The CFPB and Trueview Imaging's Commitment on Compliance

The Consumer Finance Protection Bureau (CFPB) has impacted title agencies and the outside vendors they work with in a number of ways. Title agencies are not directly controlled or monitored by the Dodd-Frank Act's rules, which resulted in the CFPB being created. They are, however, considered third party service providers to those banks and mortgage lenders. They must, therefore, show that their own procedures will satisfy the standards to which those banks, etc, are held. This also applies to vendors and service providers providing services to Title agencies such as Trueview Imaging.

Trueview Imaging has implemented internal policies to ensure that security, accuracy and care are implemented to manage risk and minimize damage to consumers. We monitor our processes in an ongoing effort to ensure their compliance and are ready to act should problems arise.

Personnel Screening and Background Checks

Our employees undergo thorough screening, testing and rigorous background checks. Coupled with a safe and secure work environment, we are dedicated to the protection of our client's information and never share it with any outside parties.

Physical Security

Trueview maintains all paper records in a secure locked facility with video surveillance technology monitoring. Employee only access is controlled by access keys and information is never allowed to leave our facility with the exception of secure destruction of records which happens under the supervised view of a designated employee.

Electronic Security and Encryption

Trueview stores all electronic records in a secure encrypted storage system comprised of databases and RAID 5 arrays. All access to records is controlled by a secure username and password. Information flowing from Trueview and the client is encrypted using SSL (secure socket layer) to ensure nothing is useable to a potential hacker or attack. All information maintained within the storage system is “Read Only” which further reduces the chance of accidental loss of information.

Data Backup and Redundancy

An additional backup of all data is maintained as a precautionary measure against natural disaster or other emergency situation. Data is backed up and maintained offsite in a hardened facility owned and maintained by Peak 10, a national leading co-location and data hosting provider. The data is protected 24/7 in a data center protected by armed guards. All access to the facility requires biometric entry authentication. Closed loop video surveillance cameras track every move. Uninterruptible power systems provide backup power and fire and & flood protection is also provided