U.S. Securities and Exchange Commission

RCB Fund Services LLC (RFS) SmartClaim System - Proprietary Claims Administration Platform (SmartClaim System) PRIVACY IMPACT ASSESSMENT (PIA)

December 1, 2015

Office of Information Technology

Publishing History

Document Publication Number	Revision	Date	Changes Made
Initial Document	Initiation	11/30/15	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.**
   RCB Fund Services LLC (RFS) SmartClaim System™ – Proprietary Claims Administration Platform (SmartClaim 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 RCB Fund Services LLC ("RFS, LLC") 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.

   RFS, LLC has developed FAQs for its current fund located at http://jpmsecfund.com/frequently-asked-questions to assist claimants with the most commonly asked questions. RFS, LLC 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. These processes are incorporated into SmartClaim System.

   This Privacy Impact Assessment (PIA) explains what personally identifiable information (PII) the SEC and RFS, LLC 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, RFS, LLC was selected as one of nine participants to implement SEC distributions. RFS, LLC has utilized the SmartClaim System since that time to carry out its activities as a fund administrator. This PIA assesses the privacy risks and vulnerabilities of RFS LLC'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 RFS,LLC 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 SmartClaim 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 RFS, LLC;
- 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?**
   RFS, LLC 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 RFS 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?**
   RFS'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) Pitney Bowes application to process address verification (CASS and NCOA), pre-sort the addresses and create the "proof" image of the notice; and (3) Emdeon application for printing and mailing notices and proof of claim forms; (4) a database repository to collect, store and disseminate information. The database can provide a vast amount of data as it tracks all aspects of the administration process; including all potential claimant contact information, claim status, total claimed and eligible loss amounts, total claimed transactions, distributions and their amounts, all correspondence with potential claimants, number of telephone calls and email inquiries, etc.

   These technologies, along with manual processes, are utilized to administer RFS'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 SmartClaim System by RFS staff members.

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

1. **Describe the uses of the data.**
   RFS, LLC 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:** SmartClaim System enables RFS, LLC 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?**
RFS, LLC 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, RFS, LLC 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 RFS, LLC 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):** SmartClaim System may share information with a U.S. District Court upon request. SmartClaim System may also share name and address information with a third-party service provider, Pitney Bowes ("PB"). SmartClaim System uploads a text file containing the potential claimants' names & addresses via secure SSH to PB. PB completes their address verification processes (CASS and NCOA), pre-sort the addresses and create the "proof" image of the notice to be uploaded to Emdeon for printing/mailing. Emdeon then commences the initial mailing in a Fair Fund administration to notify investors of the Fair Fund.

How is the data transmitted or disclosed to external organization(s)?
Information shared with the U.S. District Court is submitted to the SEC. Subsequently the SEC staff files documents related to distribution plans with the appropriate court. Sharing of information with Pitney Bowes and Emdeon is via SSH File Transfer Protocol.

3. **How is the shared data secured by external recipients?**
The processes and procedures established by the Federal court system oversee the security of information in case files. Data is encrypted during transit via SSL technology. Pitney Bowes and Emdeon data centers are physically secured with biometric and badge-reader access. The controls and procedures for the Emdeon's Patient Billing & Payment Services (PBPS) platform were reviewed by an external auditor from Ernst & Young LLP in 2013. SmartClaim System data is not shared outside of Pitney Bowes/Emdeon.

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: RFS, LLC 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. It also describes what rights users have to request removal of their PII. SORN 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: Claimants are notified that the information and data they provide will be used by SmartClaim System only as necessary to administer their claim during the claims administration process. Claimants are notified of how the information being collected will be used on the claim form, as well as on the relevant Fair Fund website. 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, RFS, LLC shall upon request transfer a trustworthy electronic copy of the records and documentation to the SEC via a Secure File Transfer Protocol. In addition, RFS, LLC will delete or destroy all physical and electronic claimant data from the SmartClaim 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?**

   RFS, LLC has designed and implemented a multi-faceted Information Technology Security Awareness and Training Program based on FISMA regulatory guidelines and the associated NIST framework as outlined in NIST Special Publication 800-50. The objective of the RFS, LLC security awareness and training program is to:

   a. ensure employees understand their roles and responsibilities as it pertains to ensuring the confidentiality of claimant information;
   b. to reinforce an understanding of information security policies and procedures amongst the RFS, LLC workforce; and
   c. to provide staff education regarding common controls for which they are responsible and which work to mitigate risk to the organization and ensure the integrity of confidential data.

   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. During onboarding company policies pertaining to acceptable use of voice and data systems, in addition to the RFS, LLC employee handbook, are reviewed and acknowledged. This ensures all new members of the RFS, LLC team are aware of their responsibility in protecting sensitive data, and equipped with the tools and knowledge to achieve that mission. All RFS, LLC employees undertake annual security awareness training and re-acknowledge their receipt and understanding of updated internal policies and security controls. This training is used as an

opportunity to further educate the RFS, LLC workforce regarding an ever evolving threat landscape, while reinforcing the importance of diligence in executing our responsibility to the confidentiality of sensitive claimant 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 (ie. 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?**

   Access to the system is restricted to users whose job function specifically necessitates such access. This includes Data Entry and Document Review staff who require access for the purposes of entering and validating the claimant's loss; Project Management staff for the purposes of auditing, data analysis, and reporting; and select Information Technology staff for the purpose of administration/management of the SmartClaim System and associated data, in addition to notice generation and reporting.

   Application developers leverage two separate environments for development and staging that utilize non-production data. Administrative access to the production SmartClaim System is provided for the purposes of debugging and troubleshooting. Contractors, such as those that may participate in the review and auditing of claims, utilize a separate claim viewer that exclusively provides read-only access to claim information.

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

   All access to SmartClaim System data is role based according to specific job functions (e.g. Data Entry, Document Review, and Audit). Access to claim data via SmartClaim System is further segmented by an active claim program. SmartClaim System offers various tiers of authorization

based on access requirements, from read-only/review access to broader access rights necessary for both data entry and the review of supporting documents and claim completeness. RFS, LLC also employs a view-only claim viewer separate from the SmartClaim System that facilities read-only access exclusively. Claim programs are processed on individualized databases and instances of SmartClaim System, meaning access to claim data and the associated permissions are reviewed and authorized for every account for each claim program. This ensures access to claim data is restricted to only that which is necessary for each individual claim program.

Are procedures documented? ☒ Yes ☐No

9. **How are the actual assignments of roles and rules verified?**
   All access to SmartClaim Systems 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. Alterations to a given permission set may be necessary due to special projects which require non-standard permissions, association with an alternate security group due to a shift in one's organizational role, or termination or temporary leave (e.g., FMLA) of employment.

   All instances of change to permissions are forwarded through the RFS, LLC ticketing system for purposes of both management and auditing. Requests are submitted by department supervisors indicating both the nature of the change and the underlying organizational driver. Once submitted, all change requests are reviewed by the Operations Manager to ensure they adhere to organizational policy. When approved the change is implemented by a system administrator, and recorded in our centralized event and log management platform for purposes of both auditing and incident response.

10. **What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?**
    RFS, LLC 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. Access to resources outside prescribed roles, or escalation of privilege due to role change, requires the submittal of a change request from a department supervisor though the RFS, LLC service desk. Any service request related to permissions and system access are reviewed and approved by the Operations Manager prior to implementation by a system administrator. All change requests are recorded and archived in the RFS, LLC ticketing system for audit purposes. Security group membership and subsequently access to system resources are reviewed weekly to ensure no unauthorized changes.

    RFS, LLC employs a centralized security information and event management platform that facilitates the aggregation of access logs and events across all SmartClaim Systems. The SIEM generates periodic reports of all changes to both system accounts and associated security groups across the entire RFS, LLC operating environment. These event reports are audited on a

daily basis and alterations to permissions, groups, or accounts correlated with approved change requests. RFS, LLC correlates all log files with a selection of security directives that scan event logs for anomalies, including denied file access and brute force attempts, and alerts administrators to occurrences of such anomalies both in real-time and as an aspect of a daily audited security operations report.

Further RFS, LLC has implemented all appropriate controls related to identification and authorization as mandated by the Federal Information Security Management Act and outlined in NIST Special Publication 800-53.

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.**

RFS, LLC recognizes the inherent risk to claimants posed by the unauthorized dissemination of personal identifiable information. Given the nature of the information collected by RFS, LLC ensuring the confidentiality of our data is an utmost priority. RFS, LLC 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.

RFS, LLC 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 RFS SmartClaim System is "Moderate Impact" with the underlying data categorization for "claimant data" = {(confidentiality, moderate), (integrity, moderate), (availability, moderate)}.

RFS, LLC has deployed a tiered security architecture that facilitates the identification and management of traffic across our network infrastructure, real-time threat assessment, intrusion and extrusion detection, and additional countermeasures and protections aimed at maximizing information system security. RFS, LLC maintains a centralized security information and event management platform that facilitates the collection and analysis of millions of system events across the entirety of the RFS, LLC network infrastructure. This system provides event correlation against thousands of security directives enabling the real-time detection of network anomalies, while bolstering incident response through log aggregation, archiving, and forensic review.

Further, RFS, LLC employs strong Information Security policies and procedures that ensure all aspects of network operations are periodically audited, assessed, and fortified.