



Federal Trade Commission
Privacy Impact Assessment

Epiq Class Action & Claims Solutions, Inc.

Claims Administration System

October 2019

Table of Contents

| | | |
|---|------------------------------------|----|
| 1 | System Overview | 1 |
| 2 | Data Type, Sources, and Use | 2 |
| 3 | Data Access and Sharing | 4 |
| 4 | Notice and Consent | 6 |
| 5 | Data Accuracy and Security..... | 7 |
| 6 | Data Retention and Disposal..... | 9 |
| 7 | Website Privacy Evaluation..... | 9 |
| 8 | Privacy Risks and Evaluation | 10 |

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 FTC and other authorized parties; (iii) to answer questions from claimants and potential claimants; and (iv) to issue and track payments to authorized claimants.

EPIQ maintains physical systems in their secure on-site location in Las Vegas, NV.

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 refunds 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.

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

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 within OCR or within EPIQ's Secure Matrix proprietary database varies depending upon the redress matter. In routine refund matters, the data elements selected in table 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 account number, loss amount, and notes of claimant contact with EPIQ, including any subsequent change requests, updates, corrections, etc. These notes may potentially contain PII. For example, a consumer may call EPIQ to update their current address, phone number, etc.

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.

In instances where a consumer calls EPIQ regarding a claims matter, the EPIQ Interactive Voice Response (IVR), which is hosted in colocation datacenter located in Las Vegas, NV , automatically logs the consumer’s phone number and the date/time/length of the call for billing and routing purposes. If the consumer chooses to talk to a live agent, the call is routed to an EPIQ contact center agent located in EPIQ facility. All consumers’ calls to live agents are recorded. Details of calls may be summarized in the EPIQ claims management system by claims processing staff.

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 EPIQ to identify potential claimants, to validate claimants and their claims, and to distribute redress payments to appropriate claimants.

The EPIQ Secure Matrix system maintains claimant information for verification and record-keeping purposes relating to refunds in FTC matters, as well as to calculate and distribute refund payments. These activities may include printing and mailing claim forms, processing claims and corrections submitted by claimants, issuing checks or other forms of payment, and providing consumer education.

Data collected by EPIQ in a specific FTC matter may also be used by the FTC and EPIQ to identify potentially fraudulent claims submitted in other FTC refund matters. For each refund matter managed by EPIQ on behalf of the FTC, EPIQ sends a complete list of claims filed to the FTC prior to the scheduled distribution. In an effort to identify potentially fraudulent claims, the FTC may analyze that information, refer back to data received in all refund matters past and present, and provide information regarding potentially fraudulent claims back to EPIQ.

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

| <i>Source of Data</i> | <i>Type of Data Provided & How It Is Collected</i> |
|----------------------------------|--|
| 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.

| <i>Data Will Be Accessed By and/or Provided To:</i> | <i>How and Why the Data Will Be Accessed/Shared</i> |
|---|--|
| FTC Staff | <p>FTC staff does not have direct access to the Secure Matrix system. EPIQ shares claimant information and reports with the FTC via secure encrypted file transfer protocol or other secure file sharing technologies, all of which are encrypted with industry standard technologies both in-transit and at-rest.. The FTC reviews the data to ensure that the redress distribution plan is implemented correctly and to ensure appropriate data security practices are in place.</p> |
| EPIQ Staff | <p>Authorized EPIQ IT professionals have access to the data for importing, validating, and storing claimant data.</p> <p>Authorized EPIQ data analysts' have the additional access to perform mass updates, such as parsing of names and National Change of Address updates.</p> <p>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.</p> <p>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.</p> <p>All EPIQ employees with access to claimant information undergo background checks completed by EPIQ Human Resources.</p> |
| Claimants | <p>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.</p> |
| Other External Parties | <p>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.</p> <p>EPIQ may share with third-party payment processors (banks,</p> |

| <i>Data Will Be Accessed By and/or Provided To:</i> | <i>How and Why the Data Will Be Accessed/Shared</i> |
|---|---|
| | 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 security training. Access to the Secure Matrix system is granted after the user has taken the training. The security awareness training program is administered by the Risk and Compliance team and includes specific training related to handling of PII.

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 will always provide claimants with a Privacy Act statement, whether the claim form is paper or Web-based. The Privacy Act statement explains the authority, purpose, and routine uses of the information to be collected; whether the information is voluntary or mandatory; and any consequences if the information is not collected (e.g., the FTC may be unable to pay the individual his or her refund 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 Analytics for processing through the encrypted mechanisms outlined in section 3.1.

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 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 they may request access to their claims records by contacting EPIQ via telephone or mail. Before making changes, EPIQ asks consumers a series of questions, including the tracking number and mailing address on file. The claimant is instructed to forward their change request in writing along with supporting documentation if needed. EPIQ accepts written documentation via mail. The system does not display/send PII as part of the inquiry process. If PII is collected and/or transmitted, encryption methods are implemented to protect sensitive information. 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.

Consistent with 4.3, claimants are provided with dedicated contact information to correct inaccurate or erroneous information. The process for receiving and responding to the requests is outlined in 4.3 and 5.1.

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 EPIQ mailing a claim form, refund check, or consumer education material, claimant addresses are standardized and cross-checked against known data sources, such as the USPS National Change of Address Database and U.S. Postal Service records regarding street names and address ranges. All resulting additions, deletions, and 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 refund checks directly to injured consumers and businesses. In other cases, individuals are contacted to provide or verify their information themselves. For example, claim forms may be mailed to a known set of claimants requesting that they validate, often under penalty of perjury, their address, loss amount, and entitlement to a refund. In other cases, claim forms will be made available to previously unknown claimants via case-specific notification and outreach. Again, claimants provide claim information, including their address, injury amount, and entitlement to a refund, often under penalty of perjury.

EPIQ 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 EPIQ to ensure that the information remains accurate, complete, and up-to-date.

Outreach material, refund checks, and claim forms always include an FTC website address for additional information, as well as a telephone number and mailing address for consumers to contact the refund administrator 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.

The Secure Matrix system uses a layered defense approach to protect sensitive information. The network itself is isolated from other EPIQ networks and systems with only service-specific access allowed for approved applications. All communication in and out of the information system is encrypted and signed using government approved encryption protocol. Data is encrypted at rest. Administrative tasks require both network level authentication and an authorized Smart Card. The ability to copy information in and out of the system is also restricted.

If personal information is collected through an online form, it is protected using NIST-approved encryption algorithms.

Only authorized EPIQ staff can access the system, on a need-to-know basis. The data is accessed via secure login and is encrypted at rest. In addition, the FTC instructs EPIQ to collect the least amount of claimant information.

Prior to maintaining and disseminating claimant data, OCR staff removes all unnecessary information from the claimant data file. OCR staff only forwards encrypted data to refund administrators. Similarly, EPIQ is instructed to collect the least amount of claimant information necessary.

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?

Not Applicable. EPIQ does not use PII in the system testing, training, or research.

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?

EPIQ and OCR 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 six years. Any copies of matter-related documents received by EPIQ 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.

EPIQ does not host permanent websites on behalf of the FTC. However, EPIQ may host a temporary website in a particular refund 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 claims and refunds sites. Temporary session cookies are used for user session verification and are terminated at the end of the visit. These cookies do not hold any PII, and the information they obtain cannot be directly correlated to an individual claimant. EPIQ 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 EPIQ limit the collection of information from website visitors to the information necessary to assess and improve user experience, respond to consumer concerns, and administer claims and refunds.

To the extent that EPIQ 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 in compliance with the Federal Information Security Management Act of 2002 (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?

| <i>Risk</i> | <i>Mitigation Strategy</i> |
|---|--|
| Incomplete, inaccurate, redundant or unnecessary sensitive PII data | <p>To reduce the risk of storing incomplete, inaccurate or unnecessary data and information, the EPIQ data control team performs a verification and standardization process before it is uploaded into Secure Matrix. To mitigate this, claim forms do not 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.</p> <p>In order to minimize privacy risks, in the vast majority of redress matters, the information stored by EPIQ 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.</p> |
| 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 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?

As described in sections 8.2 and 5.2, EPIQ has technical and operational policies and controls in place to ensure data is safeguarded and to prevent misuse or accidental claims data modification. EPIQ staff perform regular, ongoing reviews of system logs as part of 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.