

# LendingCycle Security Overview

To make sure that your data is secure, Lending Cycle, Inc. (LCI) incorporates many processes and procedures to protect the entire network environment. These processes and procedures are reviewed weekly, 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 Compliant 99.999 percent facility in Indianapolis, Indiana (see nFrame 2007 SAS 70 Report – nFrame’s team manages our network environment). 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

All LCI application and database hardware systems are protected by multiple and redundant firewalls that are monitored 24 hours a day (network environment is diagrammed later in this document). Plus, all LCI systems containing databases have no direct connection to the Internet and only multi-step/multi-layer encrypted VPN administration access that can only be utilized by LCI Corporate Officers (logs of their activity are reviewed by a committee). LCI employees perform all maintenance on production servers.

## Physical Systems

All LCI application and database hardware systems utilize redundant RAID storage systems, redundant power supplies (that are connected to separate circuits), and other redundant systems. LCI employees and vendors (including nFrame) are never granted administrative access to production application, backup, or data servers. Only two corporate officers (President and CEO) are granted access and can only do so from three controlled remote entry points via multi-step/multi-layer VPN 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 with 128-bit 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.

## Disaster Recovery

All LCI production systems are housed in Indianapolis, Indiana with a back center in Louisville, Kentucky.

## 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.