Maintaining Customer Privacy

Our Corporate Standard related to Encryption of Sensitive Data

Per CoreLogic Corporate Standards, the following Sensitive Data Elements must be Encrypted while In Transit and/or At Rest when combined with an individual's **last name** and **either** the individual's **first name** or the individual's **first initial**.

- National Identifier, including Social Security Number (SSN)
- Driver's License Number or Personal and/or State Identification Number
- Passport Number
- Date of Birth
- **Financial Account number** (Includes Loan Number, bank account number, credit card number, etc.)
- User and/ or ID in combination with any required security code, access code or password that would permit access to an individual's Financial Account
- Password or PIN number
- Electronic ID and access code
- Mother's Maiden Name
- Electronic or Digital Signature
- Biometrics (including fingerprints and photographs)

Personal identifiers such as the ones mentioned above are not necessarily NPI by themselves. However when the information is coupled with a first name or first initial and last name coupled with any of the following: Social Security Number, driver's license number, state-issued ID number, credit card number, debit card number, or other financial account numbers the information becomes NPI and must be protected. The amount of non-public information utilized in the Appraisal process is generally limited to loan number, borrower name and property address.

Regulatory Considerations

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act defines Nonpublic Personal Information ("NPI") as "personally identifiable financial information resulting from any transaction with the consumer or any service performed for the consumer." The Gramm-Leach-Bliley Act (GLBA) specifically requires that institutions doing business in the US establish appropriate standards for protecting the security and confidentiality of customers' NPI. The objectives are to:

- Ensure the security and confidentiality of customer records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to information which could result in substantial harm or inconvenience to any customer

Federal Trade Commission

Federal Trade Commission Safeguards Rule requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

FFIEC

The Federal Financial Institutions Examination Council (FFIEC), which is "empowered to prescribe uniform principles, standards, and report forms to promote uniformity in the supervision of financial institutions," adds that "Financial institutions should employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit."

State Data Breach Laws

All 50 states plus the District of Columbia have data breach laws in place that generally consider the above data elements to be Personally Identifiable Information (PII). These laws impose strict requirements and liabilities on companies maintaining PII if unencrypted PII is accessed by an unauthorized individual.