ILTA Manager Meeting
State Historical Building
February 9, 2015

Protecting Non-Public Personal Information

This information is not a substitute for legal advice, is for your reference only, and is not intended to represent the only approach to any particular issue. This information should not be construed as legal, financial or business advice, and users should consult legal counsel and subject-matter experts to be sure that the policies adopted and implemented meet the requirements unique to your company.

American Land Title Association® (ALTA®)
1800 M St NW, Suite 300 South
Washington, DC 20036
Phone: 202-296-3671
E-Mail: service@alta.org
Web: http://www.alta.org

ALTA Best Practices Framework:

The ALTA Best Practices Framework has been developed to assist lenders in satisfying their responsibility to manage third party vendors.

SEVEN PILLARS:

1. Establish and maintain current License(s) as required to conduct the business of title insurance and settlement services.
2. Adopt and maintain appropriate written procedures and controls for Escrow Trust Accounts allowing for electronic verification of reconciliation.
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.**
4. Adopt standard real estate settlement procedures and policies that help ensure compliance with Federal and State Consumer Financial Laws as applicable to the Settlement process.
5. Adopt and maintain written procedures related to title policy production, delivery, reporting and premium remittance.
6. Maintain appropriate professional liability insurance and fidelity coverage.
7. Adopt and maintain written procedures for resolving consumer complaints.

ALTA Best Practice: 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.

ALTA Definition of NPPI:

Non-public Personal Information: 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.

I've heard a lot about the ALTA Best Practices so….

- If I don't do closings, why should I care about the CFPB and ALTA Best Practices?
- Doesn't the ALTA provide the necessary resources for compliance?
- What is important from the CFPB and August 1, 2015?*

*It is the effective date for the new TILA-RESPA rule and includes two new disclosure forms to be part of the closing process: Loan Estimate (replaces Good Faith Estimate) and the Closing Disclosure (replaces the Settlement Statement). And, implementation of the three-day rule that consumers must receive a final Closing Disclosure three days before the closing date.

Iowa Title Guaranty and Best Practices:

- Steps Taken
- e-Faxing
- Requirements of Members
- Timeframe for Implementation
- Training

Procedures to meet ALTA Best Practice 3 - Create Checklist and Table of Contents:

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

    (One resource: www.IowaCriminalHistory.iowa.gov)
  - Prohibit or control the use of removable media.
  - Use only secure delivery methods when transmitting Non-public Personal Information.
- 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.
- 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.
- Establish a disaster management plan.

Procedures to meet Best Practice 3 - create a Checklist and Table of Contents (cont):

- Appropriate management and training of employees to help ensure compliance with Company's information security program.
- 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.
- 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.
- 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 useable form. When a breach is detected, the Company should have a program to inform customers and law enforcement as required by law.

ALTA Best Practices Framework: Assessment Procedures

******* ******* *	**ALTA Best Practice 3.** **Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information as required by local, state and federal law.**	***Overall Assessment Recap: If any individual procedure marked with an asterisk FAILS, Best Practice 3 FAILS.***
3.01*	Obtain the Company's information security program/policy to protect its Non-public Personal Information and verify that the program/policy is reviewed and updated at least annually, as necessary.	PASS / FAIL If no written procedures, Procedure 3.01 FAILS.
3.02*	Select a sample of 25 employees who have access to Non-public Personal Information (or 100% if fewer than 25 employees). Obtain evidence that they were trained in the Company's information security program/policy to protect Non-public Personal Information.	PASS / FAIL If 20% or more of items tested FAIL, Procedure 3.02 FAILS
3.03*	Obtain the Information Security Risk Assessment, including the risk ranking of information systems. Review the Company's process for assessing risk to its customer information and verify that it includes the following: a. Locations, systems, and methods for storing, processing, transmitting, and disposing of its customer information. b. Potential internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of Non-public Personal Information or customer information systems and assessments of the likelihood and potential damage to the Company and its customers of these threats.	PASS / FAIL If no written Information Security Risk Assessment, Procedure 3.03 FAILS.

ALTA Best Practice 3.
Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information

3.04*	Verify that key controls, systems and procedures of the information security program are regularly tested by qualified independent staff in accordance with the risk assessment. Specifically, review that the following are included in the testing: a. Management's documented approach for testing the information security program and evidence of testing. b. Frequency of testing of the information security program. c. Documentation of approach for tracking and remediating exceptions and/or control gaps.	PASS / FAIL
3.05*	Verify employees are required to complete an acceptable use of information technology assets agreement at least annually (e.g., acceptable use of the Internet, email, and Company information resources). For the sample of employees tested in Assessment Procedure 3.02 above, review the signed Acceptable Use Policy.	PASS / FAIL If 20% or more of items tested FAIL, Procedure 3.05 FAILS
3.06*	Obtain and review written policies and procedures to verify logical access to information systems (i.e., network, data base, and application layers) containing Non-public Personal Information is restricted to authorized persons only.	PASS / FAIL If no written procedures, Procedure 3.06 FAILS.

ALTA Best Practice 3.
Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information

3.07 *	a. For the sample of employees tested in Assessment Procedure 3.02 above, test the user access provisioning process to determine if access is approved in accordance with policy prior to granting. o Obtain evidence (invoice/documentation in personnel files, etc.) that 5 year Background Checks were conducted upon hiring or within the past 3 years. b. Select a sample of 5 terminated employees or 100% if less than 5 within the assessment period. o Verify the user access de-provisioning process to determine if access for terminated employees was removed per policy. c. Verify administrative access rights (i.e., ability to add, modify and remove user access) to systems containing Non-public Personal Information are not assigned to personnel performing business transactions within the system. d. Verify access review is being performed by management at least annually to confirm that only required employees have access to customer information or customer information systems necessary to perform job functions. e. Verify that logical access controls (e.g., unique User ID's, **complex passwords,** etc.) to the network and information systems containing Non-public Personal Information are in place. o Obtain listing of user ID's for systems with Non-public Personal Information. Verify ID's are unique and assigned to specific users. o Test password configuration controls in accordance with policy.	If 20% of sub-procedures 3.07.a or 3.07.b FAIL, the sub-procedure FAILS If sub-procedure 3.07.c, 3.07.d, or 3.07.e FAIL, the applicable sub-procedure FAILS <u>Overall</u> If any individual sub-procedure FAILS, Procedure 3.07 FAILS

ALTA Best Practice 3.
Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information

3.08*	a. Review documented policies regarding the use of removable media (e.g., restricting the use of USB ports, CD/DVD writable drives, etc.). b. Obtain evidence of system configuration settings demonstrating the restriction of removable media in accordance to policy.	PASS / FAIL If sub-procedure 3.08.b FAILS, Procedure 3.08 FAILS. If sub-procedure 3.08.a FAILS, but 3.08.b PASSES, then Procedure 3.08 PASSES.

ALTA Best Practice 3.
Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information

3.09*	Inquire of management to determine if the Company: a. Provides encryption of electronically transmitted Non-public Personal Information. b. Can provide evidence of system configuration settings demonstrating the use of encryption.	PASS / FAIL If sub-procedure 3.09.b FAILS, Procedure 3.09 FAILS. If 3.09.a FAILS, but 3.09.b PASSES, then Procedure 3.09 PASSES
3.10*	a. Obtain and review documented procedures for monitoring, detecting attacks/intrusions into customer information systems, and responding to incidences. If monitoring of external threats has been outsourced, obtain evidence of reporting and subsequent management review. b. Obtain a sample of 5 or 10%, whichever is greater, of notifications of security alerts (maximum of 25) and verify management's follow-up activity. c. Obtain and review documented procedures for security breach notification, including evidence of program review at least annually.	PASS / FAIL If no written procedures, Procedure 3.10 FAILS. If any individual sub-procedure FAILS, Procedure 3.10 FAILS.

ALTA Best Practice 3.
Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information

3.11*	a. Verify access to physical locations containing customer information, such as buildings, computer facilities and record storage facilities, is limited to authorized personnel only. Inspect physical locations to verify that they are secured and access is limited to authorized personnel. a. Obtain and review the Clean Desk Policy and verify compliance through inspection.	PASS / FAIL If any individual sub-procedure FAILS, Procedure 3.11 FAILS.
3.12*	a. Obtain and review change management procedures when technology and business function changes are made. b. Verify procedures are in place to determine that systems modifications (hardware and software) are consistent with the approved security program. Specifically, test a sample of 5 or 10%, whichever is greater (maximum 25) of hardware or software changes to verify that they are documented, tested and approved.	PASS / FAIL If sub-procedure 3.12.b FAILS, Procedure 3.12 FAILS. If sub-procedure 3.12.a FAILS, but 3.12.b PASSES, then Procedure 3.12 PASSES

ALTA Best Practice 3.
Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information

3.13*	Obtain management's procedure for data and system backup and business resumption to protect against destruction, loss, or damage of information from potential environmental hazards, such as fire and water damage or technological failures.	PASS / FAIL
3.14*	Determine whether the Company provides Non-public Personal Information to any other party or whether any other party has access to Non-public Personal Information through service provided directly to the Company. a. Verify and obtain evidence that Company conducted due diligence in selecting its service providers and taking information security into consideration. b. Verify that Company has controls to monitor security procedures of service providers to safeguard customer information (i.e. review the results of audits, security reviews or tests, intrusion logs, or other evaluations).	PASS / FAIL If any individual sub-procedure FAILS, Procedure 3.14 FAILS.

ALTA Best Practice 3.
Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information

3.15*	Verify whether Company provides **Privacy Policy to customers**. Obtain and inspect evidence of notification using the same sample as in Assessment Procedure 2.06 above.	PASS / FAIL If 20% or more of items tested FAIL, Procedure 3.15 FAILS
3.16*	Determine through inquiry of management whether the Company maintains a website. If so, inspect the Company's website and verify the following: a. The **website includes a privacy statement.** b. The website's privacy statement accurately discloses what Non-public Personal Information is obtained on the site.	PASS / FAIL If any individual sub-procedure FAILS, Procedure 3.16 FAILS.
3.17*	a. Obtain and inspect policies and procedures over **record retention and disposal.** Verify procedures are in place for disposal of Non-public Personal Information. a. If document/electronic media disposal services are provided by a third party, obtain evidence of the contract agreement/SLA and a recent document disposal certificate from the vendor.	PASS / FAIL If any individual sub-procedure FAILS, Procedure 3.17 FAILS.

- **Identify Your Risks**

- **Create Policies and Procedures Notebook:**
  PUT IT IN WRITING!

- **Create Your Own Business Domain Email Account and Address**

- **Train Your Employees**

- **Open Discussion and Q&A**
  Where do we go from here?

PANELISTS:

- Gary Reeder, ILTA Board President, Delaware County Abstract Co., Manchester
- Mike McLain, ILTA President-Elect, Abstract & Title Co., Mount Ayr
- Arlene Drennan, ILTA SW Regional VP, Cass County Abstract Co., Atlantic
- Gerald LoRang, ILTA Board Member, Iowa Title Guaranty, Des Moines