

Mortgage XSites

Security, GLB & Patriot Act Compliance

WE TAKE THE JOB OF PROTECTING YOUR DATA AND THAT OF YOUR CUSTOMERS VERY SERIOUSLY. WE HAVE IMPLEMENTED SYSTEMS AND POLICIES TO ENSURE THAT YOUR DATA IS SAFE AND COMPLIANT. MORTGAGE XSITES FULLY COMPLY WITH THE FTC REGULATIONS REGARDING THE GRAMM-LEACH-BLILEY ACT. THE FOLLOWING DOCUMENT DESCRIBES THE AREAS AFFECTED AND FALLING UNDER THE ACT ALONG WITH A DESCRIPTION OF HOW WE SAFEGUARD DATA AND MAINTAIN COMPLIANCE.

Protection from unauthorized access during the application entry process

Loan applications submitted by borrowers using the Mortgage XSites FlexApp 1003 are double protected by both a 128bit SSL connection on the page that loads the loan application program and by a 128bit SSL connection from the loan application program to the web services that load and save data.

Protection from unauthorized access while in our custody

Electronic access to documents is restricted to key personnel who develop and maintain the secure server environment. Monitored firewalls act as a barrier between the Internet and our secure server environment and prevent unauthorized access to any of our secure servers from outside the building.

Physical access to the data is protected in our network operations center by multiple layers of security – including armed guards. Physical access from outside the building to the general offices is secured by electronic card access and monitored by video surveillance. Anyone without a security badge is not even able to enter the general offices. Once inside the general offices, access to the network center itself is again limited by card access to key personnel who maintain the systems. Logs are kept of all access to any door. a la mode will comply with all applicable state and federal laws requiring notification in the event of a breach of personal information.

Use of loan application data by a la mode

Under no circumstances does a la mode, sell, convey, share or disseminate in any way, any data associated with your Mortgage XSite or clients' loan applications. We are in the business of providing software solutions for the real estate industry and have been a conscientious and trustworthy custodian of customer data since 1985.

As part of a la mode's process of continued enhancements and upgrades to the Mortgage XSites and FlexApp 1003 products, we monitor and compile various statistics on the habits of consumers filling out the loan application. These statistics such as which fields are left blank, most common stopping points, most common data entry formats and various other user habits, don't contain any confidential consumer information but provide us with a wealth of information we need to improve the product. In addition we reserve the right to aggregate certain data points for the purposes of measuring the level of growth of our products and tracking trends industry wide in the habits of consumers.

Protection while exporting loan applications to a loan origination system (LOS)

Mortgage XSites supports exporting loan applications to a number of popular LOS systems such as Calyx Point, Encompass, Contour, Genesis 2000, BytePro, and many others. Depending on the specific LOS, the export methods vary. For BytePro integrations an encrypted SSL connection from BytePro desktop software is made directly to our servers. For LOS systems that utilize the Fannie Mae DO/DU 3.2 format the DO/DU file is downloaded from the a la mode servers to your local computer over a secure HTTPS connection.

Protecting data from power failure and disaster

Mortgage XSites are hosted at a la mode's state of the art data center located in Oklahoma City, Oklahoma. In addition, a la mode has an office and data center in Salt Lake City, Utah. Each data center houses at least one redundant system and boasts redundant power employing uninterruptible power supplies and generators capable of supplying them with power for an indefinite period of time. In the event of a disaster affecting the physical location of the Oklahoma City data center, a la mode is capable of becoming fully functional by employing the alternate data center.

USA PATRIOT Act Compliance

Although Mortgage Brokers do not specifically or officially fall under the guidelines of the USA PATRIOT Act, upstream lenders and other financial institutions involved in the mortgage transaction do and as the origination point of the loan, the mortgage broker will be expected to assist in gathering the necessary information from consumers for upstream lenders and institutions to be compliant. Unlike other compliance requirements, there are no disclosure forms to distribute to the borrower. Rather, section 326 of the Act provides that institutions implement a customer identification program (CIP) in order to verify the identity of borrowers prior to engaging in a financial transaction. In this case, that means opening a new mortgage loan. Mortgage XSites provide mortgage brokers with the tools for implementing a CIP. Specifically, the online loan application has fields and other tools for gathering all the required information from a borrower including (name, date of birth, address and taxpayer identification number). In the event the borrower is not a U.S. resident, a passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard is required. Because of the many variances of these forms of identification, having a borrower use DirectFax to include a copy of this ID is one of the best ways to fulfill the requirements of the act.

DEFINITIONS

DirectFax

An exclusive technology of a la mode that allows borrowers to send paper based documents using any fax machine. The documents are converted to a digital PDF file and attached to the loan file automatically using a special bar coded cover page. Any hard copy document can be sent such as pay stubs, tax returns or even drivers license, passport or other official ID.

Gramm-Leach-Bliley

The Gramm-Leach Bliley (i.e., GLB) Act requires financial institutions to take steps to ensure the security and confidentiality of "customer" records such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers. The GLB Act broadly defines "financial institution" as any institution engaging in the financial activities enumerated under the Bank Holding Company Act of 1956, including "making, acquiring, brokering, or servicing loans" and "collection agency services. GLBA requires government agencies that regulate financial institutions to implement regulations to carry out the Act's financial privacy provisions. The regulations required all covered businesses to be in full compliance by July 1, 2001.

HTTPS

(Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol, developed by Netscape, built into browsers, that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is the use of Secure Socket Layer (SSL) as a sub-layer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.)

SSL

Secure Sockets Layer. Used by most commerce servers on the World Wide Web, this high-level security protocol protects the confidentiality and security of data while it is being transmitted through the internet. Based on RSA Data Security's public-key cryptography, SSL is an open protocol that has been submitted to several industry groups as the industry security standard. Denoted by the letters HTTPS in the URL.

USA PATRIOT Act

Enacted by the U.S. Congress in response to the September 11, 2001 terrorist attacks on the World Trade Centers in New York, the act enhances the authority of U.S. law enforcement for the purported intention of investigating and preempting potential terrorism.