U.S. Securities and Exchange Commission

Case Litigation Administration Support System (CLASS) and Claim Filing Portal
PRIVACY IMPACT ASSESSMENT (PIA)

December 10, 2015

Office of Information Technology

Publishing History

Document Publication Number	Revision	Date	Changes Made
Initial Document	Initiation	12/9/15	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.**
   Case Litigation Administration Support System (CLASS) and claim filing portal.

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 Garden City Group, LLC (GCG)) 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.

   To administer distribution plans associated with SEC enforcement actions GCG utilizes its proprietary CLASS legal administration and claims processing system for data intake, processing, distribution and record keeping. The Information System has various functional components that handle all aspects of legal administration including validation of information, document and case management, call center support (if desired), and web support (if desired), and fund distribution and tracking. Each of those functions provides comprehensive capabilities, including extensive audit and reporting capabilities. All functional components are completely integrated, and use a common database.

   GCG distribution programs may also include a website to provide information about the Fair Fund distribution program and include the ability to electronically submit claim forms. The courts or the SEC may provide investor mailing information to GCG by hard copy or electronically. GCG uses this data to mail and/or e-mail notices and claim forms to investors that are potential claimants. Additionally, GCG may conduct research to obtain updates to investor addresses to send notices and information about the plan. GCG maintains a database of investors notified and the status of the claims in its CLASS system.

   This Privacy Impact Assessment (PIA) explains what personally identifiable information (PII) the SEC and GCG 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, GCG was selected as one of nine participants to implement SEC distributions. GCG has utilized CLASS since that time to carry out its activities as a fund administrator. This PIA assesses the privacy risks and vulnerabilities of GCG'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 GCG 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 GCG, 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.

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:** GCG only collects the last 4 digits of a SSN for the majority of its projects, however a full SSN may be requested if deemed necessary for a specific project. SSN is used to ensure a potential claimant

is not a prohibited participant according to the OFAC's Specially Designated Nationals List. In addition, the SSN is used as a unique identifier to ensure GCG is able to perform an accurate and comprehensive de-duplication analysis for each case to prevent dilution of the claimant pool and issuance of payments for duplicate claims. On occasion the SSN is used for tax reporting purposes. The authority for requesting the SSN is Executive Order 13478.

3. **What are the sources of the data?**
   Data in CLASS 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 GCG;
   - 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), NCOA, Lexis/Nexis and address-tracing companies providing mailing address updates and correction.

4. **Why is the data being collected?**
   GCG 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 GCG 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?**
   GCG's technologies for collecting data may include (1) secure FTP sites or web portals to collect data from harmed investors via an electronic Proof of Claim form; (2) toll free numbers or phone centers to field calls from potentially eligible claimants; and (3) a database repository to collect, store and disseminate information. These technologies, along with manual processes, are utilized to administer GCG'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 GCG's CLASS system by GCG staff members.

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

1. **Describe the uses of the data.**
   GCG uses CLASS 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:**
   Data collected by GCG in a specific SEC Fair Fund matter may also be used by the SEC and GCG to identify potentially fraudulent claims submitted in other SEC Fair Fund matters. For each Fair Fund matter managed by GCG as engaged by SEC, GCG sends a complete list of claims filed to the SEC. In an effort to identify potentially fraudulent claims, the SEC may analyze that information, refer back to data received in all Fund Administrations matters past and present, and provide information regarding potentially fraudulent claims back to GCG.

3. **How will the data collected from individuals or derived by the system be checked for accuracy?**
   Data from the various sources (e.g. brokers, claimants) is entered into the system and is subject to quality assurance reviews to ensure data has been captured as instructed, and data is checked against other information when available (e.g. compare transactions against broker statements). Claimants are required to sign under penalty of perjury that the information submitted is accurate and complete.

   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, GCG 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 GCG 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 received 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)?
GCG 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 court.

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

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

SECTION IV – Notice to Individuals to Decline/Consent Use

1. **What privacy notice was provided to the different individuals prior to collection of data?**
   ☐ **Privacy Act Statement** ☐ **System of Records Notices** ☐ **Privacy Impact Assessment**
   ☒ **Web Privacy Policy** ☐ **Notice was not provided to individuals prior to collection**
   GCG provides a link to its Web privacy policy on all of its websites created for specific Funds. The Web policy describes the PII collected, its use, and how it is shared. 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: Individuals are not compelled to provide data, but they may not be eligible to receive any distribution from the fund if they do not provide the required information.

3. **Do individuals have the right to consent to particular uses of the data?**
   ☐ **Yes** ☒ **No** ☐ **N/A**
   Please explain: Injured investors who choose to submit a claim do not have the right to limit their consent to particular uses of their information. The investor exercises their consent by choosing to complete, sign, and submit a claim form. Data is only used in the administration of the fund.

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:** Click here to enter text.

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

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, GCG will delete or destroy all physical and electronic claimant data 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?**

   During onboarding, and annually thereafter, all employees are required to review and certify their receipt and understanding of applicable GCG policies. In addition, GCG employees are required to take annual training relating to privacy, security, and confidentiality.

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

   ☐ **Yes. If yes, please provide date 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?**

- 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?**
Access to GCG's network is governed by GCG account management policies. All access to CLASS data is role based according to specific job functions. The principal of least privilege is employed when providing access. Access to project data, as well as the level of access, is provisioned to specific users only upon approval. Access, both logical and physical, is regularly reviewed. Public facing websites are hosted in a DMZ providing no direct access to internal GCG systems from the internet. The DMZ utilizes Internet protocol security and can only transmit data in an encrypted format. Claimants are given system generated passwords that are needed in combination with a unique ID to access their claim.

Are procedures documented? ☒ Yes ☐No

9. **How are the actual assignments of roles and rules verified?**
Data in the system will be accessed only by authorized GCG 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 GCG has with the SEC. All requests for provisioning and de-provisioning of access, and the fulfillments thereof, are logged. There is a regular review of users and their access levels to verify the access granted is appropriate.

What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?
There are many layers of controls to protect data, both physical and logical. Password management policies address complexity, password history, limited retry attempts, inactivity logouts, and account disabling after a period of not logging in. Data Loss Prevention (DLP) systems are in place that prevent the sending of PII unless authorized and sufficiently protected. Physical access to and within each GCG facility is controlled by means of a card-key security system. Security controls are reviewed both internally and by external parties. In addition, access to data is governed by the principle of least privilege and all login attempts are maintained in a log. All systems are required to log security events and forward to a centralized reporting 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.**

GCG identified that collecting the user's PII is a potential privacy risk; when submitting a claim form, a claimant might inadvertently provide PII, including sensitive PII or health information, that is not required or requested for claims processing or verification; data provided by individuals might not be accurate, complete, or timely; and data provided by claimants might be misused or improperly disclosed or accessed.

GCG mitigates the risk of unauthorized access to claimant information by employing a number of controls, both technical and operational, coupled with a robust IT Security Program that includes the education and training of employees on IT Security best-practices. First, and foremost, mitigation occurs by limiting the data collected to only the information required to properly administer the project. Once inside GCG's environment, that data is protected by a detailed set of policies, including administrative, physical security, network security, and logical access. These policies are reviewed and updated as needed, or at minimum annually, and are subject to external audits. Some of the controls that comprise GCG's IT Security Program include, but are not limited to the following:

- Public facing websites are hosted in a DMZ providing no direct access to internal GCG systems from the internet. The DMZ utilizes Internet protocol security and can only transmit data in an encrypted format;
- Claimants are given system generated passwords that are needed in combination with a unique ID to access their claim;
- IP addresses and server events are logged and retained;
- Automated IDS/IPS systems monitor, and proactively block, any threats to the network 24/7/365;
- Data is always housed in GCG owned and operated datacenters where it is stored on SAN infrastructure protected by Data at Rest encryption;
- Data Loss Prevention (DLP) systems that prevent the sending of PII unless authorized and sufficiently protected;
- Enterprise Class Anti-Virus/Anti-Malware is deployed on all systems and configured to scan and protect in real-time;
- A mature Patch Management program which includes vulnerability and penetration testing;
- All systems are required to log security events and forward to a centralized reporting system;
- Access to information is based on relevant need by employing the principal of least privilege, and reviewed on a quarterly basis;
- Password management policies address complexity, password history, limited retry attempts, inactivity logouts, and account disabling after a period of not logging in;
- Restricting and dispersing responsibility, system access, and access to confidential information to significantly mitigate the risk posed by insider threats;
- Physical access to and within each GCG facility is controlled by means of a card-key security system;

- The creation of a Computer Security and Incident Response Team (CSIRT) comprised of experts in their respective fields;
- Validation system integrity is maintained and information contained within the system is reviewed by the Operations department.