# ARE YOUR ONLINE BUSINESS PARTNERS SECURITY COMPLIANT ? by the Insellerate Research Team

In the digital age companies have had to make significant changes to keep up with how customers want to do business. This often means email instead of traditional mail and phone calls in the place of in person meetings. In addition, the forms, data, and contact information we used to keep in our planners/desks/rolodexes have all moved online to our digital CRM (Customer Relationship Management) systems. As we have moved this information online we have also changed the way that it can be accessed and a new group of security concerns has arisen. Who can access the data? How secure is it? How can we best insure that our customer data remains safe and usable for our employees? Security and privacy of customer information isn't just something companies should do, it's something they must do in order to remain complaint under a new set of laws and regulations designed to protect consumers. In this article we are going to talk about consumer data protection and why your business needs to be on the forefront of this topic if it wants to excel.

## WHY DOES THIS MATTER?

The first thing we need to discuss is why this even matters. Companies have been handling customer data as long as they have had customers, so what is so important now that has created such a shift in the necessity to enhance data security? The answer, as it turns out, is quite complex. There are a whole host of issues that arise when data is grouped together digitally. Let's compare briefly a locked filing cabinet to a "secure" data storage site online. With a filing cabinet, perhaps one or two people have keys and if someone wants to steal the data, they would have to physically break in or attempt to carry that cabinet out of a crowded office. With digital data storage, an online threat can attempt to access your data from the comfort of their home, sitting behind a computer, hiding behind firewalls and complex mechanisms to remain undetectable. They can try to access your information as many times as they want, and in most cases you don't even know they're there.

Another issue with modern data is business size, reach, and scale. Where as an individual in the past may have had a book of business that contained the information of 100 customers, a single salesperson can now have a CRM database with hundreds of thousands of potential clients… sometimes substantially more. With CRM systems the amount of "potential clients" the system can contain is virtually limitless.

The value of combining huge pools of customer data with powerful CRM applications is very clear: Increasing the number of contacts and follow up opportunities each day allows the salesperson to productively manage more clients than ever before. However, making sure that the CRM company you work with is protecting your client's valuable data has never been more important. Understanding how to navigate this complicated landscape, and building a partnership with an established and compliant partner is how businesses are going to either succeed or fail in this new digital business landscape.

## BECOMING COMPLIANT

Now that we know what the issues are, and why we need to be aware of them, we can talk about how you can continue to house large amounts of customer data while still being compliant with current rules and regulations.

To start, you should make sure that the CRM company (or any other SaaS system) whose software you use to house your client's data is compliant with SSAE 16 (Statement on Standards for Attestation Engagements no. 16). What is SSAE16? To put it simply, companies abiding by SSAE16 are showing a commitment to insuring the safety of data that passes through their systems. They don't just make claims about the data safety either, they back it up with a series of policies, protocols, and procedures designed to eliminate the security problems


of large-scale data management systems.
first thing we need to discuss is why this even matters. Companies have been handling customer data as long as they have had customers, so what is so important now that has created such a shift in the necessity to enhance data security? The answer, as it turns out, is quite complex. There are a whole host of issues that arise when data is grouped together digitally. Let's compare briefly a locked filing cabinet to a "secure" data storage site online. With a filing cabinet, perhaps one or two people have keys and if someone wants to steal the data, they would have to physically break in or attempt to carry that cabinet out of a crowded office.

Some of the ways that SSAE16 companies demonstrate their commitment to secure data housing are:

- ***Evaluating Daily Operations*** – Reviewing their business operations daily to ensure that you are following the procedures laid out in their company's compliance plans
- ***Internal Audits –*** Conducting random audits of data.
- ***System Checks and Balances*** – Creating multiple points of control to ensure that no one action can compromise client data.
- ***Detailed Policies and Procedures*** – Creating a written control document that outlines the steps and actions taken by the company to ensure data safety. Also, putting in to detail the ongoing steps that they will take to ensure compliance moving forward.
- ***Written Assertion by Management*** – Enhancing accountability by having company management "assert" to the description, control, and criteria (amongst other things) that outline the companies' commitment to compliance.

Again, these are just some of the ways that a company must demonstrate its ongoing compliance to the SSAE16 protocols. How do you know if the company you're working with is compliant with SSAE16? Simple, ask to see a copy of their SSAE16 Audit Report. The Audit Report will show that the SaaS business whose services you utilize is taking all the necessary steps to insure your valuable customer data stays safe and secure.

## CONSEQUENCES OF INACTION

While it might not seem like an urgent issue for every company, the ramifications of not being in compliance with SAS 16 are very real. With modern cloud computing systems the size and scope of data breaches are growing every data. In fact, issues of data security are becoming so commonplace there is an entire industry category developing to track data breaches. To demonstrate just how serious these leaks are, and how much data is at stake, here are just a few examples pulled from news headlines in 2015 alone:

- Premera Blue Cross – 11 million customer health records breached*
- Army National Guard – 850,000 records of Guard members breached**
- USA Office of Personnel Management - 21.5 Million US Government employee records breached***
- Experian/T-Mobile – 15 Million T-Mobile customer accounts breached****

And the list goes on and on. Data breaches of varying size and scope happen every day, and it's not just the customers (who's data is breached) that are being affected. The SaaS companies (and equally importantly, those who utilize their services) are suffering huge loses is decreased revenue from bad publicity and the resulting lack in consumer confidence that goes with it. Long gone are the days when an internal data breach could be kept "internal" and we see more and more examples of this as articles are pulled from the headlines and virally spread across the internet.

Perhaps worst of all is the fact that there are simple steps that can be taken to protect both your client's data and your companies' reputation. Some simple due diligence in choosing SaaS partners that are SSAE16 certified will go a long way in terms of protecting your clients sensitive data and making sure that your companies name isn't next to appear next to the term "data breach" in news headlines.

---

* https://www.premera.com/wa/visitor/healthsource/community/premera-cyberattack/?WT.z_ref=www.google.com/&WT.z_redirect=www.premera.com/cyberattack/

** http://www.nationalguard.mil/News/ArticleView/tabid/5563/Article/607769/army-national-guard-announces-data-breach-establishes-call-center.aspx

*** https://www.opm.gov/cybersecurity/#Actions

****http://www.t-mobile.com/landing/experian-data-breach-faq.html


The Insellerate Research Team was formed to provide companies and consumers with pertinent and timely information on issues surrounding commerce in the digital age.

Insellerate is a simple-to-use, yet sophisticated sales force automation and lead management platform. A specialized CRM that delivers incremental sales and revenue by optimizing consumer direct lead channels, increasing prospect conversion and maximizing sales opportunities through an automated lead nurture program.