Security, Assurance & Compliance

Placing the Emphasis on Securing Your Data

ClearStar places security of client data as our top priority. With the extreme sensitivity of applicant information, we have multiple levels of security in place to ensure the data is never compromised. From the point of transmission, to the storage of your company's data, ClearStar uses the latest in security tools and practices for your protection. To protect the data from unauthorized access and usage, the ClearStar architecture has been designed with several security measures to ensure proper access. The following are some of the levels of security and processes ClearStar uses to ensure the proper and secure ordering of public records through our solutions.

Physical Security

Our production servers are located in a facility with 24 hour a day monitoring managed by SunGard Availability Services. To control access to the facility, card access and CCTV monitoring systems are used. Personnel requiring access to the data center must be on a pre-authorization list and show their valid driver's license prior to being able to proceed into the raised floor area. The servers are located in locked cabinets that can only be access by authorized technology support personnel. Once inside the cabinets, the server console can only be accessed by authorized technical personnel, using IDs with strong passwords. Under no circumstances do SunGard personnel have access to any client data.

Data Center

- SunGard datacenter in Atlanta, GA
- SSAE 16 Certified (copy of the attestation letter is available through ClearStar Client Service), ISO-certified procedures
- Redundant Internet connections through multiple Internet backbone providers
- Full power redundancy (minimum N+1 up to 2N+1), including underground dual-fed electrical utility system, double-ended electrical switch gear, dual Uninterruptible Power Systems (UPS's) to deliver conditioned A and B power at rack level, with battery backup that is equipped with battery monitoring
- Redundant Computer Room Air Conditioners
- State of the art, electrical, mechanical and fire system monitoring and fire suppression
- 24/7 security staff monitoring and security cameras

Restricted Physical Access

- All visitors with access to controlled areas must be logged in and logged out and will wear a visitor's badge while on the premises.
- Visitors are not allowed in the datacenter unless escorted by an authorized ClearStar employee.

Network Security

We use multiple firewalls to ensure only authorized network traffic is allowed. The firewalls log activity and network traffic is monitored by intrusion detection systems to proactively identify security threats. ClearStar keeps all production databases on a separate private network. The private network is protected with its own firewall and is inaccessible by the public. Our network infrastructure is proven and has been approved by Experian, Trans Union and Equifax for delivery of credit information via the ClearStar credit provider connection.

Workstation Security

- Users can only be authenticated into the ClearStar System from only one workstation at any given time.
- Users are not allowed to log into multiple workstations with the same valid user account.
- Authenticated users are automatically logged out after they are inactive for a specified time period (typically 20-30 minutes).

Server Security

- Production servers are protected with secure access and strong passwords.
- The number of access points along with the number of authorized users for the servers are limited to ensure security.
- Operating systems are configured with vendor's latest patches for security purposes.
- Additionally any services which are not required by the ClearStar architecture are disabled.
- Vendor best practices and recommended server hardening checklists are used when configuring new servers.
- All vendor supplied users and passwords are changed or removed when the software and/or hardware is configured.
- Wireless access to these networks is not provided or allowed.

Firewall

- Dual firewall configuration in use: one between the Internet and the ClearStar web/application servers (DMZ), and one between the web/application servers (DMZ) and the database servers.
- Internet to DMZ firewall allows only web (HTTP and HTTPS) traffic and VPN access.
- DMZ to database network is a private, non-routable IP subnet, and the firewall allows only database traffic.
- Firewalls provide stateful inspection, intrusion prevention (IPS) and intrusion detection (IDS).

Anti-Virus

- Anti-virus protection for all network traffic from the Internet is provided on the firewall.
- All servers run anti-virus protection software.

Data Security

Our databases are located on a separate, private sub network, which is not connected to the Internet with addresses that are not Internet routable. A dedicated firewall resides between the applications and databases only allowing data requests which originate from set private IP addresses. As an additional layer of security sensitive data is encrypted while at rest in the database. Data is also secured to prevent one customer from accessing another customer's data during each request to the database.

Secure Storage

- Sensitive information is encrypted in the database.
- Encryption key management procedures are in place to ensure the generation of strong keys, proper storage and destruction of keys, and that proper custodial practices are followed.

Compliance – Data Availability

- Data is accessible on the system for 60 days and is only available to authorized individual users from the requesting client. Final reports are available in PDF format indefinitely as a historical view of the original request.
- Credit bureau data is purged after 90 days and can only be retrieved by authorized ClearStar personnel for audit or dispute purposes. Other sensitive data is purged, if necessary, according to schedules determined by the appropriate legal or legislative authority.
- No data is stored for any length of time on the application server.

Backups and Reliability

- Our production facility is configured to provide redundancy to prevent a single point of failure.
- All production equipment is covered under service agreements with vendors to ensure optimal turnaround if any hardware failures should occur.
- Backups are completed on the applications and database to ensure copies are moved off site for storage on a regular basis.
- Databases transfer all transactional data real time using replication to ensure a secondary server is always up to date and available for failover.
- Additionally full, differential, and transaction log backups are completed on our production database servers to ensure every transaction is captured.
- Back-up media are secured in a locked safe in the ClearStar offices.

Disaster Recovery

- ClearStar has disaster recovery plans in the event of loss of production servers or the production environment.
- Business continuity plans outline scenarios and team responsibilities to implement the return of critical operations.
- Documented plans are tested to ensure decisive results if a scenario should transpire.
- Agreements and partnerships are in place to provide support and assistance during unfortunate scenarios.

- Senior management reviews plans quarterly to confirm they are up to date and ensure the entire recovery team understands their responsibilities.

Application Security

The security of the application is ensured by various measures starting with the development, test and release process. The application is developed with secure coding standards in mind, peer reviews are conducted at various stages, and the development and test environments are separate from production. All communication with the application is over secure, encrypted connections using 128-bit SSL. Personal Identifiable Information (PII) is not sent via unsecured mechanisms and is masked to the end user. To ensure the identity of each user when logging in, strict account authentication standards have been set, including strong password requirements.

Secure Encrypted Connections

- Any connection to the web applications or through the interfaces requires 128-bit SSL (secure socket layer) encryption.
- ClearStar solutions are protected via digital certificates issued by GeoTrust.
    - GeoTrust's Identity Verification Services ensures the identity of business entities and/or individuals in online transactions.
    - Users can ensure the information they are sending is protected by locating the lock icon on the browser window in the address bar or the status bar.
- Personal Identifiable Information (PII) is not e-mailed or sent over clear text. Users are sent e-mail notifications with links to the reports containing PII. The user must login to access the report.
- Personal Identifiable Information (PII) is masked when displayed to the end user.

User Authentication

- ClearStar solutions require each user to have a valid username and password.
- Strong type passwords are enforced to ensure obvious or simple passwords are not selected.
- Users are forced to changed passwords every 90 days or risk being locked out of the system.
- Only ClearStar administrators or site administrators can reset a user once they are locked out from the system.
- After 4 consecutive, unsuccessful login attempts, the user account is locked and prevented from accessing the system until a ClearStar administrator or site administrator unlocks the account.

Strong Password Support

- Password must have a minimum length of 8 characters
- Passwords must have at least one number
- Passwords must have at least one lower case letter
- Passwords must have at least one upper case letter
- Passwords must have at least one special or punctuation character
- User name, company names, initials, etc. cannot be included in the password.

- Passwords cannot be reset to be the same as one of their last three passwords.

Develop & Maintain Secure Systems and Applications

- All relevant security patches are installed within one month of release by the software vendor. Critical items are installed as soon as possible within the constraints of the production environment.
- Common coding vulnerabilities like those at http://www.owasp.org/ must be accounted for and avoided.
- Initial software development and unit testing happens in a development environment that is comparable to, and completely separate from, the test and production environments.
- Code is peer reviewed following unit testing to ensure quality and to identify and potential vulnerabilities.
- Data that is used in the development and test environments is similar to production data, but does not include any real data (e.g., credit report information), production account information (e.g., connection accounts for credit interfaces), or personal identifiable information (e.g., SSN, date of birth).
- Pre-release testing will be performed in the test environment that is comparable to, and completely separate from, the development and production environments.
- Software patches will be tested in the development and test environments prior to releasing to the production environment.

Policies & Procedures

ClearStar has established a strong security policy for both employees and contractors. By regularly tracking and reviewing system events, audit trails and log files, the ongoing security of the system is monitored regularly. The systems are subjected to vulnerability scans and penetration tests regularly by third-parties to ensure that changes and upgrades have not caused a decrease in the level of security over time. The policies are reviewed regularly, both internally and by outside organizations.

Contract Requirements

- All customers using ClearStar software as a service solution to order and obtain public records are preauthorized and predefined by contract within our system.
- The system contract is configured so only authorized services for that particular customer are available.
- A customer must be authorized to obtain credit reports prior to that service being made available to their contract.

Track & Monitor

- Server Operating System event logs are set to log:
    - Successful and failed logons
    - Denied access to Level 3 and Level 4 systems
    - Policy changes

    - System events
- ClearStar audit trails track system changes, changes to sensitive information, status changes, and other important workflow events.
- Firewall events, included IPS and IDS events, are logged and forwarded to the syslog server
- A centralized syslog server is used to store all events and send notifications and reports to system administrators.
- All level 3 and 4 events are evaluated as soon as they occur. Log reports are reviewed daily.

Regularly Test Systems

- The Information Security Officer conducts quarterly reviews of the security procedures.
- Quarterly vulnerability scans and yearly penetration tests are performed.

Maintain Security Policies

- The *Information Security Program Standards and Procedures* are maintained and updated yearly, and when changes are warranted based on business factors or new security requirements.
- All employees and contractors must read and understand the policies, as they pertain to their job function.
- All employees must pass a standard pre-employment screening process.
- The policies include an incident response plan that defines how ClearStar will respond to any potential breaches in security.

Audits and Certifications

ClearStar is audited yearly by SecureWorks to ensure that appropriated security controls are in place in the technology, the processes, procedures, and documentation. ClearStar has been approved under the Experian EI3PA process to process requests for Experian credit data. Through this certification process, ClearStar is approved to process requests for Equifax and Trans Union credit data as well.

Independent Security Audits

- ClearStar architecture is independently certified by SecureWorks, an approved third party certification agency of the major credit bureaus.
- Our technology, processes, and infrastructure are subject to audit and review at a minimum of every six months without notice. These independent findings are reported to the credit bureaus to ensure security compliance.
- Vulnerability scans are performed on the ClearStar network quarterly by SecureWorks.
- Penetration tests are performed on the ClearStar network and systems yearly by SecureWorks.

Experian EI3PA Certification

The Experian EI3PA process is based on the PCI DSS. It is a much more detailed and explicit standard than any prior Experian, Equifax or Trans Union assessments. This process mirrors the requirements, procedures, and structure of the PCI DSS, except that it is geared toward the protection of “Credit Data”

as opposed to the PCI focus on “Credit Card data”. ClearStar has been approved to process requests for all three credit vendors, Experian, Equifax, and Trans Union, since 2000 and has been EI3PA certified since the beginning of the process in 2009.