Protecting Client Data and Maintaining Compliance in an Emerging SaaS World— *Eight Critical Questions to Consider with SaaS Vendors*

As the tax and accounting profession continues its transition to SaaS (Software as a Service), client data continues its move outside the walls of firms and into the "cloud." All firms should be concerned about data security and compliance regarding their client's data. Even though the power, convenience, and cost-effectiveness of SaaS applications is widely accepted, professional standards call for healthy skepticism when it comes to safeguarding client data. This is nothing new as data security has been a long-time concern within the tax and accounting profession—oftentimes slowing the adoption of SaaS among less well-informed firms. The reality is that data security is reliant not only on the application itself, but also on the vendor's internal controls for handling the data. Fully aware of the profession's concerns, many leading SaaS vendors have taken significant steps to ensure security of client data and help firms comply with rapidly changing ethical, legislative, and regulatory mandates.

SaaS is Here to Stay

Software as a Service has arrived, and it's not going away—just look at a few recent events. SaaS vendors swept the 2009 *The CPA Technology Advisor*'s Innovation Awards—taking all five accolades. Recipients included Copanion (GruntWorx Pro), Bill.com, SmartVault, CCH (IntelliConnect) , and Capital Confirmation (CONFIRM Technology). Executive Editor Darren Root, CPA.CITP stated, "This is the first year that online technologies have won all five Innovation Awards, a noteworthy feat that clearly demonstrates the continued growth and acceptance of SaaS applications and other web-based systems by tax and accounting professionals." Earlier in the year, BigTime, SmartVault, Bill.com, and other notable SaaS applications all made The Sleeter Group's annual Awesome Add-on's list for 2009.

SaaS solutions provide users with easy-to-use and innovative offerings that help firms provide real-time service to their clients—at a comfortable price point. Strong value propositions, healthy ROIs, and easily deployable solutions are all fueling the SaaS boom. However, as SaaS becomes more mainstream, the profession is demanding that vendors continue to raise the bar on internal controls to ensure the security of data outside the firm's office as well as compliance with all regulations.

The standard for security and compliance measures includes completion of a SAS 70 Type II audit, third-party validation of privacy policies, and implementation of Extended Validation technology. Leading vendors understand the necessity of security and compliance assurance and most would suggest that user firms do their homework when looking for a SaaS vendor.

Eight Critical Questions to Consider with SaaS Vendors

1. Does the vendor publish a Privacy Policy?

Vendors that publish their privacy policy provide users with full disclosure of the standards that govern the information and practices of the firm's website. A high quality vendor's privacy policy should be easily found on every page of their website.

2. In addition to publishing the Privacy Policy, have the vendor's privacy practices and enforcement been validated by a credible, qualified third-party?

Strong vendors disclose information practices and employ an independent auditor, such as TRUSTe, to review all privacy practices for compliance. TRUSTe is a third-party entity with the mission to build users' trust and confidence in the Internet by promoting the use of fair information practices. To ensure enforcement of a SaaS vendor's privacy policy, look for an auditor's logo such as TRUSTe.

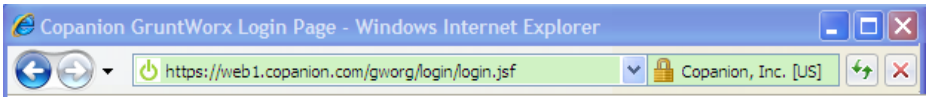
TRUSTe CERTIFIED PRIVACY

TRUSTe CLICK TO VERIFY

3. What is the process for data encryption while in transit to and from the SaaS vendor's data center?

This is a critical question in relation to the security of clients' data, especially as states start to enforce new laws requiring that all personal information be encrypted at all times. Vendors who understand the serious nature of data security will have Extended Validation technology in place. Best practices include utilizing the highest level of data security, such as VeriSign's 128-Bit Secure Sockets Layer (SSL) with Extended Validation technology. In 2008, *The CPA Technology Advisor*'s then Executive Editor Gregory L. LaFollette, CPA.CITP wrote: "These new 'super certificates' can only be issued by a select few very high-level 'certificate authorities.' Each of these high-level issuers must undergo independent audits to confirm their compliance with special standards relative to their business verification practices." To ensure use of Extended Validation technology, look for the logo on the vendor's website:

VeriSign Secured VERIFY



4. Is data housed and processed in a SAS 70 Type II data center?

SAS 70 (Statement on Auditing Standards Number 70) is an internationally recognized standard developed by the AICPA. SAS 70 was designed to provide a highly specialized audit of an organization's internal controls to ensure the proper handling of client data. SAS 70 Type II certification ensures that client data is protected in a data center that is using industry-leading best practices in information technology and security. This is a must for SaaS vendors and should be at the top of a user organization's list when evaluating a SaaS vendor. Look for a data center that is a 100% U.S.-based SAS 70 Type II certified facility, providing clients with a measure of assurance that their data is secure. In addition, make sure that the vendor does not allow anyone outside of the United States to *ever* have access to client data located in the data center.

5. Has the vendor completed a SAS 70 Type II audit (in addition to housing data in a SAS 70 Type II data center)?

How clients' data is handled is the most important factor when considering data security, so vendors must have proper internal controls in place. Vendors that undergo a SAS 70 Type II audit are stringently evaluated on such elements as systems, technology, facilities, personnel management, and detailed processes for handling client data. At the end of a six-month process, vendors receive a comprehensive audit report that includes a description of their operational controls and a description of the auditor's tests of operating effectiveness. At regular intervals after the initial audit, vendors go through additional audits to maintain their SAS 70 Type II status. In brief, SAS 70 provides assurance that a vendor has put in place comprehensive systems to ensure data security.

From the CPA firm's perspective this provides the "gold seal" of assurance that client data is secure. Client data security should be the prime focus within a service organization's operational model. A high quality SaaS vendor will be happy to provide a copy of its comprehensive audit report, including a description of operational controls and auditor's tests of operating effectiveness.

6. Does the vendor use a third-party entity to consistently test and certify against security vulnerability?

When providing software over the Internet, vendors must consistently monitor the security of their web applications. McAfee SECURE Certification applies patent-pending security auditing technology to test web applications for vulnerability issues. Best practices include utilizing McAfee SECURE or another comparable program to test the website on a daily basis. When searching for a SaaS vendor, look for the SECURE logo:

7. Do vendor processes comply with IRC 7216?

Disclosure rules set forth in Internal Revenue Code Section 7216 require tax professionals to obtain client consent before disclosing their information to certain vendors including overseas tax processors. Tax professionals using vendors (1) that are located in the US and (2) that do *not* provide substantive determinations affecting tax liabilities are exempt from §7216 disclosure requirements.

Make sure your provider complies with the first requirement of §7216 by storing and processing all client tax documents in U.S.-based data centers accessed only by U.S.-based employees. Providers must also comply with the second requirement of §7216 by transcribing data from client source documents into tax preparation software when there is only one place to put the data. The SaaS offering, whether an automated or outsourced service, cannot apply professional judgment to determine the appropriate location for tax information to be entered because that judgment could be interpreted as a substantive determination.

8. Does the vendor comply with individual state regulations?

As SaaS grows in popularity, states will start to enact their own disclosure regulations. For example, Section 54.1 of the California Board of Accountancy Regulations requires informed consent of the client "through an engagement letter or in a separate consent agreement" before disclosing confidential information to an "external service provider" or an "external technician or software vendor in order to resolve software problems."

For any tax software vendor to support products, resolve software issues, or sample returns to verify product quality, it may be necessary to access confidential information. Practitioners are advised to get client approvals in advance of needing such support by using engagement letters, a well known and widely recommended practice. This wording from the AICPA's sample language for engagement letters has been approved by the California Board of Accountancy as satisfying Section 54.1 requirements:

> The firm may from time to time, and depending on the circumstances, use third-party service providers in serving your account. We may share confidential information about you with these service providers, but remain committed to maintaining the confidentiality and security of your information. Accordingly, we maintain internal policies, procedures and safeguards to protect the confidentiality of your personal information. In addition, we will secure confidentiality agreements with all service providers to maintain the confidentiality of your information and we will take reasonable precautions to determine that they have appropriate procedures in place to prevent the unauthorized release of your confidential information to others. Furthermore, the firm will remain responsible for the work provided by any such third-party service providers.

Adoption of SaaS applications is growing at a rapid rate, and with this growth must come a dedicated focus on data handling processes and internal controls by vendors. By monitoring controls and undergoing scheduled audits, vendors can consistently work to improve processes and assure tax and accounting professionals of the security of client data.

The growth of SaaS also means additional responsibility for tax and accounting professionals—primarily in choosing SaaS vendors. Firms need to be careful in their selection process—equipped with a list of questions that center on data security and regulatory compliance related to the handling of that client data. For example: Has the vendor completed a SAS 70 Type II audit and is data housed in a SAS 70 Type II data center? Does the vendor apply advanced data encryption? Are all services U.S. based? Does the vendor avoid making substantive determinations? With the proper knowledge in hand, firms can enjoy all the convenience that SaaS offers, along with peace of mind that client data is safe.

About the Author

Steven Ladd is co-founder and CEO of Copanion—a leading innovator in tax document automation. Prior to founding Copanion, Ladd was chairman of Systematic Accounting. Earlier in his career, he founded InterChip Systems, Inc—an electronics product development company that was subsequently purchased by Honeywell. He has also acted as a consultant to technology businesses and has managed sales, manufacturing, and design operations at venture-backed and Fortune-500 sponsored start-ups.

Ladd holds Bachelor's and Master's degrees in electrical engineering and computer science from Massachusetts Institute of Technology, where he was a National Science Foundation Graduate Fellow. He can be reached by emailing **sladd@copanion.com**.

Eight Critical Questions to Consider with SaaS Vendors
Copanion's Compliance

1. **Does the vendor publish a Privacy Policy?**

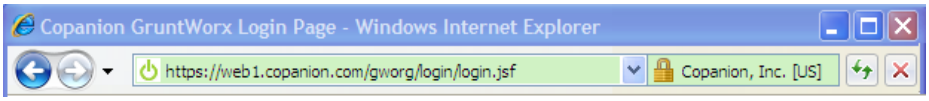
   Copanion's Privacy Policy can be found at http://www.copanion.com/about/privacy-policy.php, or as part of the footer on any page of the Copanion.com website.

2. **In addition to publishing the Privacy Policy, have the vendor's privacy practices and enforcement been validated by a credible, qualified third-party?**

   Copanion discloses information practices and employs TRUSTe to review all privacy practices for compliance. Users can verify the validity of Copanion's TRUSTe standing by clicking the "TRUSTe Click to Verify" button at the top of Copanion's privacy statement. The TRUSTe logo can also be found as part of the footer on any page of the Copanion.com website.

3. **What is the process for data encryption while in transit to and from the SaaS vendor's data center?**

   Copanion uses VeriSign 128-bit Secure Sockets Layer (SSL) with Extended Validation technology to protect client data. This technology provides the highest levels of authentication and data encryption available –protecting client data with the same levels of security as e-filing and electronic banking. Client files on Copanion servers are stored in encrypted form until they are deleted by the client. Users can verify the validity of Copanion's VeriSign security by clicking the VeriSign logo in the footer on any page of the Copanion.com website.



4. **Is data housed and processed in a SAS 70 Type II data center?**

   Copanion's data center is a 100% U.S.-based SAS 70 Type II certified facility, providing clients with a measure of assurance that client data is secure. In addition, Copanion does not allow anyone outside of the United States to *ever* have access to client data located in the data center.

5. **Has the vendor completed a SAS 70 Type II audit (in addition to housing data in a SAS 70 Type II data center)?**

   Copanion has received a comprehensive SAS 70 audit report, which includes a description of operational controls and a description of the auditor's tests of operating effectiveness –providing assurance that Copanion has put in place comprehensive systems to ensure data security. Users can request a copy of this audit report by clicking on the SAS 70 icon in the footer on any page of the Copanion.com website.

6. **Does the vendor use a third-party entity to consistently test and certify against security vulnerability?**

   Copanion uses McAfee Secure to test and certify against security vulnerabilities on a daily basis. McAfee Secure is accredited to meet the scanning requirements of the Payment Card Industry Data Security Standard. The SECURE seal shows that a web application has passed their daily audit. When security vulnerability is identified, a website must patch the issue within 72 hours to maintain certification. Users can verify the validity of Copanion's McAfee certification status by clicking the McAfee Secure button in the footer on any page of the Copanion.com website.

7. **Do vendor processes comply with IRC 7216?**

   Copanion complies with the first requirement of §7216 by storing and processing all client tax documents in U.S.-based data centers. Copanion complies with the second requirement of §7216 by transcribing data from client source documents into tax preparation software when there is only one place to put the data. When there is professional judgment required to determine the appropriate location for tax information to be entered, GruntWorx products put the information on point sheets so that the *tax preparer* can determine where to enter the information on the tax return.

8. **Does the vendor comply with individual state regulations?**

   As SaaS grows in popularity, states will start to enact their own disclosure regulations. In these instances, Copanion will take action to comply with individual state regulations, or inform users of what they can do to maintain compliance.

   For example, to remain in compliance with Section 54.1 of the California Board of Accountancy Regulations, Copanion recommends that practitioners receive client approvals in advance of needing support of external service providers by using engagement letters, a well known and widely recommended practice. Copanion even recommends sample language for engagement letters, as approved by the California Board of Accountancy. This language can be found at: http://www.copanion.com/support/data_security.php#q17.