WFG National Title Insurance Company
a Williston Financial Group company

UNDERWRITING BULLETIN

To: **All Florida Agents of WFG National Title Insurance Company**

From: **WFG Florida Underwriting Department**

Date: **June 27, 2014**

Bulletin No.: **FL 2014-13**

Re: **Legislative Update 2014 - SB 1524 Data and Information Security**

Title agents and attorney-agents have always been sensitive to their duties to protect confidential customer and client information. Our attention to this important responsibility has recently been heightened by ALTA's Best Practices initiative and some highly publicized (and very expensive) data breaches at major retailers.

This year, the Florida legislature decided to codify some of these duties in SB 1524, which unanimously passed in both the House and Senate. **This Bill** was signed into law by Governor Scott on June 20, 2014 (Laws of Florida 2014-189).

Overview of the Law:

The Bill introduces three affirmative duties that are binding on all Florida businesses and government entities (and arguably non-Florida based businesses which hold personal information about Florida residents).

1. To take "reasonable measures" to protect and secure data in electronic form which contains personal information. New §501.171(2)
2. To take "reasonable measures" in the disposal of customer records (paper and electronic) containing personal information when the records are no longer to be retained. The Bill clarifies that will involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable. New §501.171(8)
3. To report any unauthorized access to electronic data which includes customer "personal information" (a "breach") to the Florida Department of Legal Affairs and to the affected individuals. New §§501.171(3) and (4)

If you have contracted out management or storage of personal information (such as to a closing software vendor "in the cloud"), that third-party agent is under a duty to notify you (the "covered entity") within 10 days of a breach or suspected breach – and then you must give the required notices. New §501.171(6). Since not all third-party vendors will be aware of the duties imposed under Florida law, we recommend documenting that you have put them on notice and build the duty into any contract renewal agreements.

What Information is Covered?

The defined term "personal information" is what is to be required to be protected under this bill. That definition is a little different than the interpretations previously given under the Gramm, Leach, Bliley Act and other Federal interpretations. For purposes of this bill, protected "personal information" includes:

- an individual's first name or first initial and last name TOGETHER WITH:
    - A social security number;
    - A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
    - A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
    - Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
    - An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

  or

- A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

The term "Personal Information" does not include information that has been made publicly available by a federal, state, or local governmental entity. So information we gather in our title searches, even if they include one or more of these elements (such as an un-redacted SSN, or Drivers License or Passport Number in the Notary acknowledgement) do not require enhanced protection (we should anyway) or trigger notification duties.

For our purposes, we should assume any information that falls within this definition and anything traditionally covered by Gramm, Leach Bliley (and if you are an Attorney-agent, the much broader category of information that is subject to client confidentiality), should be protected by your processes and procedures (something else to tweak in developing your Best Practices manual). If you suffer a breach, it would be advisable to discuss the exact information disclosed with your legal counsel as you evaluate your duties and legal exposure.

What is Required if I Suffer a Data Breach?

If you suffer a breach of your electronic data (no reporting is required for a breach of paper data, but if it happens by all means discuss it with your legal counsel, as there are significant liability issues), and the breach affects 500 or more individuals, you must give notice to the Florida Department of Legal Affairs as "expeditiously as practicable" but no later than 30 days after you discover the breach or have reason to believe a breach has occurred.

The bill includes a list of information that must be reported, including the policies you have in place regarding breaches of security. (1)

We recommend reviewing any policies and procedures you are implementing as part of adopting ALTA Best Practices. Those policies and procedures should be modified to conform both with Best Practices and the requirements of this Bill, and should include immediate notification of your legal counsel.

Regardless of the number of individuals impacted by a breach of electronic data, you must give notice to the affected individuals as "expeditiously as practicable," but in any event within 30 days of discovery or having reason to believe a breach occurred. Law enforcement may delay this if giving notice would interfere with criminal investigation. The notice may be given by mail or email, and must include specific information.

If the number of affected individuals is very large (over 500,000 people), notice would be too costly (over $250,000), or you don't have mailing addresses or email addresses; the bill provides an alternative involving notices on your website and in print and broadcast media where the affected individuals reside. It is not clear whether this requires paid advertising, or just notice to the media outlets.

In the event of a breach affecting over 1,000 people, you must also give notice to all credit reporting agencies.

The one exception to the notice requirement is that you are not required to give notice if, after consultation with "relevant federal, state or local law enforcement agencies" your office "reasonably determines" that the breach is not likely to result in identity theft or other financial harm to the individuals. Which law enforcement agencies are considered "relevant" is unfortunately not specified.

The "no harm" determination must be documented in writing and preserved for at least 5 years (which conveniently is the longest of the potentially applicable statute of limitations period). If you make a "no harm" determination, that determination must be reported to the Department of Legal Affairs within 30 days. Wrongly determining that you fall within the "no harm" exception can nonetheless subject you to penalties, so discuss this with your legal counsel.

Any "Personal Information" and much of the other information that may come into possession of the Department of Legal Affairs pursuant to this bill is expressly exempt from public records disclosure, even after the completion of any investigation, by companion bill SB 1526.

Duties of Third-Party Data Agents

Many of our agents use closing software that captures all of the relevant information, and scans in the entire loan package, closing statements, recorded instruments and the like. Some of those software packages operate "in the cloud" or store backups of information remotely. This bill imposes an obligation on those "Third-Party Agents" to notify their customer (the agency, attorney-agent or other covered entity) of any breach within 10 days of discovery or reason to believe a breach has occurred. The duty then shifts to the customer to provide the notices required by this law.

Penalties for Violation

A violation of this bill will be treated as an Unfair and Deceptive Trade Practice under chapter 501 of Florida Statutes. In addition to other penalties under chapter 501, if you fail to give notice timely, an additional civil penalty may be imposed of up to $1,000 per day for the first 30 days, and $50,000 for each subsequent 30 day period for up to 180 days, with a maximum fine of $500,000. The penalty is per data breach, not per individual affected.

This is a very serious fine, so it needs to be taken quite seriously. These penalties are only to be assessed by the government entity. The bill does not create any private cause of action for its violation – although damages may be sought by your customers for the underlying breach.

This law will take effect July 1, 2014.

Our Recommendations:

This bill imposes serious penalties – but it is also the right thing. As you review this bill, we recommend you consider:

1. **Adjust Your Best Practices Manual**. Because the definition of protected "Personal Information" differs slightly from the definitions used in Gramm, Leach, Bliley and in the ALTA materials, adjust your Best Practices materials so they clearly apply to both. The policies and procedures for responding to any data breach (even paper ones) should include immediate consultation with your lawyer and provide the notifications set forth in this Bill.

2. **Train your Staff**. It goes without saying that even the best drawn policies and procedures won't do the job if the staff doesn't follow them, or doesn't fully understand them.

3. **Look seriously at Cyber Insurance.** The liabilities for data breaches and under this bill are serious; potentially bankrupting. We encourage all of our agents to give serious consideration to Cyber Insurance. In evaluating Cyber Insurance policies, pay special attention to (a) whether the policy covers governmentally imposed penalties; (b) the costs of providing notifications and credit protection services to potentially affected individuals; (c) any policy exclusions for un-encrypted data; and (d) a large enough limit to provide meaningful protection if the worst happens.

4. **Data Service Providers.**

a. Make certain that you understand the security protocols being used by your data service providers/closing software systems, and how those fit into your own Cyber-insurance coverages. Ask your insurance agent to confirm that the cyber-insurance coverage protects you from a breach of your closing software "in the cloud."
b. Ask your closing software companies to include indemnifications as to Data Breaches on their end in your subscription agreements.
c. Put them on written notice of the duty under Florida law to notify you of any breaches within 10 days of discovery. Some data service providers are not Florida-based and may miss the requirements this law will place on them and their Florida customers.

5. **Encrypt Everything!** Emails, data storage, data on your laptops, data on your cellphone and tablets, your data in the cloud (DropBox, Google Docs, etc).

6. **Upgrade your Windows XP Computers.** Last month, Microsoft stopped their support for Windows XP, and already a security issue has been identified with versions of Internet Explorer used on XP. If you don't have a currently supported version of Windows, you won't get updates for this and future security issues, leaving you unprotected.

Data security is and will continue to be an evolving issue. Hackers are getting better, and because we hold significant funds, we are a target. So please exercise great care in protecting your interests and those of your customers and clients.

[1] WFG's attorney-agents are naturally concerned whether a statutory duty to report may conflict with their overarching duty to protect the confidentiality of their client. Under any but the most obscure fact patterns, we believe the limited information to be reported does not disclose any client confidential information. The information to be reported includes only:

- How the breach happened.
- How many clients or other individuals were potentially affected by the breach (there is no requirement to specifically identify them).

- What services are being offered to remediate harm from the breach, and how they would take advantage of those services.
- A copy of the notice you will be sending to the affected clients or persons and an explanation of how you are giving notice.
- The contact information for the firm member who can be contacted for more information.

Obviously, if your fact pattern or subsequent information requested by the Department implicates client confidences, the matters should be discussed with the Florida Bar.

Phone: (949) 266-3774 | Web: www.wfgnationaltitle.com | Email: afields@wfgnationaltitle.com