U.S. Securities and Exchange Commission

Boston Financial Data Services' Settlement Administration Services Event Center (SASEC)
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.**
   Boston Financial Data Services' Settlement Administration Services Event Center (SASEC)

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 fund administrators to develop, oversee, and/or implement distribution plans. The Division of Enforcement oversees the appointment of fund administrators and has established a pool of nine firms (including Boston Financial Data Services (Boston Financial)) eligible for appointment as a fund administrator. These firms may be called upon to identify injured investors, provide notification and claim forms, process claim forms, and disburse funds to injured investors.

   Boston Financial 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) 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.

   SASEC is maintained in Boston Financial's secure data center in Quincy, Massachusetts and in their secondary data center in Canton, Massachusetts. Access to Boston Financial facilities, including data centers, is monitored 24X7 and is controlled by mantraps and secure card access. On-site security guards and closed circuit architecture television (CCATV) monitors all egress points. Only authorized personnel have access to the Data Centers.

   This Privacy Impact Assessment (PIA) explains what personally identifiable information (PII) the SEC and Boston Financial may collect throughout the claims administration process, who is allowed to use the information and for what purposes, and what steps are taken to identify, secure, and reduce any privacy risks to the information.

3. **Requested Operational Date?**
   In 2010, Boston Financial was selected as one of nine participants to implement SEC distributions. Boston Financial has utilized SASEC since that time to carry out its activities as a fund administrator. This PIA assesses the privacy risks and vulnerabilities of Boston Financial'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 information collected, disseminated and/or maintained on individuals will vary depending on 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 Boston Financial, 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 also 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:** When applicable, SSNs are typically requested from harmed investors on the Proof of Claim Form. Boston Financial may also request a SSN as part of the claim form process when it is required for review by the SEC appointed Tax Administrator. 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 SASEC 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 SASEC;
- 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?**
Boston Financial 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 Boston Financial to identify potential claimants, to validate claimants and their claims, and to distribute disgorgement payments to appropriate claimants. Additionally, data may be used to determine tax withholding and reporting requirements as well as respond to investor inquiries.

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

These technologies, along with manual processes, are utilized to administer Boston Financial'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 SASEC System by Boston Financial staff members.

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

1. **Describe the uses of the data.**
Boston Financial uses SASEC 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:**
   Not applicable

3. **How will the data collected from individuals or derived by the system be checked for accuracy?**
   Various steps are taken to validate the accuracy and timeliness of collected data based on its original source. For example, prior to Boston Financial mailing a claim form or distribution check claimant addresses are standardized and cross-checked against known data sources, such as the U.S. Postal Service (USPS) National Change of Address Database and U.S. Postal Service records regarding street names and address ranges.

   Individuals are contacted to provide or verify information from their file. For example, claim forms may be mailed to a known set of claimants requesting that they validate, under penalty of perjury, their address, loss amount, and entitlement to distribution. In other cases, claim forms will be made available to previously unknown claimants via case-specific distribution notification and outreach such as via an established website for potential claimants to file claims. These claimants provide claim information, including their address, injury amount, and entitlement to distribution, under penalty of perjury.

   Boston Financial 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. Outreach material, distribution checks, and claim forms include a means for additional information such as a Boston Financial hosted website, toll-free telephone number, and mailing address for harmed investors to contact Boston Financial to have their questions answered and/or to update their information.

   Additionally, SEC staff receive and review 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, Boston Financial 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 Boston Financial 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):** Boston Financial may share information with U.S. District Courts upon request. In addition, data is shared with vendors who perform NCOA and address trace services. Boston Financial will securely download and transmit required data in response to authorized requests.

   How is the data transmitted or disclosed to external organization(s)?
   Boston Financial 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):** not applicable

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: SORN SEC-36 and SEC-42 and this PIA provide 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: 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:** N/A

   ☒ **Yes. If yes, list retention period:** 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 records schedules of the United States Securities and Exchange Commission and as approved by the National Archives and Records Administration.

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, Boston Financial shall upon request transfer a trustworthy electronic copy of the records and documentation to the SEC via a Secure File Transfer Protocol. In addition, Boston Financial will delete or destroy all physical and electronic claimant data from the SASEC 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?**

   All Boston Financial associates are required to take six online annual training programs where attendance is tracked and maintained indefinitely. Security training is provided to all new employees as part of new-hire onboarding and prior to the distribution of any credentials that may grant access to network systems or sensitive data. Additionally, all users involved with this and other FISMA-moderate client data are required to read and acknowledge all relevant policies and control standards.

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 conduct address research, replacement check mailings, courtesy letter mailings, tax administration and reporting.

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 Boston Financial staff to carry out the functions listed above in question 7. 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 Boston Financial has with the SEC.
   User roles are assigned when a new associate is on boarded or a job role/change has occurred for an existing user. Appropriate access levels are determined by the job role and functions the user will be performing.

   Are procedures documented? ☒ Yes ☐No

9. **How are the actual assignments of roles and rules verified?**
   All access to the SASEC system are role-based and facilitated using departmental security groups that authorize access to the pre-determined network resources necessary to fulfill a given job function. Quality Control is conducted by the development and business teams for all new user levels that are created. Once ID levels are in production and assigned to specific users, a weekly report is generated and monitored by a data security liaison to ensure users are mapped to the correct ID based on their job function. Additionally, the Human Resources department notifies the Service Center of terminated users and transfers, on a daily basis. Upon notification of termination, the Service Center team disables the terminated user's network access.

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 SASEC application so that only users authorized to access specific projects have access. All users can only gain access to the system via a user ID and a unique password. Network passwords must conform to established security requirements and expire after a period of inactivity. Functions relating to modifying data or adding information to any settlement database are tracked by the user ID along with a timestamp. Master files in the database are tracked for additions, changes, and/or deletions. Users are not

able to extract data off a desktop system via a usb or another attachment to a system. Additionally, all traffic to the environment is Secure Socket Layer (SSL) encrypted with 128 bit encryption. An Intrusion Protection System/Intrusion Detection System (IPS/IDS) appliance is installed at the core of the network to facilitate alerting and logging. Boston Financial performs weekly vulnerability scans on workstations and daily scans on internet facing websites. An independent third party network penetration test is performed annually on both internal and external networks and all web applications.

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.**

Boston Financial recognizes the inherent risk to claimants posed by the unauthorized dissemination of personal identifiable information. Given the nature of the information collected by Boston Financial ensuring the confidentiality of the data is an utmost priority. Boston Financial identified the following risks:

- collecting the user's SSN PII is a potential privacy risk;
- when submitting a claim form, a claimant might inadvertently provide 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.

Boston Financial employs a comprehensive Information Security Program that works to ensure the confidentiality, integrity, and availability of all organizational data in accordance with both Federal Information Processing Standards and the Federal Information Security Management Act through the implementation of controls and countermeasures as outlined in NIST Special Publication 800-53 based on our security categorization as determined by FIPS 199. The FIPS 199 security categorization of the Boston Financial SASEC system is Moderate Impact.

The privacy risks identified are mitigated by administrative, technical, and physical controls implemented by Boston Financial. Boston Financial 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. Boston Financial has developed a secure web-based claim form that will enable the claimant to submit claim information. Email and DLP encryption controls are established to identify any out-of-band transactions. Because Boston Financial 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. Boston Financial personnel receive 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, Boston Financial carries out its business activity in a location protected by 24/7/365 on-site security guards, badge/picture ID access screening and escort requirements for access to the location. SSNs are also masked in the system and only the last 4 digits are displayed. Users must be authenticated by LDAP or an equivalent process.