Federal Trade Commission
Privacy Impact Assessment

JND Claims Administration System (JND-CAS)

March 2019

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission's (FTC) Bureau of Consumer Protection (BCP) brings law enforcement actions that can result in the recovery of redress money from defendants that is to be returned to injured consumers or businesses. The FTC distributes money pursuant to a distribution plan that is either approved by a court or an administrative law judge or delegated to the FTC's discretion. The FTC Office of Claims and Refunds (OCR) is responsible for administering and coordinating redress activities, and JND Legal Administration (JND), an FTC notice and claims administration contractor, supports OCR's activities. This PIA explains what personally identifiable information (PII) OCR and JND collect throughout the claims administration process, who is allowed to use this information and for what purposes, and what steps are taken to identify, secure, and reduce any privacy risks to that information.

The JND Claims Administrative System (JND-CAS) stores consumer and business data provided by OCR or obtained directly from individuals who submit redress claims in a proprietary database. JND-CAS also has a public interface that permits individuals and businesses to complete and submit an electronic claim form via a website. JND uses the data from the system to fulfill its role as the notice and claims administrator, which includes the following duties: (i) to intake and process claims filed; (ii) to answer questions from FTC and other authorized parties; (iii) to answer questions from claimants and potential claimants as to eligibility and status of materials filed; and (iv) to issue and track payments to authorized claimants.

JND's physical systems are housed in a secure, top-tier datacenter facility located in Seattle, WA.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The FTC collects this information in order to provide redress to injured consumers as part of its law enforcement activities pursuant to the FTC Act, 15 U.S.C. §§ 41-58, and other applicable statutes.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☐ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☒ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☒ Phone Number(s)	☒ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☒ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Business name, unique claimant ID, customer account number. JND operators call summary
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

Note: The online claim filing portion of JND's Claims Administration System will collect and store the IP address of systems used to submit claim data. The IP address is stored in a secure database separate from the Claim Administration System database. This data is not available to claims processors or call center agents and is only accessible by a limited group of approved individuals. IP addresses are collected for system security purposes and if requested by the FTC for fraud analysis or other law enforcement purposes. JND has the ability to disable the collection of IP addresses should the FTC request.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The claimant information that is collected, processed, stored, disseminated, or maintained either within OCR or JND-CAS varies depending upon the administration matter. In routine administration matters, the data elements selected in 2.1 are collected and maintained. Additional non-PII data elements may include business name (if needed), transaction data, transaction dates, product type, company selling product, customer number, customer

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

account number, loss amount, and notes of claimant contact with JND, including any subsequent change requests, updates, corrections, etc.

JND provides a phone number for consumers to call if they have questions. When consumers call the number, the IVR system, which is hosted by NICE inContact, automatically logs the consumer's phone number and the date/time/length of the call for billing and routing purposes. The inContact system is used only to host the toll-free number and route the call to a JND contact center agent located in a JND facility. For calls routed to the JND's contact center, staff may enter a summary of the call into JND's Claims Administration System.

2.3 What is the purpose for collection of the information listed above?

Claimant information is collected, processed, stored, disseminated, or maintained by OCR staff and JND to identify potential claimants, to validate claimants and their claims, and to distribute redress payments to appropriate claimants.

Source of Data	***Type of Data Provided & How It Is Collected***
Individual Members of the Public	Initial source data is found in defendants' files and in consumer complaints submitted to the FTC and transferred to JND; this includes the data elements listed in 2.1. Claimants also provide data directly to JND via phone, Online Claim Form, or via US mail as part of the administration process.
Third Party	Mailing address updates and corrections may be provided by third-party data sources such as the United States Postal Service, Lexis Nexis, Experian, CLEAR, etc.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

FTC staff does not have direct access to the JND-CAS system; JND shares claimant information and reports with the FTC via secure encrypted email, encrypted Secure File Transfer Protocol (SFTP) or other file sharing technologies, all of which are encrypted with industry standard technologies both in-transit and at-rest. Prior to receiving access to any JND information resources, all JND staff, temporary staff, contractors, and consultants undergo a background check. Additionally, any vendors who receive, or have access to, JND information or data are subject to review and assessment in accordance with JND's Vendor Management Policy. See table below.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC Staff	FTC staff reviews the data to ensure that the redress distribution plan is implemented correctly, and to ensure appropriate data security practices are in place.
JND Staff	Authorized JND IT professionals have access to the data for the purpose of importing, validating, updating, and storing claimant data. JND claims processors have access to data for the purpose of validating eligibility, communicating with claimants, and updating claimants' contact information. JND management staff need access to the data for reporting purposes, as well as to supervise technology and processor resources, and ensuring accuracy and adherence to data handling standards. Any communication involving claimant data between JND and the FTC is conducted via one of the secure methods mentioned in 3.1.
Claimants	Claimants will have direct access to claimant information held in JND-CAS. Individual claimants may submit information directly via the Online Claim Form on the claims website. Once submitted, claimants cannot view or change their information online but may modify, or have access to their data, via the methodologies outlined in Section 4.3.
Other External Parties	The FTC may share claimant information with law enforcement and other government agencies, courts, and defendants, or as otherwise authorized by law. OCR and JND securely download and transmit required data in response to authorized requests.

3.2 Do contractors and/or third-party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Yes, JND contractors have access to data in the system. JND employs formal, documented procedures to facilitate privacy and security awareness training, including a specific course related to PII. This training is managed and implemented by JND's Information Technology and Information Security Teams and required to be completed before onboarding and

annually thereafter. Additionally, all system users are required to review all relevant JND policies and control standards. JND maintains a comprehensive privacy policy to which all JND employees, temporary employees, contractors and vendors are required to adhere. JND's privacy policy can be found at http://www.jndla.com/privacy-policy.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third-party service provider.

JND maintains an Incident Response Plan ("IRP") for managing the aftermath of a security breach or cyberattack, or other IT incident, privacy incident, or security incident. The plan contains a framework for responding to incidents, which include situations where confidentiality of sensitive data may have been compromised. The plan includes guidance on dealing with a variety of incidents including, but not limited to, escalation of privilege, compromised credentials, and unauthorized access. No less than annually, these plans are reviewed, updated, approved, and tested by relevant staff, across multiple departments.

The primary goal of the IRP is to restore normal service operation as quickly as possible and to minimize the adverse impact on business operations and FTC data. In the event an incident is identified either by JND's IT staff or in-place utilities (i.e., network equipment), JND has an in-house response team in place to quickly respond and rectify the situation. Preventative measures include: firewalls with Intrusion Detection System/Intrusion Prevention System (IDS/IPS) scanning at all ingress and egress points; centrally managed, host-based, local firewall enabled on each computer; real-time antivirus and antimalware scanning; and IDS/IPS software. A monthly patch management program is also in place to ensure JND systems are protected from all known vulnerabilities and, should an emergency patch be released, IT staff are authorized to override the standard schedule and immediately begin deployment of the patch or update. The breach notification timeframe is governed by contractual and legal requirements; JND must immediately report to the FTC all breaches of FTC materials and information.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

For cases that require JND to collect claimant information via a claim form, a Privacy Act statement is included on both paper and web-based forms, which are compliant with the Paperwork Reduction Act (PRA) and contain an Office of Management and Budget (OMB) document control number. The Privacy Act statement explains the authority, purpose, and routine uses of the information to be collected, whether it is voluntary or mandatory for the claimant to provide the information, and any consequences if the information is not collected (e.g., the FTC may be unable to pay the individual his or her redress claim).

Those claimants who submit consumer complaints to the FTC via the FTC online complaint form – as described in the Sentinel Network Services PIA – or via the FTC telephone

complaint system (1-877- FTC-HELP), receive a similar Privacy Act statement at the time they submit their complaint. Their relevant consumer complaint information is then forwarded to JND for processing through the encrypted mechanisms outlined in section 3.1. All claimants who receive a Privacy Act statement also are provided a physical mailing address and telephone number to update and provide additional information about themselves, their eligibility to file a claim, and their claimant status.

In some cases, the FTC may receive claimant information from a defendant's customer list, and redress may be provided without the claimant having to take any action. In those instances, claimants are not provided with a Privacy Act statement; such claimants can learn about the FTC's collection, use, and disclosure of their information through the FTC's privacy policy, as noted below. In addition, all redress checks include a mailing address and/or telephone number for consumers to contact JND should they have any questions or concerns about their information.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☒ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☐ Other (*explain*):_____

☐ Notice is not provided (explain): _____

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

When the FTC obtains information about injured consumers from a defendant in order to mail checks to such consumers, there is no opportunity for individuals to provide or decline to provide their information. Rather, this use of personal information is consistent with the purpose for which the FTC collects and maintains such consumer information from its defendants and allows the FTC to provide refunds efficiently and effectively to as many injured consumers as possible.

In cases where there is a claims process, individuals can decline to provide their information. If consumers choose to submit a claim, they are consenting to, and may not limit, the routine uses of their information stated in the applicable SORN (see Section 8.3) and Privacy Act statement. The consumer exercises this consent by choosing to complete, sign, and submit a claim form.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Claimants cannot access their records through the system online, but may request access to their claims records by contacting JND via telephone or hardcopy mail. Before making requested changes to a claimant's information, JND will confirm the claimant's identity by

asking a series of questions, including the claim record tracking number, name, mailing address on file, or phone number, and instructing the claimant to forward their change request in writing along with supporting documentation if needed. JND accepts written documentation via fax, mail, or email. Finally, claimants can obtain access to their own information through a Privacy Act request filed with the FTC's Freedom of Information Act (FOIA) Office.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

As stated above in Section 4.3, claimants can request corrections to any inaccurate information by contacting JND, validating their identity, and forwarding the change request in writing along with any supporting documentation as necessary. Claimants also can file a Privacy Act request through the FTC's FOIA Office to obtain access to their own information. The FTC FOIA Office will work with the claimant to respond to any complaints, concerns, or questions.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Various steps are taken to validate the accuracy and timeliness of collected data based on its original source. For example, prior to the contractor mailing a claim form, a redress check, or consumer education material, claimant addresses are standardized and cross-checked against data sources, such as the U.S. Postal Service (USPS) National Change of Address Database and USPS records regarding street names and address ranges. All resulting additions, deletions, and address changes to the data set are approved by the OCR and reconciled against the original source data.

In many instances, claimant data obtained from defendants' files can be used to mail redress checks directly to injured consumers and businesses. In other cases, individuals are contacted to provide or verify their information. For example, claim forms may be mailed to a known set of claimants requesting that they validate their address, loss amount, and entitlement to redress. If a claimant's information is incomplete, JND mails a letter to the claimant informing the individual that their claim is incomplete due to missing or incorrect information; the claimant is sent a new blank copy of the claim form to update their information and complete the claims process. In other cases, claim forms will be made available to previously unknown claimants via case-specific redress notification and outreach. Claimants provide claim information, including their address, injury amount, and entitlement to redress, under penalty of perjury.

The notice and claims administrator reviews claimant names, check distributions, and claim form responses to confirm that the loss amounts claimed are consistent with the established

case-specific claim parameters. OCR staff reviews data entry and decisions made by JND to ensure that the information remains accurate, complete, and up-to-date. Outreach material, redress checks, and claim forms always include an FTC website address for additional information, and a telephone number and mailing address for consumers to contact the redress contractor to have their questions answered and/or to update their information.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Access to system data is based on the Principle of Least Privilege (PLP) and only provided to those individuals with authorization to access. In order to access the JND Claims Administration System (CAS), one must first have access to JND's network via Active Directory credentials and be assigned a second set of credentials specific to JND-CAS. Data is only used in accordance with uses described in the executed contract between the FTC and JND. JND reviews and approves all logical and physical access and authorization levels on a quarterly basis. Each engagement is assigned a specific database in JND-CAS to ensure the most granular of permissions may be assigned.

All data within JND-CAS is encrypted while at rest, and data is encrypted in transit. Information is also received by, and sent from JND, in secure and encrypted transmissions. Once data is received, it is verified, and standardized, before being loaded into a proprietary database in the Claims Administration System to ensure information not necessary to the processing of claims is not stored or retained.

Additional administrative and technical controls implemented to protect system data include:

- Password Complexity;
- System lockouts due to submission of invalid credentials or inactivity;
- Online Claim Filing sites are hosted on a network physically and logically segmented from JND's Claims Administration System;
- As necessary, claimants are provided with pin codes, or unique identifiers, to allow for two-factor authentication;
- Event logging is enabled on all production systems;
- Audit trails are enabled to log all access and modification of information and data in JND-CAS;
- Data is encrypted in-transit and at-rest;
- Security and Privacy awareness and training programs for JND staff;
- Management, Operational, and Technical safeguards are based on NIST 800-53 controls;
- Quarterly logical and physical access reviews;
- Vulnerability management and penetration testing;
- Production System Monitoring;
- Public facing systems are hosted in a DMZ which employs industry standard TLS encryption; and
- NIST 800-53 based controls and framework.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

JND's Development, User Acceptance Testing (UAT), and Productions environments are physically and logically segregated from each other. PII or otherwise sensitive data is never transmitted, processed, or stored in the development environment; and the development team is not permitted access to the production environment. Should FTC data be required for proper User Acceptance Testing, such testing is performed in an environment with security controls commensurate to the Production environment. Access to this environment is limited only to testers, and the data is stored no longer than needed for proper testing.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

JND and the FTC Office of Claims and Refunds will maintain the financial audit logs for claims and the records associated with issuing payments to claimants in accordance with NARA GRS 1.1, item 010, Financial Transaction Records, for a period of six years. Any copies of matter-related documents received by JND and OCR, regardless of format, will be deleted or destroyed as nonrecords per the FTC NARA-approved records retention schedule, N1-122-09-1. Item 2.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

JND does not host any permanent websites on behalf of the FTC. However, JND may host a temporary website in a particular redress matter when the FTC determines it is appropriate and necessary to support online electronic claim submission. Persistent tracking technologies will not be used on these temporary, matter-specific redress sites. Temporary session cookies will be used for user session verification during online claim submission process and will be removed at the end of the visit, when a claim is submitted, and at session timeout. See the FTC's Cookie Page for more information. JND staff reviews each temporary website for compliance with the privacy requirements.

In compliance with the Privacy Act of 1974, the E-Government Act of 2002, guidance issued by OMB, and the FTC's own Privacy Policy, the FTC mandates that JND limit the collection of information from website visitors to the information necessary to assess and improve user experience, respond to consumer concerns, and administer redress.

To the extent that JND's web hosting provider collects standard web log data, such as IP address, date and time of visit, and other required information, for cyber security and

management reporting, such collection is needed to ensure compliance with FISMA, 44 U.S.C. § 3541 et seq.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	***Mitigation Strategy***
Incomplete, inaccurate, redundant or unnecessary sensitive PII data	To reduce the risk of storing incomplete, inaccurate or unnecessary data and information, JND's data control team performs a verification and standardization process before it is uploaded into JND-CAS. To mitigate this, claim forms are designed not to include open-text comment fields. Additionally, fields are configured to undergo data validation to ensure the requested information is entered. Claimants are also presented with the ability to validate and verify their information before submitting. In order to minimize privacy risks, in the vast majority of redress matters, the information stored by JND is limited to name, contact information, and claim information, possibly coupled with validation under penalty of perjury. Comprehensive data security plans have been implemented to protect all data, including frequent, automated scans of information systems as well as policies and procedures to limit access to sensitive data and to ensure compliance with data privacy standards.
Misuse of data by individuals with access to PII or other sensitive information	JND-CAS employs Audit Trail logging to ensure all access to, or modification of, data is logged. Audit data is stored in accordance with JND's data retention policy and in accordance with requirements set forth by the FTC. In all circumstances, audit data will be stored for no less than the lifetime of the engagement. Access to audit data is limited to those who have a reasonable business need and is not accessible by individuals who process claims and claimant information.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

Yes, JND claims system includes automated privacy controls. For example, the user are granted access based on their role, limiting the information only to the projects they are assigned; account lockout after a certain number of consecutive unsuccessful attempts;

auditing and logging of users activities; password requirements, and data encryption at rest and in transit.

Additional administrative, technical, and physical safeguards are outlined in Section 5.2.

JND also maintains annual SOC II certification.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

Yes. The system is covered by Privacy Act SORNs for nonpublic FTC program records, FTC-I-1, and for computer system user and identification access records, FTC-VII-3. Consumers are assigned a unique ID that may be used to index and retrieve their system records for identification, tracking, and reporting purposes.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

JND maintains a suite of Information Security policies and procedures that cover all facets of its business operations. Each employee is required to review and attest to compliance with any and all policies relevant to their duties and responsibilities. It is also required that all organizational policies undergo a formal review and approval process no less than annually. Confidentiality and Non-Disclosure agreements are also reviewed by JND's legal department on an annual basis and, should modification occur, all employees, contractors, and vendors are required to sign the most current version.

During onboarding, and annually thereafter, JND provides mandatory Information Security and Data Privacy Training. Participation in this training is tracked to ensure timely follow-up with any individual who has not met requirements. Staff in certain roles may receive additional training, as needed, such as secure coding practices for developers and specialized training for Information Technology and Network Operations staff. JND also, no less than monthly, disseminates Information Security focused alerts that, for example, may focus on privacy requirements, new phishing techniques, indicators or compromise for emerging threats, or general security best practices information.

JND adheres to principal of least privilege and performs each quarter a full review of all authorization and access levels. Each facility manager is responsible for reviewing physical access to the facility or datacenter in their purview. A Logical access review is also performed each quarter and includes all Active Directory and JND Claims Administration System accounts and access levels. All access reviews are tracked in JND's ticketing system and project managers can immediately make modifications or corrections.

JND-CAS has account management policies and controls in place to manage system accounts, including the establishment, activation, modification, and termination of system accounts. JND's account management activities include:

- Identification of account types;
- Conditions for group membership;
- Identification of authorized users specifying access privileges;
- Requirement of appropriate approvals for requests to establish accounts;
- Establishing, activating, modifying, disabling, and removing accounts;
- Specifically authorizing and monitoring use of the guest/anonymous and temporary accounts;
- Notifying account managers when temporary accounts are no longer required and when users are terminated, transferred, or access requirements change;
- Deactivating temporary accounts and accounts of terminated users as required;
- Granting access to the system based on valid access authorization; intended system usage, and other attributes as required by the organization; and
- Reviewing accounts quarterly, at a minimum.

The collection, use, and disclosure of information from the JND-CAS system has been reviewed to ensure consistency with the FTC's Privacy Policy.