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 for injured consumers or businesses. The FTC distributes money pursuant to a plan that is approved by a court, approved by an administrative law judge, or delegated to the FTC's discretion.

The Office of Claims and Refunds (OCR) is responsible for administering and coordinating redress activities, and Epiq Class Action & Claims Solutions, Inc. (EPIQ) – an FTC notice and claims administration contractor – supports OCR's activities. This Privacy Impact Assessment (PIA) explains what Personally Identifiable Information (PII) OCR and EPIQ collect throughout the redress administration process, who is allowed to use this information and for what purposes, and what steps are taken to identify and mitigate any privacy risks.

EPIQ's Claims Administration System (Secure Matrix) system stores in a proprietary database consumer and business data provided by OCR or obtained directly from individuals who submit redress claims. EPIQ in specific cases might set up an online claims submission website that permits individuals and businesses to submit an electronic claim. EPIQ uses the data from the system to fulfill its role as the redress administrator, which includes the following duties: (i) to intake and process claims filed; (ii) to answer questions from the

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 <u>all</u> that apply.

- ☒ Full Name
- ☐ Date of Birth
- ☒ Home Address
- ☒ Phone Number(s)
- ☐ Place of Birth
- ☐ Age

Additional non-PII data elements may include: business

2.4 What are the sources of the information in the system/project? How is the information collected?

Individual Members of the Public	Initial source data comes from defendants' files and consumer complaints submitted to the FTC and transferred to EPIQ; this includes the data elements listed in 2.1. Claimants also provide data directly to EPIQ via phone or mail as part of the refund administration process.
Third Parties	Mailing address updates and corrections may be provided by third-party data sources such as the United States Postal Service (USPS), LexisNexis, 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.

	EPIQ claims processors and call center agents who are assigned to work on a specific FTC matter are granted access to data for the purpose of validating eligibility, communicating with claimants, and updating claimants' contact information. EPIQ management staff need to access the data for reporting purposes, as well as to supervise technology and processor resources, and ensuring accuracy and adherence to data handling standards. All EPIQ employees with access to claimant information undergo background checks completed by EPIQ Human Resources.
Claimants	If the claims and refunds matter requires that EPIQ set up a temporary website, individual claimants may submit information directly via online or hardcopy claim forms. Once claimants submit their information, they cannot view or change their information online.
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 EPIQ securely download and transmit required data in response to authorized requests. EPIQ may share with third-party payment processors (banks, for example) data necessary to issue payments to consumers.

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.

EPIQ maintains formally defined roles and responsibilities, separation of duties, and access requirements for all employees. All EPIQ employees receive initial and annual refresher privacy awareness and role-based information securiyb004 Tcsa(E)-12 03 T(nks)-1 (, Tm2.75 -2.3 Tde)1T0 Tv

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.

EPIQ Incident Response Plan, which includes the privacy incident response plan, provides a roadmap for implementation and defines reportable incidents, provides metrics, defines resources and management support needed. The Incident Handling Process includes the following six-phases: preparation, identification, containment, eradication, recovery, and follow-up to incidents relating to PII. EPIQ uses a Web Portal and email to automate the notification, processing, and reporting incidents. EPIQ must immediately report to the FTC any breach of FTC information.

EPIQ tests the Incident Response capabilities on an annual basis to determine the effectiveness of the plan. EPIQ personnel are also trained in their incident response roles and responsibilities with respect to the information system. The following are tested during the response exercises:

- Test reporting mechanisms to ensure that security events are routed through the appropriate management channels as quickly as possible.
- Employee responsibilities ensure that all employees, contractors and third party users know their responsibilities assigned in the plan.
- Responsiveness by employees to quickly and effectively carry out their duties in response to information security incidents.
- Follow-up corrective and management actions after an information security incident have been detected.
- Ensuring collection, retention, and preservation of evidence required for the activity.
- Documenting the incident and storing the reports and information electronically.

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.

Claims and refunds cases that require EPIQ to collect claimant information via a claim form if the informatic

In some cases, the FTC may receive claimant information from a defendant's customer list, and a refund 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 refund checks include a mailing address and/or telephone number for consumers to contact EPIQ 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 from a defendant about injured consumers in order to mail them their checks, 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 eff(or)3 o proviefon maintaiormafu (t)-2 (To)10.9 (vi)59 (

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

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system

7

	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	EPIQ employs a Security Event Information Management system (SEIM) to ensure all access to, or modification of data is logged. Audit data is stored in accordance with the EPIQ 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 one year. 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.

EPIQ Secure Matrix system includes automated privacy controls to protect the privacy of victim data. Example controls include, but are not limited to:

- Users are uniquely identified;
- Use of multi-factor authentication;
- Role-based access based on business need;
- Session termination after periods of inactivity;
- System lock-out after a certain number of failed attempts to log in;
- Automatic suspension of inactive accounts; and,
- Auditing and logging of system activities.

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

their continuous monitoring process. The account management policies and controls in place to manage EPIQ user accounts include the establishment, activation, modification, and termination of system accounts. The collection, use, and disclosure of information from the Secure Matrix system has been reviewed to ensure consistency with the FTC's Privacy Policy.