

1. Mortgage Acts and Practices—Privacy and Safeguard Policy and Procedures

1.1. Purpose

Montezuma Mortgage maintains this policy in order to comply with all state and federal privacy laws and regulations. At a minimum, Montezuma Mortgage complies with the following privacy laws in accordance to the Gramm-Leach Bliley Act. Montezuma Mortgage is committed to ensuring all customers private and sensitive information is handled, stored, and destroyed in compliance with GLB privacy rule and will provide training to its employees on these requirements on a frequent and regular basis. Customer information is defined as any information about a customer, whether publicly available or not.

1.2. Scope of Policy

This policy applies to any employee of Montezuma Mortgage. Failure to comply may result in immediate termination. Daniel Hennek, Compliance Officer, is designated to oversee the implementation of this policy and will work closely with the employees of Montezuma Mortgage to see that it is followed.

1.3. Privacy and Safeguard Practices

Montezuma Mortgage takes the following privacy actions:

- Perform reference or background checks before hiring employees who will have access to customer information.
- Ask new employees to sign a confidentiality and security standards for handling customer information agreement.
- Limit access to customer information to employees who have a business reason to see it.
- Store laptops, PDAs, cell phones, or other mobile devices that are used for company use in a secure place when not in use and ensure they are password protected in order to obtain access.
- Use “strong” passwords on any device that may contain Customer Information and password changes on a regular basis.
- Depositing any documents with Customer Information into shredding bins only.
- Trained employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
 - Locking rooms and file cabinets where records are kept;
 - Locking any device (computer, laptop, cellphone, etc) that is used for business purposes in the event of stepping away from it;
 - Not sharing or openly posting employee passwords in work areas;
 - Encrypting sensitive customer information when it is transmitted electronically via public networks;
 - Referring calls or other requests for customer information to designated individuals who have been trained in the safeguards of personal data; and
 - Reporting suspicious attempts to obtain customer information to a manger or to Daniel Hennek.
- Terminated employees will have their access to customer information immediately deactivated by changing their passwords and usernames to all company information

systems, programs and email accounts, as well as taking other appropriate measures.

Montezuma Mortgage abides by the following practices to protect their consumers:

- Montezuma Mortgage does not sell Customer Information.
- Montezuma Mortgage does not share Customer Information with affiliates or nonaffiliates.
- Montezuma Mortgage does not keep Customer Information that is not necessary to accomplish its business goals.
- Any request from a borrower to any Montezuma Mortgage employee, who requests to have their information removed from a call or email list, is immediately removed from said list.

In accordance with Montezuma Mortgage's Privacy Statement, Customer Information is only shared:

- For our everyday business purposes, such as to process transactions, maintain accounts, respond to court orders and legal investigations, or to report to credit bureaus.
- For our marketing purposes to offer products and services to our Customers.

1.4. Information Systems

In accordance with the Gramm-Leach Bliley Act (16 CFR Part 14), Montezuma Mortgage provides security and safeguarding throughout the life cycle of customer information, from data entry to data disposal by:

- Securing transmission of customer information:
 - When transmitting credit card information or other sensitive financial data, a secure connection is used, so that the information is protected in transit.
 - Customers are cautioned against transmitting sensitive data, such as account numbers, via email or in response to an unsolicited email or pop-up message.
 - If sensitive data is sent via email over the Internet, the data is encrypted.

In accordance with Federal Trade Commission Rule on Privacy of Consumer Financial Information (16 CFR Part 682), proper disposal of all sensitive data, including but not limited to, consumer information, credit reports, account numbers, etc., Montezuma Mortgage:

- Conducts destruction of data/documents monthly, on-site at Montezuma Mortgage and is done so by using a mechanical shredding device.
- Electronics and computers are destroyed on-site by an IT Contractor.

In the event of breach of customer information, Montezuma Mortgage will:

- notify affected customers if their personal information was subject to the breach;
- notify law enforcement if the breach could involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm;
- notify the credit bureaus and other businesses that may be affected by the breach.

**MODEL LETTER FOR THE
COMPROMISE OF SOCIAL SECURITY NUMBERS**

Dear _____:

We are contacting you about a potential problem involving identity theft.
[Describe the information compromise and how you are responding to it.]

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax	Experian	TransUnionCorp
800-685-1111	888-397-3742	800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call [insert contact information for law enforcement] and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

Take Charge: Fighting Back Against Identity Theft, a comprehensive guide from the FTC is available on the FTC's website to help you guard against and deal with identity theft.

[Insert closing]
Your Name