Whatcha Gonna Do

Description

Whatcha Gonna Do, Whatcha Gonna Do, Whatcha Gonna Do When a Data Breach Happens to You?

In my job, I have the privilege of speaking with title and settlement agents from across the nation. At some point during our conversations, those agents who have just been certified as compliant with ALTAâ??s Best Practices will usually voice something similar to the following:

> â??*I recently upgraded my server, and each of my office computers, to install new firewalls and anti-malware programs in an effort to achieve a higher level of secure software. All are encrypted with complex passwords which are changed every 60 days. Whenever I send a fax or email, I use encryption. I have installed new locks and familiarized my employees with newly established policies and procedures to prevent unauthorized access to my clientsâ?? personal information. Isnâ??t that enough to prevent a breach?â?•*

VLTA Examiner

The short answer is, â??No, all the steps you have taken are, at best, designed to *minimize the potential* for a breach, but there is nothing that you can do to *prevent* a breach.â?•

The steps you take in complying with the ALTA Best Practices Framework all are professionally *responsible* steps, but in todayâ??s world, those actions are just the *minimally required* steps to take when handling the data of other parties. While you might have spent â??a great deal of moneyâ?• and devoted a â??substantial amount of time and effort*â?*• in implementing adequate security controls, those costs and efforts may pale in comparison to those of other companies that ultimately have found themselves subject to a data breach. For example, the Federal Governmentâ??s Office of Personnel Management, which handles millions of federal applicantsâ?? sensitive information, recently announced that it was hacked, and background investigation databases affecting 21.5 million individuals were stolen. Even those who provide direct supervision of title agents are not immune â?? see the June 10, 2016, breach notification issued by the Virginia State Corporation Commission (providing oversight to insurance companies and agents) in which it acknowledged that access to â??names and social security or driverâ??s license information of these former [insurance] licenseesâ?• had been improperly accessed by one of its contractors.

When you consider the financial resources and time that federal and state agencies have invested in data security and realize that such efforts were not sufficient to prevent a breach, you must acknowledge that your efforts are far less stringent and leave your company far more vulnerable to even the most unsophisticated hacking attempts. Because of the data-intensive business in which you work, and the amount of money you handle daily, there is a real probability that over the next 5-10 years, your data will be hacked as a result of a security breach.

This blog is designed to assist you in planning for a potential data breach. Identifying your legal post-breach obligations and the reputational and financial losses you will likely sustain may reinforce the necessity of continued daily vigilance to ensure the steps you have put in place are meticulously followed.

Before going further, I make a disclaimer that I am not providing legal advice, nor do I purport to act as a data-breach expert. I simply am trying to provide you, as a title professional, with some resources regarding issues you immediately must address if a breach has occurred. Hopefully by providing you with a link to recent webinars, and some articles and materials published by those who have significant experience in this area, you can better fashion a game plan to contend with any future security breaches.

An extremely helpful resource is an April 13, 2016, webinar produced by ALTA, â??Life Cycle of a Data Breach: Know What You Need to Do.â?• In the webinar, Matthew Froning, of Security Compliance Associates, and Christopher Gulotta, with Real Estate Data Shield, provide a concise description of the statutes, regulations, and regulatory guidance letters which describe your obligation to protect your customersâ?? non-public personal information (NPI). But more importantly, they document a clear trend in data breach law. They discuss the passage of new state legislation, and recent amendments to currently existing legislation, that reveal that your obligations in the event of a breach are increasing every year. The breach notification time frames are becoming smaller, requirements to utilize specific forms and processes are increasing, and long-standing safe harbor exemptions are disappearing. Froning and Gulotta provide clear, practical tips for developing your data breach incident response plan and recommendations for the types of companies you should hire to ensure your post-breach obligations are satisfied. After watching this webinar, you should conclude that your best strategy is to have high-level security and NPI-protection procedures in place to direct the hackersâ?? attention elsewhere, but understand that you will remain vulnerable to a security breach. Just as in the event of a fire, knowing where the exits are located can save your life. In the event of a data breach, which is probably more likely than a fire, you must have a response plan in place ahead of the breach, along with the phone numbers of those companies with the skills necessary to implement that plan. You simply do not have the luxury of investigating what you need to do after the breach occurs.

VLTA Examiner

The advice given by Gulotta and Froning is reaffirmed in another helpful article entitled, â??Data Breach Experts Share the Most Important Next Step You Should Take After a Data Breach in 2014 â?? 2015 & Beyond,â?• updated as of May 18, 2016. This article provides insight from 30 different data security experts who were asked the same question, â??What is the first step you need to take in the event a breach occurs?â?• Each expert consistently advises you to react immediately by taking a set of steps as required under applicable state and federal regulations. Unfortunately, the â??applicableâ?• law or regulation will depend on where you are located and the location of the individuals who have been affected by the data breach. Most title companies deal with customers who are located in states other than those of their offices, compelling them to comply with not only the requirements of their state, but also with those in states where their customers live. As the following segments of this article reflect, this could mean you have to comply with the obligations of dozens of different states. But first, letâ??s discuss what *triggers* your need to notify *anyone*.

What constitutes a â??breach?â?•

If someone breaks through a locked office door and steals a server or a stack of closing files, most would agree such an event probably would meet the definition of a data breach, when non-public personal information (NPI) is accessed via fraudulent means. However, has a breach occurred if you lose a phone or laptop? As you might imagine, these latter two events happen far more often than the â??break-in-and-stealâ?• events. Does the law require you to issue a data breach notification when you misplace your phone or laptop? Does it make any difference if the phone required a passcode or if the laptop was encrypted?

Frustratingly, â??it depends.â?• Thatâ??s because your obligations are almost never governed solely by the law of a single state. In many cases, your obligations also may be determined by various federal laws. Your ultimate obligations only can be determined after a careful appraisal of (1) the laws in the state where you reside, (2) the laws in the states where each of your affected customers live, and (3) depending on your type of business, the federal laws and regulations such as those imposed by the Gramm-Leach-Bliley Act (GLBA) and regulated by the Consumer Financial Protection Bureau (CFPB) and Federal Trade Commission (FTC).

Remarkably, the same event (lost phone/laptop, hacking attempt, etc.) may be deemed a data breach in some states, but not in others. Therefore, knowing which law applies is a critical first step in determining your obligations, as one type of event can result in different obligations depending on the state in which it occurred.

VLTA Examiner

***Which* state laws may apply?**

In 2014, the Clausen Miller, PC, law firm compiled a list of individual state data breach laws. Another law firm, Baker Hostetler, also has published a state-by-state data breach law listing in a slightly different format. These online compilations can be excellent resources, *but care must be taken to verify the cited statutes have not been recently modified*. These resources provide valuable insight into state-mandated procedures and customer notification obligations that can be imposed in the event of an NPI-related incident.

As you assess these state law compilations, you will find that most states have specific, and often similar, definitions of what constitutes a data breach. A recent article indicated that until recently, 41 states agreed that the loss or unauthorized access of a device containing encrypted data would not constitute a data breach, and therefore no customer notifications would be required. This commonly is referred to as an â??encrypted data safe harborâ?• statute. Virginia has adopted a similar position in Â§ 18.2-186.6 â?? â??Breach of personal information notificationâ?• which states:

1. *As used in this section:*

â??Breach of the security of the systemâ?• means the unauthorized access and acquisition of ***unencrypted and unredacted computerized data*** [emphasis added] *that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth.*

[But note, Â§ 18.2-186.6 (C) provides that if the data breach thief also acquires the encryption key, the mere fact that you had originally encrypted your data will not give you a pass from notification

obligations.

As a result, in Virginia and many other states, there is widespread consensus that encryption of your devices is the best available preventive tool, and implementing that process should be sufficient to eliminate the need for customer notification obligations.

Virginia Attorney General updates breach notification guidelines

Virginia title and settlement agents should carefully read the entirety of Virginia Code Â§ 18.2-186.6 for specific obligations in the event of a data breach. However, the Virginia Attorney General recently provided a summary of your obligations in a notice effective July 1, 2017 which is reprinted below:

DATABASE BREACH NOTIFICATION REQUIREMENTS UPDATED JULY 1, 2017

Section 18.2-186.6 of the Code of Virginia, which became effective on July 1, 2008, requires an individual or entity that owns, maintains, or possesses personal identifying information of Virginia residents who has a reasonable belief that such personal information was accessed or acquired by an unauthorized individual or entity to report the unauthorized breach to the Office of the Virginia Attorney General and to provide notification to each affected Virginia resident.

VLTA Examiner

As part of the notification, the Virginia Attorney Generalâ??s Office requests the following information from the individual or entity making the notification:

1. *A cover letter on official letterhead to the Virginia Attorney Generalâ??s Office as notification of the breach;*
2. *Approximate date of the incident to include how the breach was discovered;*
3. *Cause of breach;*
4. *Number of Virginia residents affected by the breach;*
5. *The steps taken to remedy the breach; and*
6. *A sample of the notification made to the affected parties, to include any possible offers of free credit monitoring.*

The requirements for notification to affected Virginians are listed in section 18.2-186.6 and include:

7. *The incident in general terms;*
8. *The type of personal information that was subject to the unauthorized access and acquisition;*
9. *The general acts of the individual or entity to protect the personal information from further unauthorized access;*
10. *A telephone number that the person may call for further information and assistance, if one exists; and*
11. *Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.*

***UPDATE:** As of July 1, 2017, any employer or payroll service provider who experiences a breach of an employeeâ??s tax identification number and income tax withheld for that employee must notify the Attorney Generalâ??s Office without unreasonable delay and provide the name and federal employer identification number (FEIN) of the employer suffering the breach.*

Please address all notifications to the Attorney Generalâ??s Office to:

- Computer Crime Section
- Virginia Attorney Generalâ??s Office
- 202 North 9th Street
- Richmond, VA 23219

For further inquiries regarding database breach notification, please contact the Computer Crime Section at 804-786-2071.

As a result, determining the *applicable* state law requirements entails initial analysis of your stateâ??s laws, immediately followed by an analysis of your customersâ?? states of residence. Once a customerâ??s residence is established, you will need to read and follow the state law associated with that particular resident. For an active title agency, handling transactions for buyers and sellers moving to and from locations nationwide, this approach may force you to read and comply with dozens of state laws.

VLTA Examiner

Consider whether you are exempt in particular state statutes

In reading those applicable state laws, you need to check for any provision that exempts your company from compliance with the specifics of that particular state law. For example, some states like Virginia, provide that the statute defining the notice obligations â??does not apply to any person or entity subject to Title V of the Gramm-Leach-Bliley Act of 1999.â?• If you run a shoe repair company or other entity not governed by GLBA, this provision would not have any impact on your state-mandated obligations. However, if you are a title and/or settlement agency, which GLBA defines as a â??financial institution,â?• this type of provision may exempt you from the specific customer notification obligations requirement under *state* laws that contain such a provision. In that case, a title/settlement agency then must look at the federal laws and regulations to determine what course of action to employ.

Obligations arising under federal laws and regulations

There is a clear argument that title and settlement agencies always are covered by the obligations imposed under various federal laws. GLBA, codified at 15 U.S.C. Â§ 6801 et seq., is an all-encompassing piece of federal legislation passed in 1999 that imposes strict obligations on financial institutions to protect the NPI of their customers and consumers. By definition, title and settlement agents are deemed to be financial institutions and therefore subject to those same obligations and penalties for breach thereof. Additionally, Section 5 of the FTC Act, 15 U.S.C. Â§ 45, grants the FTC power to investigate and prevent deceptive trade practices and deems it the primary government enforcement agency with powers to impose penalties for financial institution data breaches. For that reason, the federal definition of a data breach must be considered.

The FTC defines a data breach as â??*any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.*â?• GLBA has a similar, but slightly different, definition: *â??Any unauthorized disclosure of personally identifiable financial information that was given by a consumer to a financial institution resulting from any transaction with the consumer or any service performed for the consumer or otherwise obtained by the financial institution.*â?• Note that neither of these definitions provides any

safe harbor for the loss of data that has been encrypted. So, if you determine that your customer notification obligations are governed by adherence to federal laws, although encryption is highly recommended as a defense to unauthorized access, it will not lessen your notification obligations if a device is lost, stolen, or compromised.

Window for compliance once a breach occurs

Once you have determined which law(s) apply, you then have the obligation to dig deeper and identify the specific steps you must take. It is recommended that you have access to the laws that apply to your organization to expedite your ability to react timely. Failing to act within the specific time frame could subject you to significant fines and penalties. Virginia statutes, and many other states describe the time frames for your notificaion actions in general terms, such as â??without unreasonable delay,â?• but other states have specific timing deadlines to which you must adhere. Tennessee, Ohio, Rhode Island, Vermont, Washington, and Wisconsin require that notices be given in 45 days. Other states require even shorter deadlines (Floridaâ??s is 30 days), while Connecticut currently has a 90-day deadline. This may seem like a workable time period, but there are numerous actions that must be taken within this period, and acting promptly will minimize your eventual financial and reputational losses.

VLTA Examiner

Do you find all this overwhelmingly confusing? While a complicated subject, it is essential to understand to prepare yourself for the possibility of a data breach. Hopefully, by realizing the complexity inherent in developing a post-breach plan of action, you will be even more focused on the importance of taking every step necessary to avoid a data breach event.

Finally, if you find that you are obligated to provide a breach notification to affected parties, you have to struggle with what to say and how to say it *appropriately*.

The referenced industry experts referenced hereinabove all offered advice regarding what they thought was the â??appropriateâ?• response to a data breach. However, whether or not an entity responds â??appropriatelyâ?• ultimately will be evaluated by the Federal Trade Commission (FTC), which has direct supervision over all cybersecurity issues, and acts as the final arbiter in determining whether the actions taken are enough. Therefore, is important to stay abreast of any guidance the FTC has offered on this topic.

October 25, the FTC released new guidance for businesses outlining recommended actions to take in the event of a data breach. This publication, â??Data Breach Response Guideâ?• (Guide), provides a concise description of a response plan, complete with a sample letter to send to those affected.

The Guide covers three categories of actions: securing operations, fixing vulnerabilities, and notifying the appropriate parties. Recently, Morgan Lewis & Bockius LLP released a blog that provides a good summary of these three action areas, but the FTC publication is straightforward and leaves fewer questions about the FTCâ??s expectations of an appropriate response.

The 16-page booklet provides step-by-step instructions for what should be accomplished once an entity is made aware of a data breach, along with key phone numbers and website addresses of parties that immediately should be contacted. It provides concise information about obligations regarding *required notification* of the FTC and others, as well as links to appropriate local and federal authorities. I would suggest this Guide be part of your plan for developing an appropriate response in the likely event a

data breach would occur in the future.

Remember, compliance with ALTAâ??s Best Practices Pillar 3 requires more than implementing policies and procedures designed to minimize unauthorized access to customersâ?? confidential data. It also requires that you maintain a plan to deal with any security hacks that might occur. Development of a written â??post-breachâ?• action plan is required under Pillar 3.10, which requires a third-party assessment firm to â??*obtain and review documented procedures for security breach notification, including evidence of a program review at least annually.*â?• Since itâ??s required that you have a written plan, the plan should incorporate compliance with the procedures and processes outlined in this FTC Guide. By doing so, entities can ensure they are in compliance with Best Practices assessment procedure 3.10, but more importantly, they can avoid significant fines as levied by the FTC after the occurrence of a data breach.

VLTA Examiner

*By Eugene McCullough, Esq., NTP, CIPP/US, Director of Title Industry Services for PYA, a nationwide CPA firm offering ALTA Best Practices assessments and reprinted by permission from **www.pyabestpracticesblog.com**, an ongoing firm blog series of topics relevant to the title issuance and settlement industry.*

Category

1. Cybersecurity

Date Created
2017/09/22
Author
vltaexaminer