




# The North Carolina State Bar

ALICE NEECE MINE  
Assistant Executive Director  
208 Fayetteville Street Mall  
PO Box 25908  
Raleigh, North Carolina 27611-5908  
Telephone: 919/828-4620  
Fax: 919/821-9168

 **MEMORANDUM**

FROM: Alice Neece Mine

TO: Amy A. Edwards

RE: **Proposed 2011 FEO 6, *Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property***  
**Proposed 2011 FEO 7, *Using On-line Banking to Manage a Trust Account***

DATE: November 8, 2011

---

The Ethics Committee of the North Carolina State Bar met in regular quarterly session on October 20, 2011, and reconsidered the above proposed opinions. Based upon the recommendation of a subcommittee, revised versions of the proposed opinions will be published in the next issue of the State Bar's *Journal*. Copies of the proposed opinions are attached. Assuming no criticism of the revised proposed opinions is received following their publication, the committee will recommend adoption to the Council at the Council's next meeting in January. If objection is received, the Ethics Committee will reconsider the proposed opinions at its January meeting and decide whether to recommend adoption of the opinions to the Council or to revise or withdraw the opinions. You may expect to hear from me regarding the status of the proposed opinions following the January meeting.

CC: Tom Bartolomeo Rakesh Madhava  
Nichole Black Eric Mazzone  
Jim Calloway Jack Newton  
Lee D. Cumbie Patrick Newton  
David Dahl Vaddrick Parker  
Carolyn Elefant Larry Port  
Carol Eubank Neal Ramee  
Timothy J. Evans Carey Ransom  
Christopher Fulmer Neil A. Reinmann  
Richard Granat Christine Dorrestein-Schultz  
Kris Gardner Grace Suarez  
Jeff Goens Bob Wells  
Tom Grella Robert Wirth  
Shadid Khan Randy Wooden  
Stephanie Kimbro

**Proposed 2011 Formal Ethics Opinion 6**  
**Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality**  
**and Preservation of Client Property**  
**October 20, 2011**

*Proposed opinion rules that a law firm may contract with a vendor of software as a service provided the lawyer uses reasonable care to safeguard confidential client information.*

**Inquiry #1:**

Much of software development, including the specialized software used by lawyers for case or practice management, document management and billing/financial management, is moving to the “software as a service” (SaaS) model. The American Bar Association’s Legal Technology Resource Center explains SaaS as follows:

SaaS is distinguished from traditional software in several ways. Rather than installing the software to your computer or the firm's server, SaaS is accessed via a web browser (like Internet Explorer or FireFox) over the Internet. Data is stored in the vendor's data center rather than on the firm's computers. Upgrades and updates, both major and minor, are rolled out continuously.... SaaS is usually sold on a subscription model, meaning that users pay a monthly fee rather than purchasing a license up front.<sup>1</sup>

SaaS is more pervasive than just the practice management software addressed above. For example, if a lawyer uses any of the following technologies to communicate, the lawyer is using SaaS: email attached to an internet service provider; voicemail on a mobile phone; text messaging or short message service (SMS); online backup or storage; online legal research; and online communication with other professionals or clients over social media or other web-based applications.

SaaS for law firms may involve the storage of a law firm’s data, including client files, billing information, and work product on remote servers rather than on the law firm’s own computer and, therefore, outside the direct control of the firm’s lawyers. Lawyers have duties to safeguard confidential client information, including protecting that information from unauthorized disclosure, and to protect client property from destruction, degradation or loss (whether from system failure, natural disaster, or dissolution of a vendor's business). Lawyers also have a continuing need to retrieve client data in a form that is usable outside of a vendor's product.<sup>2</sup> Given these duties and needs, may a law firm use SaaS?

**Opinion #1:**

Yes, provided steps are taken to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property, including the information in a client's file, from risk of loss.

The use of the Internet to transmit and store client information presents significant challenges. In this complex and technical environment, a lawyer must be able to fulfill the fiduciary obligations to protect confidential client information and property from risk of disclosure and loss. The lawyer must protect against security weaknesses unique to the Internet, particularly "end-user" vulnerabilities found in the lawyer's own law office. The lawyer must also engage in periodic education about ever-changing security risks presented by the Internet.

Rule 1.6 of the Rules of Professional Conduct states that a lawyer may not reveal information acquired during the professional relationship with a client unless the client gives informed consent or the disclosure is impliedly authorized to carry out the representation. Comment [17] explains, "A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision." Comment [18] adds that, when transmitting confidential client information, a lawyer must take "reasonable precautions to prevent the information from coming into the hands of unintended recipients."

Rule 1.15 requires a lawyer to preserve client property, including information in a client's file such as client documents and lawyer work product, from risk of loss due to destruction, degradation or loss. *See also* RPC 209 (noting the "general fiduciary duty to safeguard the property of a client"); RPC 234 (requiring the storage of a client's original documents with legal significance in a safe place or their return to the client); and 98 FEO 15 (requiring exercise of lawyer's "due care" when selecting depository bank for trust account).

Although a lawyer has a professional obligation to protect confidential information from unauthorized disclosure, the Ethics Committee has long held that this duty does not compel any particular mode of handling confidential information nor does it prohibit the employment of vendors whose services may involve the handling of documents or data containing client information. *See* RPC 133 (stating there is no requirement that firm's waste paper be shredded if lawyer ascertains that persons or entities responsible for the disposal employ procedures that effectively minimize the risk of inadvertent or unauthorized disclosure of confidential information). Moreover, while the duty of confidentiality applies to lawyers who choose to use technology to communicate, "this obligation does not require that a lawyer use only infallibly secure methods of communication." RPC 215. Rather, the lawyer must use reasonable care to select a mode of communication that, in light of the circumstances, will best protect confidential client information and the lawyer must advise effected parties if there is reason to believe that the chosen communications technology presents an unreasonable risk to confidentiality. *Id.*

Furthermore, in 2008 FEO 5, the committee held that the use of a web-based document management system that allows both the law firm and the client access to the client's file is permissible:

provided the lawyer can fulfill his obligation to protect the confidential information of all clients. A lawyer must take steps to minimize the risk that confidential client information will be disclosed to other clients or to third parties. *See* RPC 133 and RPC 215....A security code access procedure that only allows a client to access its own confidential information would be an appropriate measure to protect confidential client information....If the law firm will be contracting with a third party to maintain the web-based management system, the law firm must ensure that the third party also employs measures which effectively minimize the risk that confidential information might be lost or disclosed. *See* RPC 133.

In a recent ethics opinion, the Arizona State Bar's Committee on the Rules of Professional Conduct, concurred with the interpretation set forth in North Carolina's 2008 FEO 5 by holding that an Arizona law firm may use an online file storage and retrieval system that allows clients to access their files over the Internet provided the firm takes reasonable precautions to protect the security and confidentiality of client documents and information.<sup>3</sup>

In light of the above, the Ethics Committee concludes that a law firm may use SaaS if reasonable care is taken to minimize the risks of inadvertent disclosure of confidential information and to protect the security of client information and client files. A lawyer must fulfill the duties to protect confidential client information and to safeguard client files by applying the same diligence and competency to manage the risks of SaaS that the lawyer is required to apply when representing clients.

No opinion is expressed on the business question of whether SaaS is suitable for a particular law firm.

#### **Inquiry #2:**

Are there measures that a lawyer or law firm should consider when assessing a SaaS vendor or seeking to minimize the security risks of SaaS?

#### **Opinion #2:**

This opinion does not set forth specific security requirements because mandatory security measures would create a false sense of security in an environment where the risks are continually changing. Instead, due diligence and frequent and regular education are required.

Although a lawyer may use nonlawyers outside of the firm to assist in rendering legal services to clients, Rule 5.3(a) requires the lawyer to make reasonable efforts to ensure

that the services are provided in a manner that is compatible with the professional obligations of the lawyer. The extent of this obligation when using a SaaS vendor to store and manipulate confidential client information will depend upon the experience, stability and reputation of the vendor. Given the rapidity with which computer technology changes, law firms are encouraged to consult periodically with professionals competent in the area of online security. Some recommended security measures are listed below.

- Inclusion in the SaaS vendor's Terms of Service or Service Level Agreement, or in a separate agreement between the SaaS vendor and the lawyer or law firm, of an agreement on how the vendor will handle confidential client information in keeping with the lawyer's professional responsibilities.
- If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business or the service otherwise has a break in continuity, the law firm will have a method for retrieving the data, the data will be available in a non-proprietary format that the law firm can access or the firm will have access to the vendor's software or source code. The SaaS vendor is contractually required to return or destroy the hosted data promptly at the request of the law firm.
- Careful review of the terms of the law firm's user or license agreement with the SaaS vendor including the security policy.
- Evaluation of the SaaS vendor's (or any third party data hosting company's) measures for safeguarding the security and confidentiality of stored data including but not limited to firewalls, encryption techniques, socket security features, and intrusion-detection systems.<sup>4</sup>
- Evaluation of the extent to which the SaaS vendor backs up hosted data.

---

<sup>1</sup> *FYI: Software as a Service (SaaS) for Lawyers*, ABA Legal Technology Resource Center <<http://www.abanet.org/tech/ltrc/fyidocs/saas.html>>.

<sup>2</sup> *Id.*

<sup>3</sup> Paraphrasing the description of a lawyer's duties in Arizona State Bar Committee on Rules of Professional Conduct, Opinion 09-04 (Dec. 9, 2009).

<sup>4</sup> A firewall is a system (which may consist of hardware, software or both) that protects the resources of a private network from users of other networks. Encryption techniques are methods for ciphering messages into a foreign format that can only be deciphered using keys and reverse encryption algorithms. A socket security feature is a commonly-used protocol for managing the security of message transmission on the Internet. An intrusion detection system is a system (which may consist of hardware, software or both) that monitors network and/or system activities for malicious activities and produces reports for management.

---

**Proposed 2011 Formal Ethics Opinion 7**  
**Using On-line Banking to Manage a Trust Account**  
**October 20, 2011**

*Proposed opinion rules that a law firm may use on-line banking to manage its trust accounts provided the firm's managing lawyers are regularly educated on the security risks and actively maintain end-user security.*

**Inquiry:**

Most banks and savings and loans provide “on-line banking” which allows customers to access accounts and conduct financial transactions over the Internet on a secure website operated by the bank or savings and loan. Transactions that may be conducted via on-line banking include account-to-account transfers, payments to third parties, wire transfers and applications for loans and new accounts. On-line banking permits users to view recent transactions and view and/or download cleared check images and bank statements. Additional services may include account management software.

Financial transactions conducted over the Internet are subject to the risk of theft by hackers and other computer criminals. Given the duty to safeguard client property, particularly the funds that a client deposits in a lawyer's trust account, may a law firm use on-line banking to manage a trust account?

**Opinion:**

Yes, provided the lawyers use reasonable care to minimize the risk of loss or theft of client property specifically including the regular education of the firm's managing lawyers on the ever-changing security risks of on-line banking and the active maintenance of end-user security.

As noted in [proposed] 2011 FEO 6, *Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property*, the use of the Internet to transmit and store client data (or, in this instance, data about client property) presents significant challenges. In this complex and technical environment, a lawyer must be able to fulfill the fiduciary obligations to protect confidential client information and property from risk of disclosure and loss. The lawyer must protect against security weaknesses unique to the Internet, particularly “end-user” vulnerabilities found in the lawyer's own law office. The lawyer must also engage in frequent and regular education about the security risks presented by the Internet.

Rule 1.15 requires a lawyer to preserve client property, to deposit client funds entrusted to the lawyer in a separate trust account, and to manage that trust account according to strict recordkeeping and procedural requirements. *See also* RPC 209 (noting the “general fiduciary duty to safeguard the property of a client”) and 98 FEO 15 (requiring a lawyer to exercise “due care” when selecting depository bank for trust account). The rule is silent, however, about on-line banking.

Nevertheless, on-line banking may be used to manage a client trust account if the record-keeping and fiduciary obligations in Rule 1.15 can be fulfilled. The recordkeeping requirements for trust

accounts are set forth in Rule 1.15-3. Rule 1.15-3(b)(3) specifically requires a lawyer to maintain the following records relative to the transfer of funds from the trust account:

all instructions or authorizations to transfer, disburse, or withdraw funds from the trust account (including electronic transfers or debits), or a written or electronic record of any such transfer, disbursement, or withdrawal showing the amount, date, and recipient of the transfer or disbursement, and, in the case of a general trust account, also showing the name of the client or other person to whom the funds belong;

If the online banking software does not provide a method for making an official bank record of the required information when money is transferred from the trust account to another account, such transfers must be handled by a method that provides the required records.

To fulfill the fiduciary obligations in Rule 1.15, a lawyer managing a trust account must use reasonable care to minimize the risks to client funds on deposit in the trust account by remaining educated as to the dynamic risks involved in on-line banking and insuring that the law firm invests in proper protection and multiple layers of security to address those risks. *See* [proposed] 2011 FEO 6.

A lawyer who is managing a trust account has affirmative duties to regularly educate himself as to the security risks of on-line banking; to actively maintain end-user security at the law firm through safety practices such as strong password policies and procedures, the use of encryption and security software, and the hiring of an information technology consultant to advise the lawyer or firm employees; and to insure that all staff members who assist with the management of the trust account receive training on and abide by the security measures adopted by the firm. Understanding the contract with the depository bank and the use of the resources and expertise available from the bank are good first steps toward fulfilling the lawyer's fiduciary obligations.

This opinion does not set forth specific security requirements because mandatory security measures would create a false sense of security in an environment where the risks are continually changing. Instead, due diligence and frequent and regular education are required. A lawyer must fulfill his fiduciary obligation to safeguard client funds by applying the same diligence and competency to manage the risks of on-line banking that a lawyer is required to apply when representing clients.