardless of its source, information is scanned for viruses and malware and formatted for processing in Relativity and the smaller systems with which it interacts to render analyses. After undergoing centralized scanning for viruses and malware, data is moved into litigation support network share drives in preparation for ingestion into Relativity. Partner systems, such as CloudNine, Nexidia, and CaseMap, process and provide analytic products and data such as legacy data organization, audio-video transcription, text analysis, and complex case management to Relativity.

2.3 What steps are taken to minimize the collection of information in the system, project, or program?

Given the general investigative nature of the information contained in Relativity, generally steps are not taken to minimize the collection of data in the system. It is not always clear at the outset what information will be relevant to a particular matter and Relativity functions to ingest voluminous quantities of information and records in order to organize it and enable analysis.

2.4 Discuss how the accuracy, integrity, and/or quality of the information identified above are determined.

Relativity processes raw data that must remain in the state provided for purposes of an investigation or litigation, a FOIA response, effectuating a knowledge transfer, or preserving records of enduring value. In some instances, determining the accuracy, integrity, or quality of the information is facilitated within Relativity; discovering any misrepresentations in the information is a core function of CFTC's investigations. Additionally, the CFTC carefully tracks data coming into Relativity to establish chain-of-custody and maintain its integrity for use in litigation. The CFTC may also require that entities that produce data do so in accordance with the CFTC's Data Delivery Standards to ensure data quality.

2.5 Privacy Impact Analysis: Related to the Collection and Characterization of the Information

There is a risk that Relativity will collect more information than is necessary to fulfill its business purpose and that the information will not be accurate. While CFTC intakes voluminous information that is not filtered initially, through case management and analysis, identification and refinement of relevant information occurs. Additionally, requests in litigation are tailored towards the information required; they are designed to solicit information relevant to a particular case. While this risk is not fully mitigated due to the nature and purpose of Relativity, as described above, the protocols in place for taking in discovery responses in litigation or responding to same contribute to collecting only what is necessary in a particular instance do work to mitigate any over-collection. Likewise, the accuracy of the information is ensured to the greatest extent possible in context as described above.

3. USE OF THE INFORMATION

3.1 Describe how the information is used internally at the CFTC to support a business purpose.

The information in Relativity is collected, used, maintained and disseminated to support CFTC litigation and other enforcement actions from discovery through case resolution; to maintain and manage records of enduring value, related to significant events, milestones, or decision-making by individuals in executive leadership; to capture departing employees' email and other work-product to preserve for knowledge transfer; and to facilitate responding to FOIA and other external information requests.

3.2 Identify all programs or offices, and an approximate number of individuals, within the CFTC that have assigned roles and responsibilities with respect to the system, project, or program or with whom information is shared. Explain how each uses the information.

The CFTC restricts access to Relativity to those employees and contractors who have a need to know the information to perform their job duties. Relativity is primarily managed and used by DA-IT Legal Technology Services. In total approximately 300 CFTC employees and contractors from the Division of Enforcement, the Office of the General Counsel, and the Office of the Inspector General can access Relativity to review large volumes of information. In addition to the federal employees serving in those areas, contract employees use Relativity to provide both mission-specific and technical system support.

3.3 Privacy Impact Analysis: Related to the Internal Access and Use

There is a risk that unauthorized users may access the system or that authorized users may access the information and use it in a manner that is inconsistent with the purpose for which it is being collected and maintained. This risk is mitigated through the use of Role Based Access Controls (RBAC) that limit access to only

those who have a need to know the information in Relativity and only to the subset of information relevant to their business need. For example, DOE attorneys and investigators and FOIA processors only access matters and cases for which they have authorization. Relativity has functionality built to track and identify what has been accessed by an individual end user which can be reviewed as needed. Additionally, all users receive training regarding the proper use of Relativity and agree to CFTC Rules of Behavior prior to being granted access to the system.

4. INFORMATION SHARING

4.1 Is the information shared outside of the CFTC as part of usual agency operations? If so, identify the organizations or individuals with whom the information is shared, how and *why* it is shared, and how it is to be used.

Once data is processed and analyzed in Relativity, CFTC attorneys may approve the sharing of data via secure transmission with opposing counsel or other government agencies to comply with disclosure requirements related to litigation matters. While certain information in Relativity becomes public, e.g., comments submitted to proposed rulemakings, much of the information collected, used, disseminated and maintained in Relativity is confidential and is generally not publicly available.

This includes information provided by individuals, firms, and other regulators for investigatory and enforcement purposes; information from forensic searches and collections pursuant to court order or discovery rules; and certain information from other CFTC systems, to include, for example, information needed for internal investigations or to respond to FOIA or Privacy Act requests or to requests from Congress.

Information in Relativity may be shared outside of the CFTC with contractors who provide support to the system so that they can trouble shoot technical issues; with FOIA and other requesters when the information is responsive to a request and releasable under applicable law; with opposing parties in litigation and to courts and other adjudicative bodies; and with other Federal and State agencies as a part of cooperative enforcement initiatives. Sharing outside of CFTC is done via postal mail or other secure delivery services, secure email, secure file transfer protocol, or on external media.

4.2 How is the information sharing described in 4.1 compatible with the purpose for which it was originally collected described in 3.1?

The sharing described above is done to achieve the purposes described in 3.1 and/or consistent with the SORNs applicable to the records being disclosed. All disclosures of records that are covered by the Privacy Act are consistent with applicable routine uses in the relevant SORNs. For example, blanket routine use 2 permits sharing with the Department of Justice, the Securities and Exchange Commission, the United States Postal Service, the Internal Revenue Service, the

Department of Agriculture, the Office of Personnel Management, and with other Federal, State, local, territorial or Tribal law enforcement or regulatory agencies for use in meeting their statutory and regulatory requirements; blanket routine use 13 permits sharing with personnel performing or working on a contract, service, grant, cooperative agreement, or job for the Federal government; and blanket routine use 15 permits sharing with the Department of justice or in a proceeding before a court, adjudicative body, or other administrative body before which the agency is authorized to appear, when CFTC is involved and the information is relevant and necessary to the litigation.

4.3 Is the information sharing documented in a Memorandum of Understanding, other information sharing agreement, or a contract?

Contractor access to Relativity is subject to a contract with the CFTC. Certain information sharing with other agencies is permitted by 7 U.S.C. §§ 12 and 16 and documented via access agreements executed under authority delegated to the Director of Enforcement. Other sharing in the context of litigation is done pursuant to requirements and restrictions in law and regulation.

4.4 Are there limitations on re-dissemination of the information by the third party in place, either in the documents identified in 4.2 or otherwise?

The contract limits the use of the information accessed by contractor staff to only that which is necessary to meet the requirements of the contract. The cooperative access agreements entered into with other agencies govern the appropriate use of the information provided. When information is disclosed in the context of litigation, there may be a protective order restricting further use and dissemination of the information. In other instances, such as when information is provided pursuant to the FOIA or the Privacy Act, there is no restriction on what the recipient may do with that information though it would have been redacted as permitted or required by applicable law.

4.5 Describe how the system, project, or program accounts for and maintains a record of disclosures outside of the CFTC.

For those other instances in which Privacy Act covered information is disclosed external to the CFTC from Relativity, the litigation support branch records the date, nature, and purpose for sharing the information and the name and address of the entity or person to whom it will be disclosed.

4.6 Privacy Impact Analysis: Related to Information Sharing

There is a risk that information in the system will be disclosed outside of the CFTC for a purpose that is not consistent with the purpose for which it was collected and/or that once shared it will be further disseminated for an unintended purpose. This risk is mitigated by sharing information only in accordance with the applicable SORNs and/or, where the records shared are not covered by the Privacy Act,

consistent with applicable laws and regulations; and by establishing language in contracts and information sharing agreements that clearly defines appropriate use of the information.

5. DATA RETENTION

5.1 Explain how long and for what reason the information is retained.

Information in Relativity is retained in accordance with applicable retention schedules identified in Section 1, which vary in accordance with the type of information. Records are archived, deleted, or destroyed in accordance with the archiving SOP for information in Relativity. Retention timelines vary significantly. For example, investigations closed without litigation, enforcement case files, and non-records are transferred to off-site storage or destroyed 30 days after last related actions, appeal, or matter or case closure. Some records like docket files, administrative wage garnishment case files, access and disclosure request files, are generally maintained for 3 years. Customer and official inquiry files and legal representation and advice records are retained for 5 and 10 years, respectively. Some records are maintained for a mid-range of 15 years such as landmark inquiries, audits, and investigations and whistleblower submissions. Records like email and other electronic messages of capstone officials and permanent docket case files are transferred to NARA after 30 years. Closed matter summary records are maintained 50 years after matters are closed, and docket file tracking systems records are maintained until they are no longer needed for business.

The records are maintained and then disposed of in accordance with records disposition schedules for the records involved, as approved by and per the CFTC records schedule. When information is subject to a litigation hold, the normal retention period is suspended during the hold. When the litigation hold ends, the normal retention schedule applies, and the CFTC works to dispose of information according to the schedule.

Relativity has a robust tracking function that records the date a file is imported, altered or amended (the latter permitted only in cases of applying redactions for disclosure in litigation), and deleted.

5.2 Describe how the information is disposed of at the end of its retention period.

Once records in Relativity have reached the end of their retention period and are approved for disposal, CFTC staff or contractors under the supervision of CFTC staff permanently dispose of the related information. In most circumstances for information moving through Relativity, matters reach closure status and access is removed. Then, data is archived. The information stored in file shares is backed up. Records are then retired to NARA facilities in accordance with prescribed schedules and any backups are destroyed. Records are deleted in accordance with the CFTC Records Management Manual and using the Records Destruction Approval Form. On a quarterly basis in accordance with an SOP, closed matters are

identified for archiving in accordance with approved Department of Enforcement Records Schedule: 5 years for Leads, Preliminary Inquiries, and Investigations; 15 years for Litigations; and indefinitely for Permanent Records (matters identified as historical). Per standard operating procedures, electronic folders are designated in the Relativity Workspace. At the end of retention periods, records are transferred to NARA.

5.3 Privacy Impact Analysis: Related to Retention

There is risk that information in Relativity may be kept longer than is necessary to meet the business need for which it was collected. This risk is mitigated by transferring data to archive data shares for evaluation followed by deletion of source records in accordance with the applicable retention schedule. Further, quality control checks are done by team members following quarterly archiving. This risk is also mitigated by having in place and adhering to an SOP regarding record retention in Relativity.

6. NOTICE

6.1 How are individuals provided notice prior to the collection of their information? If they are not provided notice, please explain why.

Relativity does not collect information directly from individuals and, therefore, does not provide notice directly to individuals. Rather, Relativity processes information in records received from other CFTC systems and input by CFTC staff. To the extent required, notice is provided to individuals at the point of the original collection of information. Notice is also provided to the public about what information is collected and for what purposes via publication of the SORNs identified in Section 1.2. Notice is also provided through this PIA.

6.2 Do individuals have the opportunity to consent to the use of their information or decline to provide their information? Please explain.

Individuals do not interact directly with Relativity and do not have the opportunity to consent to the inclusion of their information in the system.

6.3 Privacy Impact Analysis: Related to Notice

There is risk that individuals may not receive adequate notice concerning why their information is being collected and how it will be used. Where applicable, this risk is mitigated via Privacy Act statements at the point of collection from the individual and is also mitigated via publication of the applicable SORNs and as well as through publication of this PIA. Given the nature of the records collected for investigations and litigation, it may not be feasible or required to provide notice to individuals about the collection and use of their information.

7. REDRESS

7.1 What procedures are in place that allow individuals to access their information?

Certain records contained in Relativity are included in Privacy Act systems of records that have been exempted from the access and amendment provisions of the Privacy Act. Individuals may request access to non-exempted records by following the procedures outlined in the relevant SORNs and the Commission's regulations at 17 C.F.R. Part 146.

7.2 What procedures are in place to allow individuals to correct inaccurate or irrelevant information about themselves?

Certain records contained in Relativity are included in Privacy Act systems of records that have been exempted from the access and amendment provisions of the Privacy Act. Individuals may request amendment to non-exempted records by following the procedures outlined in the relevant SORNs and the Commissions regulations at 17 C.F.R. Part 146.

7.3 How are individuals notified about the procedures for correcting their information?

The procedures for submitting a request to correct Privacy Act covered information are outlined in the applicable SORN and/or in the Commission's regulations at 17 CFR Part 146.

7.4 Privacy Impact Analysis: Related to Redress

There is a risk that individuals will not be able to access information about themselves that is contained in the system nor be afforded an opportunity to correct that information. This risk is mitigated by providing individuals, where required and appropriate, with information about how to access and request amendment of their records through the instructions provided in the applicable SORNs and relevant Commission regulations.

8. AUDITING AND ACCOUNTABILITY

8.1 How is the information in the system secured?

CFTC employs a variety of physical, technical, and administrative controls to secure Relativity. Information within Relativity is generally only accessible within the CFTC environment using CFTC-issued equipment. Access is limited by user role and "need-to-know." Further, multiple layers of approval are required for CFTC personnel to be granted access, personnel are required to follow CFTC Rules of Behavior, and annual security and privacy awareness training are required.

8.2 Are audit logs generated reflecting access and use of the information in the system? If not, please explain. If so, please describe how often they are reviewed and for what purpose.

Relativity has robust audit logs that are created continuously, whenever an action in the system is taken, and that contain information regarding login/logout, records viewed, and downloads. Logs themselves include very limited PII. Audit logs are reviewed as needed to troubleshoot any user and system anomalies.

8.3. What procedures are in place to determine who has access to the system, and are they documented?

Each CFTC practice area, Division, or Office has a Chief Trial Attorney (CTA) who determines role-based access needs. CFTC staff members route access requests through supervisors, managers, and CTA to the LSS. Then, the Electronic Document Discovery team processes the requests, grants access, and configures user functionality.

8.4 Describe what privacy training is provided to users, either general or specific to this system or project.

All CFTC staff and contractors are required to complete Cybersecurity and Privacy Awareness Training prior to gaining access to the CFTC network and annually thereafter. Users who do not complete the annual training lose their access. No additional role-based training is provided.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

There is a risk that the system is not audited and that the Commission is not accountable concerning the collection, maintenance, and use of the information in the system. This risk is mitigated because audit logs are generated and reviewed as needed to troubleshoot any user and system anomalies. It is further mitigated because the Electronic Document Discovery team has ultimate accountability for who has access to the system and at what level. Additionally, all users who access the system receive annual training and are required to sign rules of behavior.