U.S. Securities and Exchange Commission

Rust Consulting, Inc. Claims Management Database System (CMD)
PRIVACY IMPACT ASSESSMENT (PIA)

December 1, 2015

Office of Information Technology

Publishing History

Document Publication Number	Revision	Date	Changes Made
Initial Document	Initiation	11/27/15	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.**
   Rust Consulting, Inc. Claims Management Database System (CMD)

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 Rust Consulting, Inc. (Rust)) 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.

   Rust 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, Interaction Client, 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 Rust's Claims Management Database System (CMD).

   CMD is maintained in Rust's secure on-site location in Minneapolis, MN, and their secure off-site location in Troy, MI. This site is protected by 24/7/365 on-site security guards, indoor and outdoor security monitoring, badge/picture ID access screening and escort requirements for access to the location.

   This Privacy Impact Assessment (PIA) explains what personally identifiable information (PII) the SEC and Rust 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, Rust was selected as one of nine participants to implement SEC distributions. Rust has utilized CMD since that time to carry out its activities as a fund administrator. This PIA assesses the privacy risks and vulnerabilities of Rust'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 CMD 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 Rust, 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. Rust reviews the Plan of Distribution and/or Plan of Allocation to ensure Rust requests the proper information for input into the CMD system to calculate eligibility and losses/award amounts.

   In instances where a claimant calls Rust regarding an SEC disgorgement distribution matter, the Rust Interactive Voice Response and Contact Center system records the number that the individual calls from, the date/time/length of call, and the contact center script and if necessary, escalation used to route the call. Details of calls may be summarized in the CMD by contact center staff.

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 CMD 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 Rust;
   - 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?**

   Rust 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 Rust 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?**

   Rust'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 VoIP (Voice over Internet Protocol) communication solution, Interaction Client, to field calls from potentially eligible claimants; and (3) a database repository, CMD, to collect, store and disseminate information. These technologies, along with manual processes, are utilized to administer Rust'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 Rust's CMD system by Rust staff members. Records of telephone calls between Rust and other callers are stored in Interaction Client and summaries of calls may be entered into the CMD database.

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

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

   Rust uses CMD 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:**
   Click here to enter text.

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 Rust 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.

   Rust 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 Rust hosted website, toll-free telephone number, and mailing address for harmed investors to contact Rust to have their questions answered and/or to update their information.

   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, Rust 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 Rust 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)?
   Rust provides the information to the SEC and its vendors in encrypted format. 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 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: Rust 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: 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, Rust shall transfer a trustworthy electronic copy of the records and documentation to the SEC using Rust's Managed File Transfer secure data transfer site via the Secure File Transfer Protocol. After review and approval of the SEC, Rust shall then destroy all records and documentation in its possession associated with the matter, in accordance with NARA, OMB, and NIST regulations and guidelines.

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

   Rust employs formal, documented procedures to facilitate security awareness training, including a specific course related to PII, which is managed and implemented by Rust's Security and Compliance Team and Human Resources. 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:** Authorization to operate issued October 7, 2015.

   ☐ **No. If the project does not trigger the SA&A requirement, state that along with an explanation:**

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 Rust 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 Rust has with the SEC.

   Are procedures documented? ☒ Yes ☐No

9. **How are the actual assignments of roles and rules verified?**
   Rust has account management policies and controls in place to manage CMD to include the establishment, activation, modification, and termination of system accounts. Rust's 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 the guest/anonymous and 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; and
   - Reviewing accounts quarterly, at a minimum.

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 CMD application, so that only users authorized to access specific projects have access. Projects are logically separated in CMD and have individual approved user lists, including username and role. Users must be assigned to a role within each project by the Project Manager, based on their need to know. Users who are inactive for 30 days are automatically disabled.

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 CMD, 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.

    The privacy risks identified are mitigated by administrative, technical, and physical controls implemented by Rust. Rust 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. Rust has developed a secure web-based claim form that will enable the claimant to submit claim information. Because Rust 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. Rust 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, Rust carries out its business activity in a location protected by 24/7/365 on-site security guards, indoor and outdoor security monitoring, badge/picture ID access screening and escort requirements for access to the location.