Revisiting the Protection of Non-public Personal Information

Greg Henshaw, Title Counsel - Triad

As we quickly move into 2015 and prepare for all of the changes that will be occurring in the areas of real property law and loan closings, it may be helpful to take another look at one of the important pillars in the ALTA Best Practices, the protection of Non-public Personal Information. Many of you have already performed a self-audit of your law practice to see what areas of Best Practice compliance need some work. Protecting your clients' personal information is clearly one of the more challenging pillars of the Best Practices, and one that lenders will certainly be stressing.

What is Non-public Personal Information (NPI or NPPI)? NPI is defined as "Personally identifiable data such as information provided by a customer on a form or application, information about a customer's transactions, or any other information about a customer which is otherwise unavailable to the general public. NPI includes 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." Due to the size of closing packages and the multitude of other information provided to closing attorneys by lending institutions, it is clear that closing attorneys have access to large amounts of NPI related to their clients.

As with several of the other pillars in the Best Practices, the Best Practice regarding protection of NPI also has a requirement that the closing attorney develop and maintain **written** procedures regarding the implementation of the protections, in this case the adoption and maintenance of a privacy and information security program. ALTA has created a document entitled "Best Practices Policy and Procedure Creation Guidance" to assist closing attorneys in the creation of these written controls.

The ALTA Best Practice regarding protection of NPI reads as follows:

Best Practice No. 3: Adopt and maintain a written privacy and information security program to protect Non-public Personal Information as required by local, state and federal law.

Purpose: Federal and state laws (including the Gramm-Leach-Bliley Act) require title companies to develop a written information security program that describes the procedures they employ to protect Non-public Personal Information. The program must be appropriate to the Company's size and complexity, the nature and scope of the Company's activities, and the sensitivity of the customer information the Company handles. A Company evaluates and adjusts its program in light of relevant circumstances, including changes in the Company's business or operations, or the results of security testing and monitoring.

This Best Practice has several sections related to specific procedures that must be considered when creating a privacy and information security program for your firm or office. These procedures must be met in order to be in compliance with this Best Practice.

- Physical security of Non-public Personal Information

- Restrict access to Non-public Personal Information to authorized employees who have undergone Background Checks at hiring.

- Prohibit or control the use of removable media.

- Use only secure delivery methods when transmitting Non-public Personal Information.

In order to be in compliance with this first procedure, it will be necessary for a closing attorney to control the availability of NPI to third parties. We are all aware of the need to keep information such as the Social Security numbers and financial information of clients protected, but NPI is much more than that. Prior to the recordation of a deed or Deed of Trust, the information contained in these documents may be seen as NPI. This may extend to all information in a closing package, including applications, TIL statements and HUD-1 statements. In order to protect this information, the attorney must develop procedures including "clean desk" policies, limitations on the ability of certain employees to view client documents or limitations on copying, faxing or e-mail duties. There will also need to be controls put in place for technology. Computer screens will need to be set up so that they are not visible to the public and will need to "time out" after a certain period of time. The encryption of NPI delivered by a closing attorney must be considered as well. Other delivery methods, such as texting, e-mailing or faxing, must also be reviewed from a security standpoint.

- Network security of Non-public Personal Information.

- Maintain and secure access to Company information technology.

- Develop guidelines for the appropriate use of Company information technology.

- Ensure secure collection and transmission of Non-public Personal Information.

This procedure will obviously be impacted by the size of a firm or office. Smaller firms or solo practitioners may not have their offices on a computer network and may simply use stand alone stations. Regardless, procedures will need to be set up to secure all information technology. Issues to consider will include proper password development and use, protection of NPI from the risk of malware or other hacking concerns and, again, encryption of NPI to be transmitted.

.

- Disposal of Non-public Personal Information.

- Federal law requires companies that possess Non-public Personal Information for a business purpose to dispose of such information properly in a manner that protects against unauthorized access to or use of the information.

Although most closing attorneys have already switched to shredding or other document disposal, whether in-house for small firms or solo practitioners, or through a vendor for larger firms, such disposal will now be a necessity. Many vendors already exist that can perform on-site shredding and other document removal/disposal services. The days of news reporters finding boxes and boxes of old client files beside the back dumpster have hopefully passed.

- Establish a disaster management plan.

Again, this is a procedure than many closing attorneys already have in place. The written portion of a disaster management plan may be more detailed and time consuming to create and maintain, so plan accordingly.

- Appropriate management and training of employees to help ensure compliance with Company's information security program.

Because the terms and final versions of the Best Practice procedures may change over time, it will be important to keep the attorney's staff up to date on the requirements and expectations to protect client NPI. This may include periodic staff meetings and written handbooks for each staff member.

- Oversight of service providers to help ensure compliance with a Company's information security program.

- Companies should take reasonable steps to select and retain service providers that are capable of appropriately safeguarding Non-public Personal Information.

As mentioned above, there are numerous service providers/vendors available to assist with implementing your NPI protection procedures, including those for document disposal and network/computer security. Many of these providers are familiar with the Best Practices requirements, and will be marketing their services to closing attorneys. Be sure that any providers that you work with have knowledge of the practices necessary to become or remain in compliance with the Best Practices.

- Audit and oversight procedures to help ensure compliance with Company's information security Program.

- Companies should review their privacy and information security procedures to detect the potential for improper disclosure of confidential information.

It has not been determined at this time how often assessments of an attorney's compliance with the ALTA Best Practices will be required (every one year, two years, etc.). Regardless of the period ultimately chosen, it will be important to review and maintain effective procedures so that the attorney can make necessary changes prior to an assessment. Internal audits and oversight procedures should play an important role in becoming and remaining in compliance. Changes in staff, including attorneys and non-attorneys, changes to office space (leading to NPI accessibility changes) and changes in business models should all be considered during internal audits.

- Notification of security breaches to customers and law enforcement.

- Companies should post the privacy and information security program on their websites or provide program information directly to customers in another usable form. When a breach is detected, the Company should have a program to inform customers and law enforcement as required by law.

This final procedure again presents the importance of a clear and concise written privacy and information security program. These programs will need to be available on the Company website or distributed otherwise, such as in an attachment to an initial engagement letter to a client. As we have seen recently with the breaches of confidential consumer information with some of the retail giants, it appears that there are many different "plans" to handle such breaches. It will be necessary to not only have a means to inform clients of a breach, but also to determine a proper time frame for disclosure. A review of state and federal law may also be prudent to determine the legal requirements for disclosure.

Although many closing attorneys have already created and implemented procedures for protecting the NPI of their clients, others are still in the process of doing so. This process, as discussed above, can be both time consuming and potentially costly, so it is important to develop a good understanding of the required procedures and the impact that becoming compliant may have on your practice. Please contact your local Attorneys Title office with any questions, or visit www.AttorneysTitle.com and click on the tab labeled "Best Practices" for the latest information and tips.