



**A-LIGN**

LoanPro Software, LLC

Type 2 SOC 3

2023



**SOC 3 FOR SERVICE ORGANIZATIONS REPORT**

**July 1, 2022 to June 30, 2023**

# Table of Contents

<b>SECTION 1 ASSERTION OF LOANPRO SOFTWARE, LLC MANAGEMENT .....</b>	<b>1</b>
<b>SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT .....</b>	<b>3</b>
<b>SECTION 3 LOANPRO SOFTWARE, LLC'S DESCRIPTION OF ITS COMPUTER SOFTWARE SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2022 TO JUNE 30, 2023 .....</b>	<b>7</b>
OVERVIEW OF OPERATIONS .....	8
Company Background .....	8
Description of Services Provided.....	8
Principal Service Commitments and System Requirements.....	8
Components of the System .....	9
Boundaries of the System .....	17
Changes to the System in the Last 12 Months .....	17
Incidents in the Last 12 Months.....	17
Criteria Not Applicable to the System.....	17
Subservice Organizations.....	17
COMPLEMENTARY USER ENTITY CONTROLS .....	18

**SECTION 1**  
**ASSERTION OF LOANPRO SOFTWARE, LLC MANAGEMENT**

## ASSERTION OF LOANPRO SOFTWARE, LLC MANAGEMENT

July 13, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within LoanPro Software, LLC's ('LoanPro' or 'the Company') Computer Software Services System throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that LoanPro's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "LoanPro Software, LLC's Description of Its Computer Software Services System throughout the period July 1, 2022 to June 30, 2023" and identifies the aspects of the system covered by our assertion.

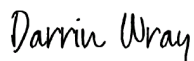
We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that LoanPro's service commitments and system requirements were achieved based on the trust services criteria. LoanPro's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "LoanPro Software, LLC's Description of Its Computer Software Services System throughout the period July 1, 2022 to June 30, 2023".

LoanPro uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at LoanPro, to achieve LoanPro's service commitments and system requirements based on the applicable trust services criteria. The description presents LoanPro's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of LoanPro's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve LoanPro's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of LoanPro's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2022 to June 30, 2023 to provide reasonable assurance that LoanPro's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of LoanPro's controls operated effectively throughout that period.



---

Darrin Wray  
VP of Operations  
LoanPro Software, LLC

**SECTION 2**  
**INDEPENDENT SERVICE AUDITOR'S REPORT**



## INDEPENDENT SERVICE AUDITOR'S REPORT

To LoanPro Software, LLC:

### *Scope*

We have examined LoanPro Software, LLC's ('LoanPro' or 'the Company') accompanying assertion titled "Assertion of LoanPro Software, LLC Management" (assertion) that the controls within LoanPro's Computer Software Services System were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that LoanPro's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

LoanPro uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at LoanPro, to achieve LoanPro's service commitments and system requirements based on the applicable trust services criteria. The description presents LoanPro's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of LoanPro's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at LoanPro, to achieve LoanPro's service commitments and system requirements based on the applicable trust services criteria. The description presents LoanPro's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of LoanPro's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

### *Service Organization's Responsibilities*

LoanPro is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that LoanPro's service commitments and system requirements were achieved. LoanPro has also provided the accompanying assertion (LoanPro assertion) about the effectiveness of controls within the system. When preparing its assertion, LoanPro is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

### *Service Auditor's Responsibilities*

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

#### *Independence and Ethical Responsibilities*

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

#### *Inherent Limitations*

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

#### *Opinion*

In our opinion, management's assertion that the controls within LoanPro's Computer Software Services System were suitably designed and operating effectively throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that LoanPro's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of LoanPro's controls operated effectively throughout that period.

The SOC logo for Service Organizations on LoanPro's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

#### *Restricted Use*

This report, is intended solely for the information and use of LoanPro, user entities of LoanPro's Computer Software Services during some or all of the period July 1, 2022 to June 30, 2023, business partners of LoanPro subject to risks arising from interactions with the Computer Software Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.



This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

---

Tampa, Florida  
July 13, 2023

### **SECTION 3**

## **LOANPRO SOFTWARE, LLC'S DESCRIPTION OF ITS COMPUTER SOFTWARE SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2022 TO JUNE 30, 2023**

## **OVERVIEW OF OPERATIONS**

### **Company Background**

LoanPro Software, LLC ('LoanPro') was organized in 2008, with a vision to create a robust loan management system ('LMS'). LoanPro's corporate offices are located in Farmington, Utah.

The LoanPro LMS was created to offer lenders in the United States and Canada a modern, cloud-based solution for managing and servicing loans. The LoanPro LMS is offered under a subscription-based model. The LoanPro application programming interface (API) allows users to integrate LoanPro's LMS for servicing loans with a lender's existing applications.

### **Description of Services Provided**

The services provided by the LoanPro LMS include the following:

- Providing customizable features, line of credit and loan calculators that can be configured for multiple loan types
- Providing day-to-day, accurate information for loan balances, credit available, balances past due, payoff quotes, etc.
- Providing customizable advanced communication, allowing lenders to automate routine loan- line of credit servicing communication tasks
- Providing a customer-facing website where borrowers can log in, view their loan data, credit available and make payments on their loans and line of credit
- Providing transaction history reports, including operational, management and ad hoc reports in a variety of formats
- Providing onboarding, customer service, custom programming and account management services to enterprise customers
- Providing a programmable interface in the form of an API, allowing lenders to integrate the full set of LoanPro LMS features with their existing backend services

LoanPro's LMS is hosted by Amazon Web Services ('AWS'), using the AWS Infrastructure-as-a-Service ('IaaS') offering. The description includes the control objectives and related controls of LoanPro's LMS but does not include the controls of AWS. In addition, the description addresses only the LoanPro LMS and services provided to user entities, and excludes other services provided by LoanPro, including Secure Payments and Connections. The description is intended to provide information for user entities of the LoanPro LMS and their independent auditors who audit and report on such user entities' financial statements or internal control over financial reporting, to be used in obtaining an understanding of the LoanPro LMS and the controls over the system that are likely to be relevant to user entities' internal control over financial reporting. The description of the system includes certain business process controls and information technology (IT) general controls that support the delivery of LoanPro's LMS.

### **Principal Service Commitments and System Requirements**

The following five interrelated components of internal control at LoanPro include the following:

- Control environment
- Risk assessment process
- Monitoring activities
- Information and communication
- Control activities

## *Control Environment*

The control environment sets the tone of an organization and influences the control awareness of the organization. LoanPro's control environment has been established by members and senior management, who understand the need for controls. The emphasis placed on appropriate controls is supported through the actions of the Board of Directors and senior management of LoanPro and by policies, processes and procedures and organizational structure.

The primary elements of LoanPro's control environment include the following:

- Commitment to integrity and ethical values
- Oversight responsibility of the Board of Directors
- Assignment of authority and responsibility
- Commitment to competence
- Accountability

## **Components of the System**

### *Infrastructure*

LoanPro's network infrastructure is provided by AWS and consists of three subnet groups: private (no inbound and outbound connections), protected (only outbound connections) and public (inbound and outbound connections). Servers are divided into topics, keeping them single-purpose both for performance and security reasons. Some topics are grouped in load balancers (such as Web/API servers). Servers are placed into one of the three subnets above.

Services provided by AWS for LMS infrastructure are hosted in the US-East-1 (North Virginia) AWS region. When possible, infrastructure is hosted in multiple availability zones.

AWS is responsible for the security of the cloud and is responsible for patching and fixing flaws with its infrastructure; however, LoanPro is responsible for patching its guest operating system and applications. AWS is also responsible for maintaining the configuration of its infrastructure devices; however, LoanPro is responsible for configuring the guest operating system, databases and applications.

LoanPro maintains established and documented processes for the hardening and configuration of servers. AWS provides a "vanilla" image, and an automated hardening process is applied before servers are allowed to serve any traffic. Production images have built-in security provided by a cloud security agent.

LoanPro's operating procedures dictate the patch management process to be followed. New vulnerabilities are reviewed weekly, and a log is maintained documenting the patched and unpatched vulnerabilities. Non-critical vulnerabilities are patched on a monthly basis, while critical vulnerabilities are patched immediately.

Servers are not patched directly in production; rather, new images are created with applicable patches applied, and live servers are substituted with new servers created from the patched images. Servers are monitored on a quarterly basis with both an internal scan (using AWS Inspector with available rule definitions) and an external scan using a third-party provider.

### *Software*

Primary software used to provide LoanPro's Computer Software Services System includes the following:

<b>Primary Software</b>		
<b>Software</b>	<b>Operating System</b>	<b>Purpose</b>
LMS	Multiple	Manage customers, loans, payment profiles, line of credit, payment information, collateral, payment terms, etc.

## People

The control environment at LoanPro originates with a five-member Board (equity owners of the Company). Three members of the Board participate in the day-to-day operations of LoanPro; however, this Board has unanimously appointed one of the members as Chief Executive Officer (CEO) of the Company. The Board provides oversight of LoanPro's operations and activities, including oversight of the internal control environment.

LoanPro has also created an Adviser's Council, which consists of legal, tax and financial technology professionals with experience in the lending and financial industry sector. These individuals provide additional insight and perspective to the Board. The Adviser's Council meets with the Board semiannually.

LoanPro has an Audit, Process and compliance Director who is responsible for establishing sound business processes throughout the organization and developing policies supporting the internal control environment. The CEO, C-level and/or Process Owners are responsible for reviewing LoanPro's policies and procedures on at least an annual basis.

## Data

LoanPro has specified its control objectives and identified its controls to achieve these objectives as determined by management. For each control objective, there are controls that are designed to achieve the stated control objective.

The components of the LoanPro LMS included within this report are as follows:

- Customer Onboarding, Contract-Matching Process and Loan Calculators
- Data Validation, Error Checking and Processing Activity
- Customer Payment Transaction Cycle
- Reporting
- Application, System Development and Change Management
- Logical and Physical Security
- Network Infrastructure
- System Operations, Monitoring and Data Transmission
- Data Backup and Recovery

### Customer Onboarding, Contract-Matching Process and Loan Calculators

Prospective customers are provided with a trial version of the LoanPro LMS. At the time the free trial is established, the prospective customer is required to enter an email address. A live instance of the LoanPro LMS is created and includes a database populated with templated sample data. The prospective customer is considered the default administrative user and has administrative access to the newly established tenant. Upon executing a Software-as-a-Service ('SaaS') or Private-Software as-a-Service ('PSaaS') agreement with LoanPro, the customer onboarding process is initiated. The customer receives an initial orientation overview on the onboarding process.

The onboarding process consists of the following steps identified below:



During discovery, the customer provides diagrams and internal process documentation regarding lending processes, examples of loan contracts used by the customer, and any other documentation necessary for the Onboarding team to assist in the customer's configuration.

Payment processing is an important component of Onboarding. The Onboarding team and software engineers assist the customer by providing information about integrating with the LoanPro LMS application programming interface ('API') to best process payments using the customer's chosen payment processing method. Credit/Debit card and bank data do not reside in the LoanPro LMS.

During the configuration process, the Customer Onboarding team assists new customers in configuring the LoanPro LMS to conform to the customer's business rules and practices identified in discovery.

Settings for calculations (payment application calculator, loan/interest, line of credit calculator, payoff calculator, waterfall calculator) are integral in establishing settings for customers. Although calculations can be performed in different ways, calculation settings should be consistent across loans and line of credit. LoanPro achieves the correct settings and configurations for each customer's account via a contract-matching process. The customer is required to provide examples of contracts that illustrate loans and/or line of credit with various servicing or repayment statuses which include current, paid-off, past-due, renewed, modified, or sold. These contracts should include the payment history and the application of payments in the case of the loans. LoanPro's Onboarding team then finalizes the configuration of the customer's loan/line of credit and payment application calculation settings. This process ensures that loan/lines of credit and payment settings are configured to match the customer's existing portfolio of loans/lines of credit and to apply consistent settings to the customer's future loans. The types of calculators in the LoanPro LMS are described below:

#### Loan Calculator

Customers can select the appropriate settings at both a tenant level and in some cases at a loan level, which impacts the loan calculation of that account. For example, when setting up the configuration of a loan account, a selection can be made to establish the frequency of scheduled payments, such as weekly, monthly, etc. The selection of this will not only impact the calculations of the payment due on the account, but also will impact the calculation of delinquency on the performance of the loan. Advanced configuration settings include loan type, loan category, calculation type, discount calculation and discount split, days in the year, first period days, interest application, begin/end (due at the beginning or end of the period), last as final (include any extra accrued interest), first day interest, fees paid by, payment date application, etc.

#### Payoff Calculator

In the LoanPro LMS there are specific settings at both a tenant level and also at a loan level which impact the way in which a payoff amount is calculated. Similar to the Loan Calculator, the Payoff Calculator is a specific calculation used to determine the remaining amount needed to pay off a loan in full. The LoanPro Platform can be configured to consider repossession fees, early payoff fees, today's payoff or a payoff based on some date in the future.

#### Waterfall Settings Calculator

When payments are applied to a loan, they are applied in a waterfall manner, namely they are applied first to the due component and if there are remaining funds, they are then applied to the next due component in the waterfall. The terms of a loan agreement typically include the outline of the application of such payments. The most common waterfall application order is to apply payments towards due fees, due interest and then due principal. Customers have the ability to change how payments are applied within the calculator.

### Line of Credit Calculator

In the case of Line of Credit (LOC) the calculator has the ability to calculate total balance, payoff, last payment amount, next payment amount, interest, amount past due, available credit, etc. to ensure that the line of credit is consistent with the contracts given by the creditor.

The onboarding process also includes updating the administrative user of the customer's account, if applicable. The administrative user is responsible for granting appropriate access to other customer users within the LoanPro LMS.

During the data import phase of the onboarding process, an import validation process is conducted to ensure the population of loans/lines of credit provided by the customer matches the number of loans/lines of credit included in the LoanPro LMS. If an exception is noted, it is resolved to ensure the entire population of loans/lines of credit are imported into the LoanPro LMS. At this point, an initial import validation report is provided which identifies the customer's loan/line of credit balances that agree to LoanPro's calculations and the loans that do not match.

Onboarding personnel work with the customer to resolve individual loan/line of credit balance discrepancies. This process is repeated until there are no exceptions remaining.

A training program is provided to the customer on the LoanPro LMS once the data import is verified. Users may also access the LoanPro's "knowledge center" to obtain articles and additional information on how to operate the system.

When the customer is ready to launch the LoanPro LMS, the customer is required to accept the data import and configuration settings established by the Onboarding team and the customer. In the event that a discrepancy is subsequently found, the customer can contact the Support team.

### Input and Data Validation

Although customers are ultimately responsible for data submitted to the LMS, LoanPro has created various input and data validation rules to assist customers in identifying errors and incomplete data fields prior to activating a loan/line of credit. LoanPro has defined data fields used in the LMS, consisting of required data fields (fields which are necessary to calculate a loan/line of credit) and non-required fields (fields that may be applicable to a loan / line of credit but are not necessary to calculate a loan). There are three ways to import and activate loans within the LoanPro LMS:

1. Customers can manually input data using the user interface (UI) in multiple screens and modules within the LMS. Various error messages occur when data fields either contain a type of data that is not accepted by field format, or a required field contains an error or is incomplete. After remediation for required fields, a list of nonrequired fields appears on a transaction warning pop-up that the customer accepts. In addition, once a loan/ line of credit is submitted and accepted, another pop-up warns the customer that the terms and settings of the loan line of credit are locked.
2. Large data sets can be imported into the LoanPro LMS using a comma-delimited value ('CSV') file template that can be accessed within the application. This import feature allows customers to import data sets containing different types of transactions and actions. Batches are either accepted or rejected. If the batch is rejected, the LMS identifies the particular data fields that need to be corrected.
3. Data imports can be processed automatically via the customer's API, where customer systems import data into the LoanPro LMS on API-enabled functionality. The customer's website can also be accessed by borrowers to add payments and update personal, collateral or insurance information.

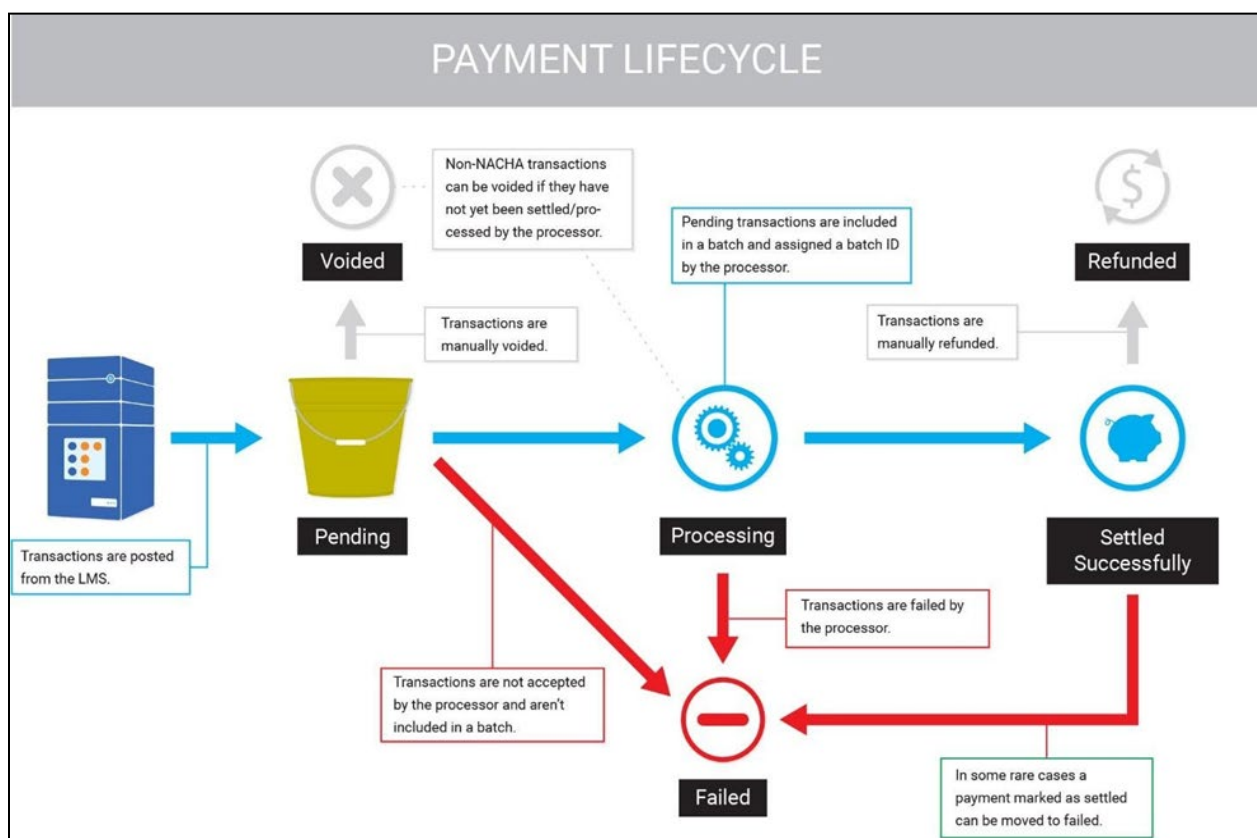
Additional rules identify whether a duplicate payment has previously been submitted, the first payment date is prior to the loan contract date, etc.

## Customer Payment Transaction Cycle

Payment transactions are also governed by validation controls built within the LMS. A payment import transaction template (CSV) can be accessed and used by customers to ingest payment information into the LMS. A UI for uploading payment information ingests the import and reports the percentage of records validated, percentage of records imported, and number of records updated. Validation controls also screen import data for improper values based on payment type, payments on non-existent loans, etc.

Payment transactions are only processed if data imports are successful. Payment requests are transmitted by the LoanPro LMS to Secure Payments to the customer's payment processor or financial institution and are based on the customer's requirements. At the completion of the transmission, the payment processor or financial institution relay a status back to the LoanPro LMS, as follows:

A call-back URL is used to capture data sent about transactions by payment processors. When updated status information is received, statuses are changed in near real-time.



## Reporting

Customers can access reports available on the UI of the LoanPro "reports" section. Templated reports have been created by LoanPro; however, customers may request additional report templates. Customers also can create output CSV files from varying parts of the application. The LoanPro LMS has the ability to provide API outputs that are consumed by customer systems. Reporting problems or errors identified by customers should be communicated to the Support team. Issues and problems that cannot be resolved immediately are tracked. Resolution timelines are governed by service legal agreements based on the customer's subscription level.



Report queries can be manually or automatically set and are available for download for 24 hours and are stored within AWS' S3. Report downloads are encrypted using transport layer security ('TLS') 1.2. Reports generated for loan balances/line of credit, payment statuses and interest use available near real-time data held within the LMS.

Modification of report templates follow established change management processes and procedures. Report servers are clustered and secured in the private subnet and are also protected by a cloud security agent.

### *Processes, Policies and Procedures*

LoanPro has developed policies, processes and procedures centered around control activities to ensure LoanPro's objectives are carried out and risks are mitigated.

Control activities are performed throughout the organization and include automated and manual procedures. In addition, control activities are performed at various stages during business processes. Controls activities may be preventive or detective in nature. Duties and responsibilities are allocated across LoanPro to ensure appropriate segregation of incompatible duties.

A formal process is in place to review policies, processes and procedures and control activities on at least an annual basis. Changes in policies and procedures are approved by the Process Owners, CEO and/or other C level members and are communicated to employees.

### Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system.

### Logical Access

LoanPro has implemented role-based security in the LMS environment, which is defined through AWS' Identity and Access Management ('IAM') roles. Additionally, employees are granted logical access to in-scope systems based on documented approvals by appropriate management personnel. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. Software Support and IT personnel conduct quarterly reviews to verify whether individuals' access is necessary for their job function and to identify the existence of inappropriate accounts.

In the event an employee terminates employment with LoanPro, the employee's access to information assets and to the LMS environment is removed immediately.

Administrative access to private subnets within the LMS production environment requires user access through the protected network. Such access is limited to only authorized individuals.

LoanPro utilizes the Amazon Aurora database engine within AWS. Databases containing customer data are stored within volumes. The primary Aurora instance is replicated across multiple availability zones for reliability.

Database fields containing confidential data or personally identifiable information (social security numbers, passwords, date of birth, driver's license) are encrypted. The LoanPro LMS is a multi-tenant application, where the tenancy is defined at the database layer (each tenant has their own database in one of the available database servers, or in a non-shared database server if requested).

Aurora database clusters are created in AWS' Virtual Private Cloud ('VPC'), and access to database instances is controlled through a VPC security group managed by LoanPro. By default, databases are placed in a private subnet with no public connectivity allowed. To establish a connection to a database instance, LoanPro uses Systems Manager ('SSM') through AWS' Command Line Interface ('CLI') tool. To monitor individuals who access the console, a log collects activities performed; the log is stored in the SSM service.

LoanPro uses AWS' S3 to store documents. Storage is segregated by tenant using a unique identifier, which relates the customer to the attachment stored in Amazon S3.

### Computer Operations - Backups

LMS data is backed up according to LoanPro's Data Backup Policy. LoanPro employs a real-time hot standby database for operating SQL databases. Data is synchronously replicated automatically to multiple availability zones, even if the database itself is hosted in a single availability zone. This provides data redundancy, but also allows for instance fail-over. In the event of a failure, the cluster automatically selects a read replica to be promoted as the master with minimum service interruption (within 30 seconds) with no manual interaction required. LoanPro database servers use AWS' Aurora MySQL engine.

Point-In-Time Recovery ('PITR') is enabled for the entire database fleet. This is achieved through AWS' Relational Database Service ('RDS') which creates automated snapshots and Aurora backup data. LoanPro has the capability to restore the database to one of the existing daily snapshots (up to the past seven calendar days) or to a specific point in time in the same period within five minutes.

LoanPro utilizes the snapshot feature of Amazon RDS to perform incremental backups up to the past seven calendar days. These daily backups are redundantly stored in AWS' S3. Amazon S3 redundantly stores data in multiple facilities and on multiple devices within each facility. To increase durability, Amazon S3 synchronously stores snapshot data across multiple facilities before confirming that the data has been successfully stored.

For documents, images and files uploaded to the application, LoanPro utilizes Amazon S3 cloud storage with versioning enabled. This versioning allows LoanPro to retrieve not only the most recent version of the file, but up to the last 100 saved revisions of the file.

### Computer Operations - Availability

#### System Operations, Monitoring and Data Transmission

LoanPro's security team (Chief Technology Officer ('CTO') and the Software Support and Operations Managers) have established a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, application environment and log monitoring and reporting, firewall notifications, intrusion detection systems ('IDS'), file integrity management, internal vulnerability assessment reports and operating system event logs. These alerts and notifications are reviewed daily by the Software Support and Operations IT Support team.

An on-call monitoring team on different levels has been established to ensure that in the occurrence of a significant event after hours that requires immediate attention, LoanPro personnel are available to respond.

Data within the LMS and the greater LoanPro infrastructure is carefully guarded. Data is encrypted in transit using current TLS standards. Depending on the sensitivity of data, it may also be encrypted at rest (i.e., social security numbers, passwords, date of birth, driver's license).

LoanPro utilizes encryption keys provided by AWS. Encryption keys are rotated every 90 days. LoanPro is responsible for managing encryption keys.

Input of data (either manually or automatically via the API) into the LMS is also secured by TLS. Input files are directly imported into AWS' S3.

Output data reports are produced by customers and are available in (electronic PDF, comma-delimited value file exports, or electronically from the customer website). The availability of accessing these reports is based on customer access controls. Reports delivered outside of the boundaries of the system are secured by trusted security certificates. LoanPro uses the latest TLS to encrypt such outputs.

### Change Control

The application used in the LoanPro LMS is developed and maintained by LoanPro. Software updates are released on a monthly basis using the continuous integration and continuous delivery service ('CI/CD') through AWS' CodePipeline. Prior to releasing major software updates to the production environment, LoanPro provides release notes to customers explaining the changes in the software update.

LoanPro has a formalized change management process in place, which requires the identification, documentation, assessment of risk and potential impact of changes, approval of changes, and testing of changes to verify operational functionality.

LoanPro uses a "Voice of the Customer" process to identify customer-requested changes to features within the LMS. Weekly meetings and/or company communication channels and tools are used by the Product Management team as needed to determine the criticality of the issue before it is assigned to the development team.

LoanPro utilizes an agile based development methodology. Developers are assigned tasks which are organized in a continuous delivery flow. Phabricator and Monday.com are used to monitor the progress of changes.

The development environment within AWS is segregated within the VPC and includes local and beta environments.

Software Support personnel are responsible for deploying code to the production environment and may do so only after the necessary testing and final code is published to the master branch within AWS.

In the event a change management process may impact any of the following: interest accrual calculations, APR calculations, waterfall application of payments and/or live payment processing workflows, additional change management processes are initiated. These processes include additional testing by a Finance Business Analyst/UAT specialized team and are conducted in an appropriate test environment to ensure that there is no impact to past, current or future calculations.

LoanPro has the ability to initiate roll-back to an earlier version of the application in the event the deployment of a new version of the software has significant unintended consequences.

### Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled or disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications, and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a monthly basis in accordance with LoanPro policy. The third-party vendor uses industry standard scanning technologies and a formal methodology. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the LoanPro system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system from the Internet through the use of leading Virtual Private Network (VPN) technology. Employees are authenticated through the use of a token-based MFA system.

### **Boundaries of the System**

The scope of this report is limited to the Computer Software Services System performed in Farmington, Utah and by remote employees.

### **Changes to the System in the Last 12 Months**

LoanPro moved to a new facility in July of 2022 to accommodate the growth of the company.

### **Incidents in the Last 12 Months**

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

### **Criteria Not Applicable to the System**

All Common Criteria/Security criteria was applicable to the Computer Software Services System.

### **Subservice Organizations**

This report does not include the cloud hosting services provided by AWS at the various facilities.

#### *Subservice Description of Services*

AWS is responsible for monitoring and managing the supporting infrastructure that supports the Computer Software Services. As such, all physical and environmental controls are the responsibility of AWS.

#### *Complementary Subservice Organization Controls*

LoanPro's services are designed with the assumption that certain controls will be implemented by subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the Trust Services Criteria related to LoanPro's services to be solely achieved by LoanPro's control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of LoanPro.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - AWS		
Category	Criteria	Control
Common Criteria / Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic IDS are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.

LoanPro's management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as service level agreements. In addition, LoanPro performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

## COMPLEMENTARY USER ENTITY CONTROLS

LoanPro's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to LoanPro's services to be solely achieved by LoanPro control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of LoanPro's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to LoanPro.

2. User entities are responsible for notifying LoanPro of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of LoanPro services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize LoanPro's services.
6. User entities are responsible for providing LoanPro with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying LoanPro of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.