ALTA Best Practices – Pillar III

As professionals in the Title industry seek to reduce cost and secure sensitive communications regarding files and messages in various forms of decentralized environments to meet new Pillar III requirements, they are running up against a clock and the lack of truly secure solutions. The risks associated with the use of current methods of protecting critical data from cyber-attack/theft and exploitation are becoming increasingly apparent and ineffective.

The information that is disseminated requires effective yet flexible high-security solutions capable of supporting authorized control over this critical information while protecting that information regardless of its location as well as service provider from internal and external loss and exploitation.

Common Mortgage Settlement Documents Containing sensitive forms of information:

 Uniform Residential Loan Application (Form 1003) Borrower Tax Returns Payoff Letter

 Lender Engagement Letter Settlement Statement or Disclosure Forms Identification

 IRS Form 4506-T, Request for Transcript of Tax Returns

 IRS Form W-9, Request for Taxpayer Identification Number and Certification

Common Title Documents Containing sensitive forms of information:

 Identification (Driver's license, passport, etc.) Title Order Form Payoff Letter Recordable Documents

 Escrow Agreements with Tax Searches Real Estate Transfer Tax Forms Affidavits Title Bill

What are you doing to protect your data?

It is believed that more than 20% of documents transmitted between various channels are not using any form of protection whatsoever. In other words, standard email is being utilized as transportation medium, placing this sensitive and personal information at risk while in transit to others as well as while it at rest. This includes but is not limited to personal computers in addition to mobile devices. I think we all agree that this is not a best practice nor is it an acceptable practice any longer.

Some have instituted the use of "Encrypted" email systems, which in most cases adds a layer of protection for the "Data in transit", which is not fool proof by any means, but certainly an improvement over no security at all. This method, again in most cases, does little to nothing to protect "Data at rest", or sitting on a device. With that in mind one should question whether or not that should be considered to be a "Best Practice".

There are easily implementable solutions in the marketplace that allow for the protection of data while in transit, at rest, while archived, to be protected. If the cost is nearly the same why would you use anything but the best to ensure your firm's reputation and your client's data? By putting forth a little extra effort and by taking a proactive approach to the challenge you can protect all forms of sensitive information. Many firms are just one breach away from being driven out of business. How is your firm protected? Are you confident that your firm is not at risk? What have you done to ensure your firm's data security?

Contact **Secure Cloud Systems** or visit **www.certainsafe.com** for more information.