Policy for Safeguarding Private Information

Last Updated October 16, 2023

Policy

As LoanPro Software provides software to lenders in many spaces, several spaces that we operate in require our client (the business engaging in lending) to have a policy for their lending business that outlines how they safeguard Personal Information about their customers. To stay in compliance with the Gramm-Leach-Bliley (GLB) Act, federal law, and Federal Trade Commission (FTC), where relevant, as the software provider and system of record for our clients LoanPro Software, to its knowledge, is compliant with all aspects of these statutes and rulings. It is the financial institution's responsibility to be compliant with all federal, state, or other governmental regulations. To this end, Secure Payments assists in this compliance in many ways, including:

(a) Data Storage and Data Transmission -- Secure Payments is a cloud-hosted SaaS software, where all of the data is stored in secure physical locations maintained by Amazon AWS. We transmit all data using HTTPS (secure socket layer) encrypted data transmission. All stored data is encrypted at rest.

(b) Payment Profile information -- all payment profile information including credit card, debit card, name on card, and card expiration date, is tokenized & stored in a compliant manner with PCI-DSS Level 1 certification. When integrated applications (Third Party applications, including LoanPro family products) processes a payment, it submits only the token, payment amount, and processor ID (identification of third-party payment processor) to Secure Payments. This process limits the exposure and interaction with the raw payment-profile data. All data in Secure Payments related to the payment profile is encrypted using cryptographically secure keys managed by Amazon Key Management System (KMS). Keys are rotated on a yearly basis.

(c) Personally Identifiable Information -- Secure Payments encrypts all stored values in a database for organization & limiting exposure.

(d) Fraud and Data Verification Tools -- Secure Payments provides several tools, some, including third-party integrations through the Connections software product, to verify if the data provided is accurate. This includes phone number verification, USPS address verification, bank account verification, OFAC testing, and other tools to help limit the fraudulent use of personal, private information.

The Gramm-Leach-Bliley (GLB) Act, a federal law, requires that financial institutions take steps to ensure the security and confidentiality of this kind of customer data. Secure Payments provides the tools necessary for our clients to comply with this in regards to payment profiles and payment processing.

Safeguarding Personal Information is a top priority to Secure Payments and should be to all of our clients. We suggest the following steps be followed to ensure that personal data remains confidential and secure.

1. Develop a written information security plan that describes the policy and procedures to protect customer information. Keep in mind the nature and scope of your activities, business operations, and the type, reliability, sources, life cycle, transmission, and storage (in all forms, including hard copy - if applicable) of data.
2. Designate team members/employees who are responsible to coordinate all safeguards for your organization, identify and assess the risks to the customer information for each business operation. Evaluate the effectiveness of current safeguards and if any changes are needed. Also include control measures to monitor these safeguards, and make any adjustments needed if conditions change.
3. Select appropriate service providers and require them, by contract, to implement the necessary safeguards. Perform testing to ensure Secure Payments is compliant with our policies regarding these disclosed safeguards.
4. Areas of focus should include at least the following, which are of potentially high-risk to information security:
    a. Employee Training and Management
    b. Information Systems, including network, software design, information transmission, storage, transmission and retrieval, security management.
    c. Security Management, including prevention, detection, and response to attacks, intrusions, etc.

References:

- https://www.ftc.gov/tips-advice/business-center/guidance/safeguarding-customers-personal-information-requirement
- https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
- https://www.ftc.gov/