U.S. Securities and Exchange Commission

Epiq Class Action Secure Matrix (ECA System)
PRIVACY IMPACT ASSESSMENT (PIA)

December 10, 2015

Office of Information Technology

Publishing History

Document Publication Number	Revision	Date	Changes Made
Initial Document	Initiation	12/09/15	Document Creation
Document update	1		
Document update	2		
Document update	3		
Document update	4		
Document update	5		
Document update	6		

General Information

1. **Name of Project or System.**
   Epiq Class Action Secure Matrix (ECA System)

2. **Describe the project and its purpose or function in the SEC's IT environment.**
   The Securities and Exchange Commission (SEC) prosecutes violations of Federal securities laws and holds violators accountable through appropriate sanctions and remedies. Under the Sarbanes-Oxley Act of 2002, the SEC has the authority to seek disgorgement and penalties as a remedy in civil actions and administrative proceedings and to distribute the disgorged funds to harmed investors. When distributing monies, the SEC may appoint or recommend that a court appoint a fund administrator to develop, oversee, and/or implement a distribution plan related to an SEC enforcement action. The Division of Enforcement oversees the appointment of fund administrators and has established a pool of nine firms (including Epiq Class Action ("ECA") eligible for appointment as a fund administrator. These firms may be called upon to develop distribution plans; determine economic harm or loss; administer distribution funds; process claims; determine claimant eligibility; implement a distribution; perform periodic and final accountings; provide reporting and record-keeping services; and to work with independent distribution consultants or with SEC staff to provide economic analysis relating to loss calculation and allocation of a Distribution Fund.

   ECA has developed the following processes to administer distribution plans associated with SEC enforcement actions: (1) creation of a website and an electronic and paper Proof of Claim form to identify and notify potentially eligible claimants and allow them to submit their claims; (2) establishment of a toll-free number to respond to claimant inquiries via telephone; and (3) use of its proprietary database to maintain a repository of the information collected from the harmed investor/claimant regarding the claim status, contact information, payment amounts, awards, and financial information. These processes are incorporated into ECA System.

   The ECA System is the main database for housing and reconciling payments. Bank software and reports are used for check cashing reconciliation in comparison against ECA System. For reconciliation of payment calculation, we utilize standard scripted reconciliation, manual review, and the internal Quality Assurance Department to ensure all payments are correct.

   This Privacy Impact Assessment (PIA) explains what personally identifiable information (PII) the SEC and ECA may 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

3. **Requested Operational Date?**
   In 2010, ECA was selected as one of nine participants to implement SEC distributions. The appointment to the pool of administrators began October 1, 2013. ECA has utilized the ECA System since that time to carry out its activities as a fund administrator. This PIA assesses the

privacy risks and vulnerabilities of ECA's processes in administrating the funds to which it has been appointed.

4. **System of Records Notice (SORN) number?**
   SEC-36 Administrative Proceeding Files & SEC-42 Enforcement Files

5. **Is this an Exhibit 300 project or system?**
   ☒ **No**
   ☐ **Yes**

6. **What Specific legal authorities, arrangements, and/or agreements allow the collection of this information?**
   Section 308(a) of the Sarbanes-Oxley Act; the Commission's Rules of Practice, 17 CFR 201.100-900, the Commission's Rules of Fair Fund and Disgorgement Plans, 17 CFR 201.1100-1106, and the Commission's Delegation of Authority to Director of the Division of Enforcement, 17 CFR 200.30-4.

Specific Questions

SECTION I – Data in the System

1. **What data about individuals could be collected, generated, or retained?**
   The claimant information that is collected, used, disseminated, or maintained either within the SEC or within ECA proprietary database varies depending upon the disgorgement matter. In routine disgorgement matters, the following information may be collected: first and last name; business name (if needed); unique claimant ID; street address; city; state; postal code; country; home phone number; work phone number; email address; transaction data; transaction dates; and account number. Social Security numbers (SSNs) and Tax ID numbers may also be collected and used, to ensure valid identification of harmed investors. Bank account information may be collected to implement electronic distribution payments. IRS forms W-8 and W-9 may be collected to facilitate tax reporting.

2. **Does the project/system use or collect the social security number (SSN)? (This includes truncated SSN's)**
   ☐ **No**
   ☒ **Yes. If yes, provide the function of the SSN and the legal authority to collect:** The SSN is collected primarily to enable the Fund Administrator to ensure a potential claimant is not a prohibited participant according to the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals List. In addition, the SSN is used as a unique identifier to ensure the Fund Administrator is able to perform an accurate and comprehensive de-duplication analysis for each case to prevent dilution of the claimant pool due to the issuance of payments for duplicate claims. The authority for requesting the SSN is Executive Order 13478.

3. **What are the sources of the data?**

Data in ECA System is collected primarily from the following sources:

- Defendant/Respondent records, which may include information obtained during the course of the SEC's investigation or action and provided to ECA;
- Transfer agent or other third party source records;
- Proof of Claim forms or supporting documentation submitted directly by potentially eligible claimants during the notice and claim process; and
- Third-party data sources such as transfer agents of the relevant issuer, banks, and broker dealer firms who held the relevant securities for investors as nominees.

4. **Why is the data being collected?**

ECA collects the data to carry out an efficient and cost-effective distribution administration plan, which permits eligible harmed investors to receive monetary disbursement from Distribution Funds established by a court or administrative order, as expeditiously as possible. Claimant information is collected, used, disseminated, or maintained by ECA to notify and identify potential claimants, to validate claimants and their claims, to distribute disgorgement payments to appropriate claimants, and to respond to inquiries from the SEC or a U.S. District Court.

5. **What technologies will be used to collect the data?**

ECA's technologies for collecting data may include (1) the use of a website to collect data from harmed investors via an electronic Proof of Claim form; (2) An application to process address verification; and (3) a database repository to collect, store and disseminate information. The ECA database can provide a vast amount of data as it tracks all aspects of the administration process; including housing and reconciling payments. Bank software and reports are used for check cashing reconciliation in comparison against ECA System. For reconciliation of payment calculation, we utilize standard scripted reconciliation, manual review, and the internal Quality Assurance Department to ensure all payments are correct.

These technologies, along with manual processes, are utilized to administer ECA's disgorgement plans. Information collected from claims submitted in paper and information provided by the SEC in case files or other third parties are entered into the ECA System by ECA staff members.

SECTION II – Attributes of the Data (use and accuracy)

1. **Describe the uses of the data.**

ECA uses data to (1) develop a distribution plan that includes developing a methodology related to loss calculation and allocation of the Distribution Fund; (2) develop a notice and claims process to identify and notify potentially eligible claimants; (3) administer a distribution fund, to include when applicable, opening escrow accounts, FDIC-insured controlled distribution accounts, or managed distribution accounts; (4) maintain record keeping and accounting of all monies in the Distribution Fund and distribution payments made; and (5) provide additional support services to assist potentially eligible harmed claimants in obtaining information relating

to the Distribution Fund (investor eligibility and fund distribution); and requirements for participation in the distribution.

2. **Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? ☐ No ☒ Yes. If yes, please explain:** ECA System enables ECA to identify any patterns or trends in an administration, as well as across all of its SEC Fair Fund cases.

3. **How will the data collected from individuals or derived by the system be checked for accuracy?**
ECA will typically design the Claim Form (and the information needed to be collected) based upon review of the Distribution Plan. ECA will consult with the SEC on the information begin requested.

ECA 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. ECA drafts, and receives approval from the SEC for any outreach material. In the majority of Notices, the SEC's website and information are included, unless the SEC has directed and approved otherwise. For other outreach material, such as checks or status letters, the content will still be approved by the SEC before mailing and may or may not include direct contact information for the SEC, depending on the context and approval of the SEC. In many matters ECA is engaged by the Courts to be the main contact for questions or for claimants to update their information.

ECA takes certain steps to validate the accuracy of the information and data that is collected. For example, prior to commencing a mailing (notice, claim form, or check), address files are reviewed, 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. In most cases, individuals are contacted to provide their information. The information provided by claimants, including contact information and transaction data, is submitted under penalty of perjury.

Additionally, SEC staff receives and reviews payment file reports for accuracy and completeness. In some instances, files may also be subjected to an independent third party review by an outside party to review the data collected and the calculation of payment amounts for accuracy.

SECTION III – Sharing Practices

1. **Will the data be shared with any internal organizations?**
☐ **No** ☒ **Yes. If yes, please explain:** Before distributing money to harmed investors, ECA provides SEC staff a distribution list containing names of payees and amounts to be distributed to them for approval. Additionally, periodic reports regarding investor and financial transaction information, i.e. accounting reports are provided to the SEC staff. The SEC and ECA exchange information via encrypted email or a secure internet connection.

2. **Will the data be shared with any external organizations?**
   ☐ **No** ☒ **Yes. If yes, please list organization(s):** District courts receive information related to distribution plans in court cases. In addition, data is shared with vendors who perform NCOA and address trace services.

   How is the data transmitted or disclosed to external organization(s)?
   ECA provides the information to the SEC and its vendors in encrypted format. Sharing of information is via SSH File Transfer Protocol. Subsequently the SEC staff files documents related to distribution plans with the appropriate government entity.

3. **How is the shared data secured by external recipients?**
   The processes and procedures established by the Federal court system oversee the security of claimant information in case files provided to the courts. Third party vendors who perform NCOA and address trace services are provided only public information such as name and address.

4. **Does the project/system process or access PII in any other SEC system?**
   ☒ **No**
   ☐ **Yes. If yes, list system(s):** Click here to enter text.

SECTION IV – Notice to Individuals to Decline/Consent Use

1. **What privacy notice was provided to the different individuals prior to collection of data?**
   ☐ **Privacy Act Statement** ☒ **System of Records Notices** ☒ **Privacy Impact Assessment**
   ☒ **Web Privacy Policy** ☐ **Notice was not provided to individuals prior to collection**
   Please explain: ECA provides a link to its Web privacy policy on its electronic Proof of Claim forms. The text of ECA's "Privacy Policy: The Administrator is committed to maintaining the privacy of your personal information. With respect to the collection, use and disclosure of personal information, the Administrator makes every effort to ensure compliance with applicable law, including, but not limited to, the Data Protection Act, 1998, the U.S. Privacy Act of 1974, the U.S. Paperwork Reduction Act of 1995, the US-EU Safe Harbor Privacy Principles and internal information quality guidelines. In connection with the administration process, you may be asked to provide certain information, including, but not limited to, name, postal address, telephone number and transactional account data. The information collected will be used solely for the purposes of the Settlement and the administration process." Other similar privacy act information will be included in the text of the Notice or Claim Form where necessary and as approved by the SEC. SEC SORNs SEC-36 and SEC-42 and this PIA provide additional notice to individuals of uses of their PII.

2. **Do individuals have the opportunity and/or right to decline to provide data?**

☒ **Yes** ☐ **No** ☐ **N/A**

Please explain: Claimant may decline to provide information and data; however refusal to provide certain information and data has a direct effect on the validity and eligibility of their claim.

3. **Do individuals have the right to consent to particular uses of the data?**

☐ **Yes** ☒ **No** ☐ **N/A**

Please explain: Harmed investors who choose to submit a claim do not have the right to limit their consent to particular uses of their information. The Privacy Policy that is posted on each Fair Fund website directly addresses the use of any information that is collected.

SECTION V – Access to Data (administrative and technological controls)

1. **Has the retention schedule been established by the National Archives and Records Administration (NARA)?**

☒ **No. If no, please explain:** The retention schedule is under development by the NARA and SEC. These records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with instructions of the SEC consistent with and as approved by NARA.

☐ **Yes. If yes, list retention period:**

2. **What are the procedures for identification and disposition of the data at the end of the retention period?**

At the end of the required retention period, ECA shall upon request transfer a trustworthy electronic copy of the records and documentation to the SEC via a Secure File Transfer Protocol. In addition, ECA will delete or destroy all physical and electronic claimant data from the ECA System as directed by internal company policy and in accordance with the Federal Information Security Management Act and associated NIST guidelines pertaining to data retention.

3. **Describe the privacy training provided to users, either generally or specifically relevant to the program or system?**

Data privacy is included in Security & Technology training and the Code of Conduct & Business Ethics training which are required for all new hires and again annually for all associates. ECA also employs formal, documented procedures to facilitate appropriate handling of sensitive data.

4. **Has a system security plan been completed for the information system(s) supporting the project?**

☐ **Yes. If yes, please provide date Security Assessment and Authorization (SA&A) was completed:** Click here to enter text.

☒ **No. If the project does not trigger the SA&A requirement, state that along with an explanation:** A SA&A in accordance with the requirements of the Federal Information Security Act of 2002 (FISMA) is pending.

5. **Is the system exposed to the Internet without going through VPN?**

   ☐ **No**

   ☒ **Yes. If yes, is secure authentication required?** ☐ **No** ☒**Yes; and**

   Is the session encrypted? ☐ **No** ☒**Yes**

6. **Are there regular (i.e. Periodic, recurring, etc) PII data extractions from the system?**

   ☐ **No.**

   ☒ **Yes. If yes, please explain:** Periodic and recurring extracts are needed to create management, operational, and fund accounting reports for distribution plans; and to conduct address research, replacement check mailings, courtesy letter mailings, and preparation of tax administration documents.

7. **Which user group(s) will have access to the system?**

   (1) Information Technology and Data Analysis teams, for the purpose of importing, validating, updating, and storing claimant data; (2) Claims Analysts and Call Center Analysts, for the purpose of validating eligibility, communicating with claimants, and updating their contact information; and (3) Management, for the purpose of reporting, supervising technology and processor resources, and ensuring accuracy and adherence to data handling standards.

8. **How is access to the data by a user determined?**

   All access to ECA System data is role based according to specific job functions. ECA has account management policies and controls in place to manage system accounts, to include the establishment, activation, modification, and termination of system accounts. All access to ECA System data is role based according to specific job functions. ECA 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 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.

Are procedures documented? ☒ Yes ☐No

9. **How are the actual assignments of roles and rules verified?**
   User access requests follow established approval and review processes, which includes verifying the appropriateness of the access being requested prior to provisioning the access.

10. **What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?**
    ECA's audit trails maintain a record of events both by system and the ECA System and by user activity within systems and applications. Audit logging is continuous, and logs are archived to provide access for review. ECA adheres to role based access policies and controls that ensure user accounts are authorized access only to pre-determined assets based on job function and security group membership. The ECA Systems is periodically reviewed by authorized ECA staff and third-party auditors.

SECTION VI – Privacy Analysis

1. **Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.**
   In considering the ECA System, the following privacy risks were identified:
   - When submitting a claim form, a claimant might inadvertently provide PII, including sensitive PII that is not required or requested for claims processing or verification;
   - Data provided by individuals might not be accurate, complete, or timely; and
   - Data provided by claimants might be misused or improperly disclosed or accessed.

   When submitting a claim form, a claimant might inadvertently provide PII, including sensitive PII or health information, that is not required or requested for claims processing or verification; Data provided by individuals might not be accurate, complete, or timely; and Data provided by claimants might be misused or improperly disclosed or accessed.

   To mitigate the risk of unnecessary PII being provided by claimants, the claim forms do not include an open-text comments field. Furthermore, fields are limited to the minimum information necessary to process a claim to reduce the risks of a user accidentally providing unnecessary information. SSNs are not routinely collected on claim forms.

   As to the risk that the data provided might not be accurate, complete, or timely, it is important to note that individuals voluntarily provide claim information on the website, so that they may receive Fair Fund disgorgement. The process of filing claims is made as easy as possible for individuals. Claimants have the ability to validate and verify claimant information and to update any inaccurate information.

To mitigate the risk of improper use and disclosure of injured investor data, ECA employs a significant number of layered technical controls to help prevent the misuse or improper disclosure or access to injured investor data. These controls include, but are not limited to the following: Secure hosting of claim websites; Username and password authentication negotiated via application layer security; Claimants are provided a unique claim identifier and a system-generated password; Passwords are encrypted when transmitting between the web server and client based computing device; Administrative controls include a number of failed attempts and lockout, server event logging, and IP address tracking.

Data in the ECA system will be accessed only by authorized ECA staff to review and determine claimant eligibility for Fair Fund disgorgement. The data will be accessed via secure login, and access will only be made available to authorized staff on a need-to-know basis.

The ECA system uses a defense-in-depth strategy to protect system resources against attacks by utilizing security technologies and services that maintain the Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation requirements as mandated by the Federal Information Security Management Act and outlined in National Institute of Standards and Technology (NIST) Special Publication 800-53. The FIPS 199 security categorization of the ECA System is Moderate Impact.