U.S. Securities and Exchange Commission

A.B. Data, Ltd. - Class Action Administration Division (CAAD)
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.**
   A.B. Data, Ltd. - Class Action Administration Division (CAAD)

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 A.B. Data, Ltd (A.B. Data)) 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.

   A.B. Data 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 and call center to respond to claimant inquiries via telephone; and (3) creation of a 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 A.B. Data's Class Action Administration Division (CAAD).

   This Privacy Impact Assessment (PIA) explains what personally identifiable information (PII) the SEC and A.B. Data 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, A.B. Data was selected as one of nine participants to implement SEC distributions. A.B. Data currently utilizes CAAD to carry out its activities as a fund administrator. This PIA assesses the privacy risks and vulnerabilities of A.B. Data'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 CAAD proprietary databases 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; account number; and notes of claimant contact with A.B. Data, including any subsequent change requests, updates, or corrections. 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. A.B. Data reviews the Plan of Distribution and/or Plan of Allocation to ensure A.B. Data requests the proper information for input into the CAAD system to calculate eligibility and losses/award amounts.

   A.B. Data CAAD information system environment encompasses two physical facilities/Local Area Networks (LANs) connected together by a private dedicated Wide Area Network (metro-Ethernet) solution. Both A.B. Data CAAD facilities are physically located in Milwaukee, WI.

   A.B. Data Hopkins facility provides CAAD scanning, imaging, fulfillment and mail processing functions, while the A.B. Data Ironwood facility provides data center, administration, call center, claims processing, data processing and quality assurance/quality control functions.

   In instances where a claimant calls A.B. Data regarding an SEC disgorgement distribution matter, details of calls may be summarized in the CAAD by contact center staff located within A.B. Data's Ironwood Road, Milwaukee, Wisconsin campus.

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:** When applicable, SSNs are typically requested from harmed investors on the Proof of Claim Form. SSNs are collected and used to validate identities of harmed investors and to verify information on the Proof of Claim form. The authority for requesting the SSN is Executive Order 13478.

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

   Data in CAAD 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 A.B. Data;
   - 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 the United States Postal Service (USPS) and address-tracing companies providing mailing address updates and corrections.

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

   A.B. Data 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 A.B. Data to identify potential claimants, to validate claimants and their claims, and to distribute disgorgement payments to appropriate claimants.

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

   A.B. Data's technologies for collecting data include (1) the use of a website to collect data from harmed investors via an electronic Proof of Claim form; (2) a toll-free number call center, to field calls from potentially eligible claimants; and (3) a database repository, CAAD, to collect, store and disseminate information. The CAAD is comprised of seven applications/databases in order to provide services to the SEC. A brief description of each application/database is presented below.

   - Class Action Database (CADB): CADB is a custom database and application utilized by A.B. Data to track claimant qualification status.
   - CheckBook: A custom application closely tied to CADB to manage the layout, and printing of claimant disbursement checks.
   - BankRec: BankRec is a custom application used to reconcile all A.B. Data's Qualified Settlement Fund (QSF) bank accounts.
   - Fulfillment: An application closely tied to CADB to manage bulk names and addresses received from Banks, Brokers, and Nominees.

- OnBase: A purchased software and hardware solution that digitally images all paper claim forms and correspondence tied to a claim.
- New Technology File System (NTFS): A.B. Data Class Action utilizes NTFS as a central repository for case data. A new file share location is created for each SEC case for which all case specific documents (e.g., notice, claimant response forms, supporting documentation, etc.) are uploaded and archived. Staging SQL Database: The staging SQL database is utilized to upload large claimant data files onto the NTFS.
- Reporting Systems (SSRS): We use SQL Server Reporting Services (SSRS) to generate and view most database driven reports on claim data.
- A.B. Data Web Servers: Our web servers provide general information on cases that A.B. Data Administers.
- i3 CIC: The i3 (Interactive Intelligence Incorporated) CIC (Customer Interaction Center) is a system used to support telecommunications related to our claim support center.

The A.B. Data CAAD does not currently engage or permit external information systems access to A.B. Data information systems. These technologies, along with manual processes, are utilized to administer A.B. Data's disgorgement plans.

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

1. **Describe the uses of the data.**
   A.B. Data uses CAAD 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.

   Investor contact information is used to notify the investor of his, her, or its potential eligibility to receive a payment from the Fair Fund, to request any additional information or documentation needed to complete any claim, and/or to issue any payment (if eligible) or notice of final disposition of any claim.

   Investor transactional information is used to determine the investor's potential eligibility to receive proceeds of the Fair Fund, and the investor's allocation of the Fair Fund if applicable, pursuant to the requirements of the Plan of 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:**
   Click here to enter text.

3. **How will the data collected from individuals or derived by the system be checked for accuracy?**
   AB Data uses the United States Postal Service ("USPS") National Change of Address database to ensure that investor mailing addresses are accurate.

   AB Data also uses a third-party aggregator of information to ascertain updated mailing addresses for any mail sent to investors that is returned by USPS as undeliverable as addressed.

   AB Data currently uses a service offered by Lexis-Nexis that updates investor mailing addresses based on outdated addresses, names, contact information, etc. associated with the investor. Transactional information provided by investors is validated against supporting documentation, such as brokerage statements or confirmations, subject to the requirements of the relevant Plan of Distribution.

   AB Data has a devoted Quality Assurance Department that runs a standard set of audits and quality checks to ensure that all data entered into the system are accurately captured.

   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:** Authorized AB Data staff have access to the information within the following functions: Information Technology professionals, for the purpose of importing, validating, updating, and storing claimant data; Claims processors, for the purpose of validating eligibility, communicating with claimants, and updating their contact information; and Management, for the purpose of reporting, supervising technology and processor resources, and ensuring accuracy and adherence to data handling standards. Periodic reports regarding investor and financial transaction information, i.e. accounting reports are provided to the SEC staff. The SEC and A.B. Data 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, A.B. Data utilizes external vendors for printing and various class action administration functions. Outsourced IT vendors' employees must each sign information security policy agreement and network acceptable use policy. Any IT Outsourcing is addressed in compliance contracts with our clients/vendors prior to starting any work.

How is the data transmitted or disclosed to external organization(s)?
A.B. Data utilizes various methods for data transmission and employs security controls as needed. All A.B. Data traffic traveling over public networks, including VoIP, is fully encrypted. Any company, customer, client or vendor data traveling over public networks (Internet, email, etc.) and security networks is encrypted. A.B. Data cryptographic mechanisms recognize changes during data transmission as part of encryption protocol (i.e., verification). A.B. Data cryptographic mechanisms include network session timeout values or inactivity timeouts as part of encryption protocol. A.B. Data 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?**
A.B. Data requires all external vendors to sign a mutual confidentiality agreement, connection agreement, and other applicable terms and conditions prior to allowing individuals to process, store, and/or transmit A.B. Data information. All vendors who perform maintenance services on behalf of A.B. Data are subject to the same security policies as A.B. Data Employees. Outsourced IT vendors must sign non-disclosure agreements. In addition, the processes and procedures established by the vendors and the Federal court system oversee the security of information in case files.

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: A.B. Data provides a link to its Web privacy policy on its electronic Proof of Claim forms. The Web policy describes the PII collected, its use, and how it is shared by A.B. Data. In addition, SEC system of records notices, SEC-36 and SEC-42, and this PIA provide additional notice to individuals of uses by the SEC of their PII.

2. **Do individuals have the opportunity and/or right to decline to provide data?**
☒ **Yes** ☐ **No** ☐ **N/A**
Please explain: Yes. The Proof of Claim form provides instructions to the claimants on completing the form. The instructions include a clause advising the claimants they have a right to decline providing their data but they may be precluded from any recovery.

3. **Do individuals have the right to consent to particular uses of the data?**
☐ **Yes** ☒ **No** ☐ **N/A**

Please explain: No. Harmed investors who choose to submit a claim do not have the right to limit their consent to particular uses of their information.

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:** Click here to enter text.

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, A.B. Data shall transfer an electronic copy of the records and documentation to the SEC via the Secure File Transfer Protocol. After review and approval of the SEC, A.B. Data shall then destroy all records and documentation in its possession associated with the matter, in accordance with instructions of the SEC consistent with and as approved by NARA.

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

   A.B. Data requires certain (high risk or elevated security) divisions undergo annual security and awareness training. These annual training sessions address the purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities and compliance.

   Annual training sessions are reviewed annually by the security team of every year to review and update the material and make relative changes and recommendations to content.
   All A.B. Data employees, including CAAD, undergo basic security awareness training as part of the new hire employee training. All A.B. Data employees, including CAAD, have access to security policies posted on the A.B. Data intranet.

   All employee training attendance records are maintained in a central database for the duration of an individual's employment with A.B. 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, preparation of tax administration documents.

7. **Which user group(s) will have access to the system?**
   - Customer service representatives for responding to inquiries from potential claimants;
   - Information Technology professionals, for the purpose of importing, validating, updating, and storing claimant data;
   - Claims processors, for the purpose of validating eligibility, communicating with claimants, and updating their contact information; and
   - 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?**

   Data in the system will be accessed only by authorized A.B. Data staff to carry out the functions listed above in question 7. Account access modifications are requested by account managers and require approval from the appropriate management personnel prior to being granted. Access to the network, systems, and applications is disabled/removed for terminated employees upon notification. Access to A.B. Data security functions must be approved by the IT Manager. A.B. Data has established a formal Remote Access Acceptable Use Policy which defines policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of A.B. Data Group's network. The data will be accessed via secure login, and access will only be made available to authorized staff on a need-to-know basis. Data usage is in accordance with the uses described in the Letter of Engagement A.B. Data has with the SEC.

   Are procedures documented? ☒ **Yes** ☐**No**

9. **How are the actual assignments of roles and rules verified?**

A.B. Data has account management policies and controls in place to manage CAAD to include the establishment, activation, modification, and termination of system accounts. A.B. Data's account management activities include:

- A.B. Data performs a review of inactive accounts on a monthly basis; accounts that have been inactive for more than 60 days are manually deactivated.
- A.B. Data employs the concept of least privilege. The organization has pre-defined department roles for users in each department to help facilitate restricting user access to only those business functions that are necessary. The A.B. Data CAAD has implemented predefined roles within the system to prevent unauthorized changes to claimant information, unauthorized changes to the case database, and unauthorized changes to case status requiring supervisor approval.
- The A.B. Data CAAD has implemented separation of duties to prevent unauthorized changes to claimant information, changes to the case database, and changes to case status requiring supervisor approval.

10. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?

User access controls are in place within the CAAD application, so that only users authorized to access specific distribution projects have access. A.B. Data has defined pre-populated user profile templates (including the Class Action Administration Division, CAAD) which reflect the software and security settings provided by each A.B. Data department to the IT Department for corresponding employee positions/work roles.

Audits of user access controls (physical and logical) are conducted biannually in the event of an incident or user position changes. Audit event logging is maintained on the domain controller and includes network account authentication attempts, access changes, physical security access control doors, and information systems where possible.

All network accounts are authenticated against a central database of accounts using the Microsoft Active Directory model against Active Directory Servers. Vendor accounts are set up in Active Directory with automatic expiration dates for consultants that reflect the term of the engagement as defined by the vendor point of contact at A.B. Data.

A.B. Data performs a review of inactive accounts on a monthly basis; accounts that have been inactive for more than 60 days are manually deactivated.

A.B. Data employees are assigned a unique information system account regardless of security functions. Audit event logging is maintained on the domain controller and includes network

account authentication attempts, access changes, physical security access control doors, and information systems, where possible.

Network Accounts will lockout after three consecutive failed authentication attempts within 5 minutes. Alarm messages will be sent to the IT Department for all locked out accounts. Locked out Network Accounts will require IT Department unlock.

Network Account re-authentication is required for systems that have been inactive for 10 minutes or longer. No user actions can be taken without identification or authentication on the information system.

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 CAAD, 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;
- Data provided by claimants might be misused or improperly disclosed or accessed.

The FIPS 199 security categorization of the CAAD System is "Moderate Impact". The privacy risks identified are mitigated by administrative, technical, and physical controls implemented by A.B. Data. A.B. Data has limited information collection to the minimum necessary to carry out its activities related to distribution plans that it administers. Specifically, the information collected from claimants is limited to information used to notify and identify them, allocate a distribution, and disburse the funds in accordance with the distribution plan. A.B. Data has developed a secure web-based claim form that will enable the claimant to submit claim information.

Because A.B. Data collects as much information as is practical directly from the claimant the likelihood of erroneous PII is limited. In addition claimants may be required to provide supplemental documentation as proof of identity. A.B. Data personnel receive privacy training for handling the PII collected. Personnel only have access to information needed in the performance of their duties.

The periodic monitoring, of logs and accounts, helps to prevent and/or discover unauthorized access attempts. Audit trails are maintained and monitored to track user access and unauthorized access attempts. Additionally, by default, all remote access is denied, requests for remote access must be submitted by an employee's manager. Use of Remote Access technologies (VPN, Remote Desktop, etc.) is only allowed under written authorization under A.B. Data remote access policy requirements. Remote Access VPN users are required to use data encryption when VPN-connecting to A.B Data Group networks. A.B. Data limits remote access

(e.g., VPN) through two managed access points. A.B. Data actively monitors unauthorized access attempts. The enterprise firewall is configured to alert IT (via email and log) of any failed login attempts, including unauthorized remote connections.

Physical security boundaries are defined, created and enforced with fully audited and logged electronic key card ACS (Access Control Systems) and video surveillance systems within A.B. Data. Security zones are established based on security risk. Physical access to key CAAD information systems, servers and infrastructure are limited to approved IT staff after completing back ground checks and appropriate internal IT training. Additionally CAAD employees receive full back ground checks, training and clearance prior to gaining access to CAAD Information Systems for production purposes.