Security Overview

Lending Cycle, Inc. (LCI, LCI Corp.) incorporates many processes and procedures to protect their network and application environment. These processes and procedures are reviewed frequently and updated as needed. The following items describe many of the security measures in place today.

Physical Environment

All LCI application and database hardware systems are hosted in a SAS 70 Type II and SSAE16 audited 99.999 percent environment (primary is in Indianapolis, Indiana). This environment has 24-hour physical security and network monitoring by on-premises staff, redundant generators and power sources, redundant network feeds, and other redundant systems.

Network Environment

LCI application and database hardware systems are protected by multiple and redundant firewalls that are monitored 24 hours a day. Plus, LCI production systems are accessed by mutli-step/multi-layer encrypted VPN administrator access. LCI performs all maintenance on their production servers.

Physical Systems

All LCI application and database hardware systems utilize redundant storage systems, redundant power supplies (that are connected to separate circuits), and other redundant systems.

Database Environment

All client data tables are separated and only contain their data. Sensitive and actionable information is encrypted with AES cryptology. Direct access to production databases is highly restricted.

Data Encryption

All sensitive data (including passwords) is encrypted with AES cryptology (which is considered secure for U.S. Government data by the NSA).

Application Encryption

LCI encrypts user activities using Secure Sockets Layer (SSL) technology. Plus, all login points utilize multiple security methods and have AutoComplete restricted.

User Access & Password Management

LCI utilizes multiple user authentication roles that are accessible via multiple password protection schemes and methodologies including strong 8+ character alpha numeric passwords, complex usernames, previous password restrictions, selectable password expiration time frames, multiple challenge questions, instant team expirations, and many others.

Security Breach Notifications

If there is a breach, intrusion, and/or otherwise unauthorized access involving customer data stored by LCI, LCI will immediately notify customers (within 90 minutes) of the breach discovery and disconnect involved databases from the network. That notification will include the details of the issue, immediate steps taken by LCI, and an action plan to remedy the issue.