2015 ABA Conference on Professional Responsibility

Emerging Issues in Confidentiality:
Confidentiality in a Mobile Technology-Laden Society

Pamela A. Bresnahan
pabresnahan@vorys.com
(202) 467-8861

Raymond D. Pinkham
rdpinkham@vorys.com
(202) 467-8806

Vorys, Sater, Seymour and Pease, LLP
1909 K St., NW, Ninth Floor
Washington, DC 20006
2015 ABA Conference on Professional Responsibility

Emerging Issues in Confidentiality: Confidentiality in a Mobile Technology-Laden Society

1. **Mobile Devices**

   Given the proliferation of mobile devices, including laptops, smartphones and tablets, confidential information is taken with us everywhere we go. Increasingly, lawyers and law firms have become targets of cyber attacks. This risk is greatest when an attorney accesses unencrypted data over an unsecured wireless network.

   The latest ABA Legal Technology Survey Report indicates that 14% of law firms experienced a breach last year in the form of a lost or stolen computer or smartphone, a hacker, a break-in or a website exploit.¹

   The ABA CyberSecurity Handbook even goes so far as to state that “it may be prudent for all lawyers and law firms to adopt a working assumption that their computer networks and critical IT systems – as well as those of vendors to whom they may outsource the storage and processing of client confidential information – are vulnerable to such attackers, increasingly the target of such attackers, and at this time remain largely indefensible and at high risk of being breached.”

   One important aspect of dealing with the current environment is knowing and understanding the professional rules and ethical obligations applicable to cyber security and the protection of client information in the digital world.

   ABA Model Rule 1.6(a) states that “[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent.” The amended Model Rule 1.6 has the following new paragraph (c): “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”

   Model Rule 1.6, Comment [18], was revised to include factors to be considered in determining the reasonableness of a lawyer’s efforts to prevent the disclosure of confidential client information.

   Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not

---

required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.

As examples, a lawyer should make reasonable efforts to prevent disclosures or access, such as avoiding a lawyer’s sending an email to the wrong person, someone’s “hacking” into a law firm’s network, or staff’s posting client information on the internet. As Comment [18] makes clear, not every disclosure is a violation, but reasonable precautions are required.

One of the main concerns is access to a loss or stolen device by unauthorized users. See Vincent J. Syracuse & Matthew R. Maron, Attorney Professionalism Forum, N.Y. State Bar Ass’n Journal, May 2013, Vol. 85, No. 4. One of the most basic rules regarding protecting confidentiality is the protection of the data itself, including password protection. This includes making a password “strong” and not simply “password” or “123456.” A “strong” password includes upper and lower case letters, numbers, symbols and even spaces.

Due to the “vast amounts of confidential information” that now can be stored on laptops, flash drives or smartphones, the ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies is considering the following precautions as recommendations related to the protection of confidential client information:

1. providing adequate physical protection for devices (e.g., laptops) or having methods for deleting data remotely in the event that a device is lost or stolen;

2. encouraging the use of strong passwords;

3. purging data from devices before they are replaced (e.g., computers, smartphones, and copiers with scanners);

4. installing appropriate safeguards against malware (e.g., virus protection, spyware protection);

5. installing adequate firewalls to prevent unauthorized access to locally stored data;

6. ensuring frequent backups of data;

7. updating computer operating systems to ensure that they contain the latest security protections;

8. configuring software and network settings to minimize security risks;

9. encrypting sensitive information, and identifying (and, when appropriate, eliminating) metadata from electronic documents before sending them; and,

10. avoiding “wifi hotspots” in public places as means of transmitting confidential information (e.g., sending an email to a client).

Attorneys and firms should also consider use of Mobile device management which allows firms to update all devices – and potentially remotely wipe the device if necessary.
An Ethics Opinion from the Florida Bar provides practical steps for lawyers to take in order to protect client confidentiality before a device is disposed of, including (1) identification of potential threats to confidentiality and implementation of policies to address such threats; (2) inventory all devices that contain hard drives or other storage media; (3) proper supervision of all nonlawyers to adequately assure that confidentiality will be maintained; and, (4) proper sanitization of a device by requiring meaningful assurances from a vendor at intake of a device and confirmation or certification of sanitization at disposition. The Florida Bar Ethics Op. 10-2 (2010).

A number of state bar ethics opinions generally address the issue of the types of measures attorneys should take in protecting confidential client information:

1. Alabama State Bar Association, Ethics Opinion 2010-02 (electronic documents must be secured and reasonable measures must be in place to protect the confidentiality, security and integrity of the documents and the lawyer must ensure that the process is at least secure as that required for traditional paper files. Attorneys must have “reasonable measures in place to protect the integrity and security of the electronic file, including ensuring that only authorized individuals have access to the electronic files, appropriate firewalls and intrusion detection software is in place and that electronically stored files are “back up” in case of file corruption or damage to the office).

2. Arizona Bar Opinion No. 09-04 (issued in December 2009). This opinion references specific acts to take such as secure socket layer (SSL) protocols, firewalls, password protections, encryption and anti-virus software. “As technology advances, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients’ documents and information.

3. State Bar of California, Standing Committee on Professional Responsibility and Conduct, formal Opinion No. 2010-179 (before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and, 6) the client’s instructions and circumstances, such as access by others to the client’s devices and communications.

4. State Bar of Massachusetts, Opinion 00-01 (use of unencrypted e-mail for purposes of transmitting confidential or privileged client communications does not, in most instances, constitute a violation of any applicable
ethical rule, including Rule 1.6, because both the lawyer and the client typically have a reasonable expectation that such communications will remain legally and effectively private).

5. Nevada Standing Committee on Ethics and Professional Responsibility Formal Opinion 33 (February 9, 2006) ("attorney may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney’s direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third party storage services.")

6. New Jersey Committee on Professional Ethics Opinion 701 (April 24, 2006) ("the critical requirement . . . .is that the attorney ‘exercise reasonable care’ against the possibility of unauthorized access to client information. A lawyer is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access.").

7. New York State Bar Association Committee on Professional Ethics, Opinion 1019 (August 6, 2014) (a law firm may give its lawyers remote access to client files, so that the lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing client of the risks).

8. Pennsylvania Bar Association, Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2011-200 (November 2011) (with regard to web-based e-mail, i.e., Gmail, AOL Mail, Yahoo! and Hotmail, the Committee concluded that “attorneys may use e-mail but that, when circumstances require, attorneys must take additional precautions to assure the confidentiality of client information transmitted electronically).

It is also important to keep in mind that various state and federal laws and regulations mandate the confidentiality of certain types of client information, including social security numbers, driver’s license information, financial accounts and related information, health and medical information, etc.

2. Confidentiality and Conflicts of Interest / Screening

There are increasing conflicts and disqualification risks due to increased lawyer mobility and firm mergers. One example was a recent attempt to disqualify Sidley Austin in defense of an auditor against allegations that the auditor failed to spot fraud at commercial lender Oak Rock Financial. A Sidley attorney brought the client to Sidley from Winston and Strawn, but Sidley transactional lawyers were involved in a 2010 investment in Oak Rock.
At a March 2015 hearing on the matter, New York Supreme Court Judge Shirley Werner Kornreich noted that due to mergers and how large firms have become, there are conflicts constantly.2

In another recent decision in a Motion to Disqualify in Lennar Mare Island, LLC v. Steadfast Insurance Company, Judge Kimberly Mueller in the US District Court for the Eastern District of California granted plaintiff’s motion to disqualify Hogan Lovells from its representation of defendant Steadfast Insurance Company.3

Beginning in 2005, Hogan started representing the parent corporation of one of the plaintiffs, CH2M Hill Constructor’s Inc., in the Lennar Mare Island matter. The General Counsel for the plaintiff described in a declaration that CH2M is “wholly dependent on Hogan Lovells for nearly all of the most important corporate and regulatory issues currently facing the company.” In August 2014, several attorneys for Hogan started to represent Steadfast Insurance as additional counsel because Steadfast’s counsel at the time informed it that the firm did not have the resources to continue as lead counsel.

Although Judge Mueller focused on the law firm’s duty of loyalty because she concluded that the conflict involved concurrent representation, confidentiality remained a concern in both concurrent and former client representation.

The duty of confidentiality is reflected in ABA Model Rule 1.6(b)(7) stating that “a lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary: (7) to detect and resolve conflicts of interest arising from the lawyer’s change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

The NY State Bar Association’s Committee on Standards of Attorney Conduct recently recommended that New York adopt new Comments to Rule 1.6 “to give lawyers more guidance about the disclosures that the existing New York Rules of Professional Conduct permit when lawyers and law firms contemplate lateral moves or law firm mergers.” The proposed comments provided more detailed guidance than the ABA comments regarding the specific types of information that is permitted to be shared without client consent in the context of a potential lateral move or law firm merger.

Proposed comment 18B states:

Disclosure without client consent in the contest of a possible lateral move or law firm merger is ordinarily permitted regarding basic information such as: (i) the identities of clients or other parties involved in a matter; (ii) a brief summary of the status and nature of a particular matter,

---


including the general issues involved; (iii) information that is publicly available; (iv) the lawyer’s total book of business; (v) the financial terms of each client-lawyer relationship; and (vi) information about aggregate timeliness of payments. Such information is generally not “confidential information” within the meaning of Rule 1.6.

Proposed comment 18C states:

Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily not permitted, however, if information is protected by Rules 1.6(a), 1.9(c), or Rule 1.18(b). This includes information that a lawyer knows or reasonably believes is protected by the attorney client privilege, or is likely to be detrimental or embarrassing to the client, or is information that the client has requested be kept confidential. For example, many clients would not want their lawyers to disclose their tardiness about paying bills; the amounts they spend on legal fees in particular matters; forecasts about their financial prospects; or information relating to sensitive client matters (e.g., an unannounced corporate takeover, an undisclosed possible divorce, or a criminal investigation into the client’s conduct).

The Proposed comments also state that attorneys and firms should take all reasonable measures to prevent unauthorized or inadvertent disclosures, including such measures as:

(1) disclosing client information in stages, initially identifying only certain clients and providing only limited information, and providing a complete list of clients and more detailed financial information only at subsequent stages; (2) limiting disclosure to those at the firm, or even a single person at the firm, directly involved in clearing conflicts and making the business decision whether to move forward to the next stage regarding the lateral hire or law firm merger; and/or (3) agreeing not to disclose financial or conflict information out the firm(s) during and after the lateral or merger process.

Moreover, effective Ethical Screens include things such as:

1. Notice to affected clients;
   a. ABA Model Rule 1.10(a)(2)
2. Training/guidance for attorneys and others;
3. Written checklists / protocols;
4. Notice to all screened persons;
5. Notice all persons working on screened matter;
6. Physical and operational separation;
7. Limited access to electronic files;
8. Continuing monitoring of the screen and reminders about the screen.

3. Ethical Implications of NSA Surveillance

In February 2014, the NY Times reported that a top-secret document obtained by former N.S.A. contractor Edward Snowden indicated that an American law firm was “monitored while representing a foreign government in trade disputes with the United States.”4 The article reported that the Australian Signals Directorate, the NSA’s Australian counterpart, notified the NSA that it was conducting surveillance, “including communications between Indonesian officials and the American law firm, and offered to share the information.”

The lesson should be clear. Attorneys and law firms engaged in international communications have to consider the potential for interception, especially in high profile cases or cases where the government may have a particular interest, including narcotics and terrorism cases.

On February 20, 2014, in light of these developments, James Silkenat, President of the ABA at the time, sent a letter to General Keith Alexander, who at the time, was Director of the NSA, and Rajesh De, General Counsel at NSA. The letter requested the NSA’s support in “preserving fundamental attorney-client privilege protections for all clients and ensuring that the proper policies and procedures are in place at NSA to prevent the erosion of this important legal principle.”

Mr. Silkenat’s letter explained that the interception and sharing of attorney-client privilege information and communications by government agencies “raises concerns, including chilling the full and frank discussion between lawyer and client that is essential for effective legal representation.” The letter continued, stating that “[a]ny government surveillance and interception of confidential communications between law firms and their clients threaten to seriously undermine and weaken the privilege. . . .”

The letter also referenced the ABA Resolution and Report 118, which was adopted by the ABA House of Delegates in August 2013. The ABA resolution condemned “unauthorized, illegal governmental organizational and individual intrusions in the computer systems and networks utilized by lawyers and law firms.” The resolution also urged federal, state, local, territorial and tribal governmental bodies to “examine, and if necessary, amend or supplement, existing laws to promote deterrence and provide appropriate sanctions for unauthorized, illegal intrusions into the computer networks utilized by lawyers and law firms” as well as urging the United States government to “work with other nations and organizations in both the public and private sectors to develop legal mechanisms, norms and policies to deter, prevent, and punish

---

unauthorized, illegal intrusions into the computer systems and networks utilized by lawyers and law firms."

On March 10, 2014, General Alexander responded to Mr. Silkenat’s letter, explaining that the “NSA is firmly committed to the rule of law and the bedrock legal principle of attorney-client privilege” and that the “NSA has afforded, and will continue to afford, appropriate protection to privileged attorney-client communications acquired during its lawful foreign intelligence mission in accordance with privacy procedures required by Congress, approved by the Attorney General, and, as appropriate, reviewed by the Foreign Intelligence Surveillance Court.”

Obviously, General Alexander’s letter reframed the issue, explaining that “[g]iven the inevitability of incidental collection of U.S. person information during the course of NSA’s lawful foreign intelligence mission—to include potentially privileged information—the issue is how to provide appropriate protections for any such information when it may be acquired.” General Alexander explained that NSA has policies and procedures in place that are “designed to minimize the acquisition, retention, and dissemination of information to, from, or about U.S. persons, including any potentially privileged information, consistent with the NSA’s foreign intelligence mission.” He further explained that potentially privileged information is given special review and consideration, in that any information that constitutes privileged communications must be reviewed by the Office of General counsel before dissemination, that the collection or reporting of such information be limited, that intelligence reports be written so as to prevent or limit privileged material and to exclude U.S. identities and that dissemination of such reports be limited and subject to appropriate warnings or restrictions on their use.

Nevertheless, concerns remain over the collection of information that could include attorney-client communications and privileged documents and/or work-product. The lack of detail regarding the scope of such surveillance makes it practically impossible to know which communications and types of data storage are secure.

Particularly sensitive communications are increasingly problematic. Attorneys and clients could meet face to face, but that could potentially involve costly international travel. Encryption of portable devices, e-mail and other communication is another option. Engagement Agreements with clients may start to include disclaimers that given potential governmental surveillance, absolute confidentiality of any attorney-client communications cannot be guaranteed. A July 2014 Human Rights Watch report on the impact of such surveillance indicated that some attorneys have started warning clients that they cannot guarantee their communications will remain confidential, only using e-mail, Gchat or WhatsApp for casual, non-substantive communications, and increasing amounts of travel in order to meet clients face to face.⁵

⁵ “With Liberty To Monitor All, How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy,” Human Rights Watch, July 2014.
4. **Confidentiality in Limited Scope Representation**

As the cost of legal services has increased, the frequency of limited scope representation, commonly known as “unbundling” has also increased. Limited scope representation, or unbundling, refers to the allocation between the lawyer and the client of the duties and responsibilities for handling a legal matter. California Rules of Court, Rule 3.35 defines the phrase as “a relationship between an attorney and a person seeking legal services in which they have agreed that the scope of the legal services will be limited to specific tasks that the attorney will perform for the person.”

Colorado Bar Association Ethics Committee, Formal Opinion 101 (1998) emphasized the importance of “unbundled” representation to “individuals who do not qualify for public or private legal assistance programs, but who cannot afford the full service of a lawyer.” The Colorado Bar Association Ethics Committee concluded that the ethics rules of Colorado allowed “unbundled legal services in both litigation and non-litigation matters.”

It is important to note that the attorney’s fiduciary duties of loyalty and confidentiality are not encumbered, even though the scope of representation may be limited. A publication by the State Bar of California, Committee on Professional Responsibility and Conduct, entitled “An Ethics Primer on Limited Scope Representation” states:

The fiduciary duties of loyalty and confidentiality apply with equal force and effect whether an attorney is providing full service representation for a transactional or litigation matter, or representing the client only on a limited scope basis. The duty of confidentiality is “fundamental to our legal system” and attaches upon formation of the attorney-client relationship, or even in the absence of such a relationship where a person has consulted an attorney in confidence.

Even in limited scope representations, attorneys must perform conflicts checks and avoid the disclosure of confidential client information. In some jurisdictions, this includes even including the fact that the representation is of a limited scope. State Bar of Arizona ethics opinion 06-03: Limited Scope Representation; Confidentiality; Coaching; Ghost Writing goes so far as to the state that “[i]n fact, unless required to do so by the rules, e.g., E.R. 1.6, an attorney may not disclose information pertaining to the limited representation unless authorized to do so by the client. Disclosure of the limited scope may indeed adversely affect the client’s situation.”

Other states frame the issue as one of making sure professional rules against “dishonesty, fraud, deceit or misrepresentation” are not violated. One New York City Bar Opinion (Formal Opinion 1987-2) states that pro se litigants are typically afforded “special treatment” by the courts and are generally held to less stringent standards. The opinion indicates that drafting any pleading, except for assisting a litigant in filing out a form, is “active and substantial legal assistance” that required disclosure to opposing counsel and the courts.

Similarly, Delaware State Bar Association Committee on Professional Ethics, Opinion 1994-2 (May 6, 1994) concluded that it would be improper for an attorney to fail to disclose his/her help when there has been “significant assistance,” which was defined as help that goes
beyond mere assistance with an initial pleading or providing initial general advice and information. Further, if an attorney provides advice on an on-going basis to an otherwise pro se litigant, the Committee on Professional Ethics concluded that this fact must also be disclosed.

Conclusion

Technology allows lawyers and their clients to communicate anytime and anywhere. Confidentiality is sometimes at risk because of the lawyers’ and clients’ mobility. Increased care must be taken because of the risk of interception and use of these otherwise privileged communications.
Formal Opinion 11-459  August 4, 2011

Duty to Protect the Confidentiality of E-mail Communications with One’s Client

A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party.¹

Introduction

Lawyers and clients often communicate with each other via e-mail and sometimes communicate via other electronic means such as text messaging. The confidentiality of these communications may be jeopardized in certain circumstances. For example, when the client uses an employer’s computer, smartphone or other telecommunications device, or an employer’s e-mail account to send or receive e-mails with counsel, the employer may obtain access to the e-mails. Employers often have policies reserving a right of access to employees’ e-mail correspondence via the employer’s e-mail account, computers or other devices, such as smartphones and tablet devices, from which their employees correspond. Pursuant to internal policy, the employer may be able to obtain an employee’s communications from the employer’s e-mail server if the employee uses a business e-mail address, or from a workplace computer or other employer-owned telecommunications device on which the e-mail is stored even if the employee has used a separate, personal e-mail account. Employers may take advantage of that opportunity in various contexts, such as when the client is engaged in an employment dispute or when the employer is monitoring employee e-mails as part of its compliance responsibilities or conducting an internal investigation relating to the client’s work.² Moreover, other third parties may be able to obtain access to an employee’s electronic communications by issuing a subpoena to the employer. Unlike conversations and written communications, e-mail communications may be permanently available once they are created.

The confidentiality of electronic communications between a lawyer and client may be jeopardized in other settings as well. Third parties may have access to attorney-client e-mails when the client receives or sends e-mails via a public computer, such as a library or hotel computer, or via a borrowed computer. Third parties also may be able to access confidential communications when the client uses a computer or other device available to others, such as when a client in a matrimonial dispute uses a home computer to which other family members have access.

In contexts such as these, clients may be unaware of the possibility that a third party may gain access to their personal correspondence and may fail to take necessary precautions. Therefore, the risk that third parties may obtain access to a lawyer’s e-mail communications with a client raises the question of what, if any, steps a lawyer must take to prevent such access by third parties from occurring. This opinion addresses this question in the following hypothetical situation.

An employee has a computer assigned for her exclusive use in the course of her employment. The company’s written internal policy provides that the company has a right of access to all employees’ computers and e-mail files, including those relating to employees’ personal matters. Notwithstanding this

¹ This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2011. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

² Companies conducting internal investigations often secure and examine the e-mail communications and computer files of employees who are thought to have relevant information.
policy, employees sometimes make personal use of their computers, including for the purpose of sending personal e-mail messages from their personal or office e-mail accounts. Recently, the employee retained a lawyer to give advice about a potential claim against her employer. When the lawyer knows or reasonably should know that the employee may use a workplace device or system to communicate with the lawyer, does the lawyer have an ethical duty to warn the employee about the risks this practice entails?

Discussion

Absent an applicable exception, Rule 1.6(a) requires a lawyer to refrain from revealing “information relating to the representation of a client unless the client gives informed consent.” Further, a lawyer must act competently to protect the confidentiality of clients’ information. This duty, which is implicit in the obligation of Rule 1.1 to “provide competent representation to a client,” is recognized in two Comments to Rule 1.6. Comment [16] observes that 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 [17] states in part: “When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.... Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.”

This Committee has recognized that these provisions of the Model Rules require lawyers to take reasonable care to protect the confidentiality of client information, including information contained in e-mail communications made in the course of a representation. In ABA Op. 99-413 (1999) (“Protecting the Confidentiality of Unencrypted E-Mail”), the Committee concluded that, in general, a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating Model Rule 1.6(a) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The opinion, nevertheless, caucasion lawyers to consult with their clients and follow their clients’ instructions as to the mode of transmitting highly sensitive information relating to the clients’ representation. It found that particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters.

Clients may not be afforded a “reasonable expectation of privacy” when they use an employer’s computer to send e-mails to their lawyers or receive e-mails from their lawyers. Judicial decisions illustrate the risk that the employer will read these e-mail communications and seek to use them to the employee’s disadvantage. Under varying facts, courts have reached different conclusions about whether an employee’s client-lawyer communications located on a workplace computer or system are privileged, and the law appears to be evolving. This Committee’s mission does not extend to interpreting the substantive law, and

---

3 See, e.g., ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 08-451 (2008) (Lawyer’s Obligations When Outsourcing Legal and Nonlegal Support Services) (“the obligation to ‘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’” requires a lawyer outsourcing legal work “to recognize and minimize the risk that any outside service provider may inadvertently -- or perhaps even advertently -- reveal client confidential information to adverse parties or to others who are not entitled to access ... [and to] verify that the outside service provider does not also do work for adversaries of their clients on the same or substantially related matters.”).

therefore we express no view on whether, and in what circumstances, an employee’s communications with counsel from the employee’s workplace device or system are protected by the attorney-client privilege. Nevertheless, we consider the ethical implications posed by the risks that these communications will be reviewed by others and held admissible in legal proceedings. Given these risks, a lawyer should ordinarily advise the employee-client about the importance of communicating with the lawyer in a manner that protects the confidentiality of e-mail communications, just as a lawyer should avoid speaking face-to-face with a client about sensitive matters if the conversation might be overheard and should warn the client against discussing their communications with others. In particular, as soon as practical after a client-lawyer relationship is established, a lawyer typically should instruct the employee-client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney-client communications, because even seemingly ministerial communications involving matters such as scheduling can have substantive ramifications.

The time at which a lawyer has an ethical obligation under Rules 1.1 and 1.6 to provide advice of this nature will depend on the circumstances. At the very least, in the context of representing an employee, this ethical obligation arises when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party. Considerations tending to establish an ethical duty to protect client-lawyer confidentiality by warning the client against using a business device or system for substantive e-mail communications with counsel include, but are not limited to, the following: (1) that the client has engaged in, or has indicated an intent to engage in, e-mail communications with counsel; (2) that the client is employed in a position that would provide access to a workplace device or system; (3) that, given the circumstances, the employer or a third party has the ability to access the e-mail communications; and (4) that, as far as the lawyer knows, the employer’s internal policy and the jurisdiction’s laws do not clearly protect the privacy of the employee’s personal e-mail communications via a business device or system. Unless a lawyer has reason to believe otherwise, a lawyer ordinarily should assume that an employer’s internal policy allows for access to the employee’s e-mails sent to or from a workplace device or system.

The situation in the above hypothetical is a clear example of where failing to warn the client about the risks of e-mailing communications on the employer’s device can harm the client, because the employment dispute would give the employer a significant incentive to access the employee’s workplace e-mail and the employer’s internal policy would provide a justification for doing so. The obligation arises once the lawyer has reason to believe that there is a significant risk that the client will conduct e-mail communications with the lawyer using a workplace computer or other business device or via the employer’s e-mail account. This possibility ordinarily would be known, or reasonably should be known, at the outset of the representation. Given the nature of the representation—an employment dispute—the lawyer is on notice that the employer may search the client’s electronic correspondence. Therefore, the lawyer must ascertain, unless the answer is already obvious, whether there is a significant risk that the client will use a business e-mail address for personal communications or whether the employee’s position entails using an employer’s device. Protective measures would include the lawyer refraining from sending e-mails

inapplicable to communications with counsel using workplace computer); Scott v. Beth Israel Medical Center, Inc., 847 N.Y.S.2d 436, 440-43 (N.Y. Sup. Ct. 2007) (privilege inapplicable to employer’s communications with counsel via employer’s e-mail system); Long v. Marubeni Am. Corp., No. 05CIV.639(GEL)(KNF), 2006 WL 2998671, at *3-4 (S.D.N.Y. Oct. 19, 2006) (e-mails created or stored in company computers were not privileged, notwithstanding use of private password-protected e-mail accounts); Kaufman v. SunGard Inv. Sys., No. 05-CV-1236 (JLL), 2006 WL 1307882, at *4 (D.N.J. May 10, 2006) (privilege inapplicable to communications with counsel using employer’s network).

For a discussion of a lawyer’s duty when receiving a third party’s e-mail communications with counsel, see ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-460 (2011) (Duty when Lawyer Receives Copies of a Third Party’s E-mail Communications with Counsel).

This opinion principally addresses e-mail communications, which are the most common way in which lawyers communicate electronically with clients, but it is equally applicable to other means of electronic communications.
to the client’s workplace, as distinct from personal, e-mail address,\(^7\) and cautioning the client against using 
a business e-mail account or using a personal e-mail account on a workplace computer or device at least for
substantive e-mails with counsel.

As noted at the outset, the employment scenario is not the only one in which attorney-client
electronic communications may be accessed by third parties. A lawyer sending or receiving substantive
communications with a client via e-mail or other electronic means ordinarily must warn the client about the
risk of sending or receiving electronic communications using a computer or other device, or e-mail account,
to which a third party may gain access. The risk may vary. Whenever a lawyer communicates with a client
by e-mail, the lawyer must first consider whether, given the client’s situation, there is a significant risk that
third parties will have access to the communications. If so, the lawyer must take reasonable care to protect
the confidentiality of the communications by giving appropriately tailored advice to the client.

---

\(^7\) Of course, if the lawyer becomes aware that a client is receiving personal e-mail on a workplace computer
or other device owned or controlled by the employer, then a duty arises to caution the client not to do so,
and if that caution is not heeded, to cease sending messages even to personal e-mail addresses.
Formal Opinion 11-460  August 4, 2011

Duty when Lawyer Receives Copies of a Third Party’s E-mail Communications with Counsel

When an employer’s lawyer receives copies of an employee’s private communications with counsel, which the employer located in the employee’s business e-mail file or on the employee’s workplace computer or other device, neither Rule 4.4(b) nor any other Rule requires the employer’s lawyer to notify opposing counsel of the receipt of the communications. However, court decisions, civil procedure rules, or other law may impose such a notification duty, which a lawyer may then be subject to discipline for violating. If the law governing potential disclosure is unclear, Rule 1.6(b)(6) allows the employer’s lawyer to disclose that the employer has retrieved the employee’s attorney-client e-mail communications to the extent the lawyer reasonably believes it is necessary to do so to comply with the relevant law. If no law can reasonably be read as establishing a notification obligation, however, then the decision whether to give notice must be made by the employer-client, and the employer’s lawyer must explain the implications of disclosure, and the available alternatives, as necessary to enable the employer to make an informed decision.

This opinion addresses a lawyer’s ethical duty upon receiving copies of e-mails between a third party and the third party’s lawyer. We explore this question in the context of the following hypothetical scenario.

After an employee files a lawsuit against her employer, the employer copies the contents of her workplace computer for possible use in defending the lawsuit, and provides copies to its outside counsel. Upon review, the employer’s counsel sees that some of the employee’s e-mails bear the legend “Attorney-Client Confidential Communication.” Must the employer’s counsel notify the employee’s lawyer that the employer has accessed this correspondence?

When an employer’s lawyer receives copies of an employee’s private communications with counsel, which the employer located in the employee’s business e-mail file or on the employee’s workplace computer or other device, the question arises whether the employer’s lawyer must notify opposing counsel pursuant to Rule 4.4(b). This Rule provides: “A lawyer who receives a document relating to the representation of the lawyer’s client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.”

Rule 4.4(b) does not expressly address this situation, because e-mails between an employee and his or her counsel are not “inadvertently sent” by either of them. A “document [is] inadvertently sent” to someone when it is accidentally transmitted to an unintended recipient, as occurs when an e-mail or letter is misaddressed or when a document is accidentally attached to an e-mail or accidentally included among other documents produced in discovery. But a document is not “inadvertently sent” when it is retrieved by a third person from a public or private place where it is stored or left.

The question remains whether Rule 4.4(b) implicitly addresses this situation. In several cases, courts have found that Rule 4.4(b) or its underlying principle requires disclosure in analogous situations, such as when “confidential documents are sent intentionally and without permission.”

1 This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2011. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

2 For a discussion of the employee’s lawyer’s obligation to take reasonable steps to prevent a situation such as this from arising, see ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011) (Duty to Protect the Confidentiality of E-mail Communications With One’s Client).

990 A.2d 650, 665 (N.J. 2010), the court found that the employer’s lawyer in an employment litigation violated the state’s version of Rule 4.4(b) by failing to notify the employee’s counsel that the employer had downloaded and intended to use copies of pre-suit e-mail messages exchanged between the employee and her lawyers. 5

Since Rule 4.4(b) was added to the Model Rules, this Committee twice has declined to interpret it or other rules to require notice to opposing counsel other than in the situation that Rule 4.4(b) expressly addresses. 6 In ABA Formal Op. 06-442 (2006), we considered whether a lawyer could properly review and use information embedded in electronic documents (i.e., metadata) received from opposing counsel or an adverse party. We concluded, contrary to some other bar association ethics committees, that the Rule did not apply. We reasoned that “the recent addition of Rule 4.4(b) identifying the sole requirement of providing notice to the sender of the receipt of inadvertently sent information [was] evidence of the intention to set no other specific restrictions on the receiving lawyer’s conduct.” 7 Likewise, in ABA Formal Op. 06-440, this Committee found that Rule 4.4(b) does not obligate a lawyer to notify opposing counsel that the lawyer has received privileged or otherwise confidential materials of the adverse party from someone who was not authorized to provide the materials, if the materials were not provided as “the

lawyer of receipt as matter of compliance with ethics rules).

4 The New Jersey rule provided: “[a] lawyer who receives a document and has reasonable cause to believe that the document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender, and return the document to the sender.” New Jersey Rule of Professional Conduct 4.4(b) (2004).

5 The Stengart court found that the employee “had an objectively reasonable expectation of privacy” in the e-mails based on the fact that the employee “could reasonably expect that e-mail communications with her lawyer through her personal account would remain private, and that sending and receiving them via a company laptop did not eliminate the attorney-client privilege that protected them.” 990 A.2d at 655. In contrast, other decisions arising in different factual situations have found that the attorney-client privilege did not protect client-lawyer communications downloaded by an employer from a computer used by its employees. These other decisions have not suggested that the employer’s lawyer had a notification duty when the employer provided copies of the employee’s attorney-client communications to the employer’s lawyer. See, e.g., Long v. Marubeni Am. Corp., No. 05-CIV-639(GEL)(KNF), 2006 WL 2998671, at *4 (S.D.N.Y. Oct. 19, 2006); Kaufman v. SunGard Inv. Sys., No. 05-CV-1236 (JLL), 2006 WL 1307882, at *3 (D.N.J. May 9, 2006); Scott v. Beth Israel Medical Center, Inc., 847 N.Y.S.2d 436, 444 (Sup. Ct. 2007). 6 One might argue, for example, that the lawyer is prohibited from reading or using the e-mails by any of several other rules. These include Rule 4.4(a), which requires lawyers to refrain from using “methods of obtaining evidence that violate [a third person’s] legal rights,” and which, according to the accompanying comment, fords “unwarranted intrusions into privileged relationships, such as the client-lawyer relationship.” These also include Rule 8.4(c), which forbids “conduct involving dishonesty, fraud, deceit or misrepresentation,” and Rule 8.4(d), which forbids “conduct that is prejudicial to the administration of justice.”

7 ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 06-442 (2006) (Review and Use of Metadata). Prior to the adoption of Rule 4.4(b) in February 2002, this Committee had issued opinions addressing a lawyer’s obligations upon receiving materials of an adverse party on an unauthorized basis when the lawyer knew that the materials were privileged or confidential, and addressing a lawyer’s obligations when the opposing party inadvertently disclosed privileged or confidential materials. See ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 94-382 (1994) (Unsolicited Receipt of Privileged or Confidential Materials), in FORMAL AND INFORMAL ETHICS OPINIONS 1983-1998 (ABA 2000) at 233; ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 92-368 (1992) (Inadvertent Disclosure of Confidential Materials), id. at 140. The Committee concluded that the lawyer’s obligations implicitly derived from other law and from provisions such as Rule 8.4 (prohibiting “conduct involving dishonesty, fraud, deceit or misrepresentation” and conduct “prejudicial to the administration of justice”) that did not expressly address these situations. Id. at 144-49, 234. However, the Committee withdrew both of these opinions following the adoption of Rule 4.4(b). See ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 06-440 (2006) (Unsolicited Receipt of Privileged or Confidential Materials: Withdrawal of Formal Opinion 94-382); ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 05-437 (2005) (Inadvertent Disclosure of Confidential Materials: Withdrawal of Formal Opinion 92-368).
result of the sender’s inadvertence.”

We noted that other law might prevent the receiving lawyer from retaining and using the materials, and that the lawyer might be subject to sanction for doing so, but concluded that this was “a matter of law beyond the scope of Rule 4.4(b).”

To say that Rule 4.4(b) and other rules are inapplicable is not to say that courts cannot or should not impose a disclosure obligation in this context pursuant to their supervisory or other authority. As Comment [2] to Rule 4.4(b) observes, “this Rule does not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been wrongfully obtained by the sending person.” Pursuant to their supervisory authority, courts may require lawyers in litigation to notify the opposing counsel when their clients provide an opposing party’s attorney-client confidential communications that were retrieved from a computer or other device owned or possessed by the client. Alternatively, the civil procedure rules governing discovery in the litigation may require the employer to notify the employee that it has gained possession of the employee’s attorney-client communications. Insofar as courts recognize a legal duty in this situation, as the court in Stengart has done, a lawyer may be subject to discipline, not just litigation sanction, for knowingly violating it. However, the Model Rules do not independently impose an ethical duty to notify opposing counsel of the receipt of private, potentially privileged e-mail communications between the opposing party and his or her counsel.

When the law governing potential disclosure is unclear, the lawyer need not risk violating a legal or ethical obligation. The fact that the employer-client has obtained copies of the employee’s e-mails is “information relating to the representation of [the] client” that must be kept confidential under Rule 1.6(a) unless there is an applicable exception to the confidentiality obligation or the client gives “informed consent” to disclosure. Rule 1.6(b)(6) permits a lawyer to “reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary ... to comply with other law or a court order.” Rule 1.6(b)(6) allows the employer’s lawyer to disclose that the employer has retrieved the employee’s attorney-client e-mail communications to the extent he or she reasonably believes it is necessary to do so to comply with the relevant law, even if the legal obligation is not free from doubt. On the other hand, if no law can reasonably be read as establishing a reporting obligation, then the decision whether to give notice must be made by the employer-client. Even when there is no clear notification obligation, it often will be in the employer-client’s best interest to give notice and obtain a judicial ruling as to the admissibility of the employee’s attorney-client communications before attempting to use them and, if possible, before the employer’s lawyer reviews them. This course minimizes the risk of disqualification or other sanction if the court ultimately concludes that the opposing party’s communications with counsel are privileged and inadmissible. The employer’s lawyer must explain these and other implications of disclosure, and the available alternatives, as necessary to enable the employer to make an informed decision. See Rules 1.0(e) (Terminology, “informed consent”), 1.4(b) (“A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation”), and 1.6(a) (“lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by [the exceptions under Rule 1.6(b)]”).

8 Supra n. 7.

9 Id. A recent article suggests that Rule 1.15(d) imposes a notification duty in the analogous situation in which a lawyer comes into possession of physical documents that appear to have been wrongly procured from another party. Brian S. Faughan & Douglas R. Richmond, “Model Rule 1.15: The Elegant Solution to the Problem of Purloined Documents,” 26 ABA/BNA LAW. MAN. PROF. CONDUCT 623 (Oct. 13, 2010). Rule 1.15(d) provides, in pertinent part: “Upon receiving ... property in which a client or third person has an interest, a lawyer shall promptly notify the client or third person.” The provision arises out of the lawyer’s fiduciary duty to safeguard money and property belonging to another and entrusted to the lawyer. Regardless of whether this rule may apply when stolen physical items come into a lawyer’s possession, we do not believe it applies when an organizational client gives its lawyer copies of documents that were on a computer in the client’s lawful possession for the lawyer’s potential use in litigation. What is at stake is not the third party’s proprietary interest in the copies of e-mails but the third party’s confidentiality interest, which Rule 1.15(d) does not address.


11 See, e.g., Rule 3.4(c)(“A lawyer shall not knowingly disobey an obligation under the rules of a tribunal except for an open refusal based on an assertion that no valid obligation exists.”).
PROTECTING YOUR CLIENT’S CONFIDENTIAL INFORMATION: ESI, PRIVILEGE, AND FRE 502

ABA Center For Professional Responsibility
41st Annual National Conference on Professional Responsibility

May 29, 2015

David M. Greenwald

dgreenwald@janner.com
Topics

- The Ethical Backdrop

- FRE 502(a): Limitations on Scope of Waiver

- FRE 502(d): The Power of a Federal Court to Provide Protection Against Waiver and Certainty as to Scope of Waiver

- FRE 502(b): A costly Alternative to a FRE 502(d) Order

- Practical alternatives for privilege logging
Duty of Confidentiality

ABA Model Rule of Professional Conduct 1.6(a):

“A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b) [certain specific exceptions, e.g., to prevent death or substantial bodily harm].

ABA Model Rule of Professional Conduct 1.6(c):

“A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”
Duty of Competence

ABA Model Rule of Professional Conduct 1.1:

“A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

ABA Model Rule of Professional Conduct 1.1, comm. 8 (2012):

“To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing legal study and education and comply with all continuing legal education requirements to which the lawyer is subject.”
Duty to Expedite Litigation

ABA Model Rule of Professional Conduct 3.2:

“A lawyer shall make reasonable efforts to expedite litigation consistent with the interests of the client.”

FRCP 1:

“These rules govern the procedure in all civil actions and proceedings in the United States district courts, except as stated in Rule 81. They should be construed and administered to secure the just, speedy, and inexpensive determination of every action and proceeding.”
Duty to Expedite Litigation

FRCP 26(b)(2)(c):

(c) “On a motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

* * *

(iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.”
The Basics: What Law Applies

• **Attorney-Client Privilege**
  – Federal court: choice of law per FRE 501
    • State law in diversity cases
    • Federal common law in federal question cases (even if state claims too)
  – State court: per state choice of law rules
  
    • **CAUTION:** Because state law applies, results can differ state-to-state – if privilege issue arises, should look at applicable state law rather than relying on general rule

• **Work-Product Doctrine**
  – Federal court: per FRCP 26(b)(3) and federal common law
  – Rule 26 analogues in state court
FRE 502: Scope Of Waiver

• **PRE-RULE 502:**
  
  – **AC Privilege:** Subject Matter Waiver
  
  – **WP Protection:** Waiver of WP disclosed and perhaps underlying documents; generally no subject matter waiver
FRE 502

- Eliminates Risk that Inadvertent Waiver Will Lead To Broad Subject Matter Waiver. (FRE 502(a))

- Limits Scope of Waiver for Voluntary Disclosures. (FRE 502(a))

- Enables One Federal Court To Bind All Other Proceedings, State and Federal. (FRE 502(d))

- Enables Parties To Establish Discovery Protocols
  - Claw Back Agreements
  - “Quick Peek” Arrangements
  - Privilege Log Protocols
  - E-Discovery Protocols Regarding Privilege Review
  - Agreement on Scope of ESI Preservation
  - Agreement to Conduct Phased Discovery

- Consider an FRE 502(d) order in all federal litigation.
Rule 502(a)

(a) Disclosure made in a federal proceeding or to a federal office or agency; scope of a waiver. — When the disclosure is made in a federal proceeding or to a federal office or agency and waives the attorney-client privilege or work-product protection, the waiver extends to an undisclosed communication or information in a federal or state proceeding only if:

(1) the waiver is intentional;

(2) the disclosed and undisclosed communications or information concern the same subject matter; and

(3) they ought in fairness to be considered together.
Rule 502(a)

Explanatory Note: Subdivision (a). The rule provides that a voluntary disclosure in a federal proceeding or to a federal office or agency, if a waiver, generally results in a waiver only of the communication or information disclosed; a subject matter waiver (of either privilege or work product) is reserved for those unusual situations in which fairness requires a further disclosure of related, protected information, in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary. Thus, subject matter waiver is limited to situations in which a party intentionally puts protected information into the litigation in a selective, misleading and unfair manner. It follows that an inadvertent disclosure of protected information can never result in a subject matter waiver.
FRE 502 Limitations: “Use” vs. “Disclosure”

• FRE 502 addresses “disclosure” not “use” of privileged information.
• Substantive law regarding “strategic use” unchanged.
  – Direct use of protected information – e.g., producing party’s use as exhibit
    • Potentially creates strategic issues in pre-trial preparation.
• FRE 502(d) order can address use as well as disclosure of privileged information.
  – For example, FRE 502(d) order may provide that the scope of waiver resulting from affirmative use of otherwise privileged information by the Producing Party will be governed by FRE 502(a).
Rule 502(b)

(b) Inadvertent disclosure. – When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if:

(1) the disclosure is inadvertent;
(2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and
(3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Fed.R.Civ.P. 26(b)(5)(B).

Parade of Horribles

• May require proof of:
  – Inadverternce
  – Reasonableness
  – Promptness

• An expensive and unnecessary side show

• FRE 502(d) can prevent this expense and distraction.
Rule 502(d), (e) and (f)

(d) **Controlling effect of a court order.** – A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court – in which event the disclosure is also not a waiver in any other federal or state proceeding.

(e) **Controlling effect of a party agreement.** – An agreement on the effect of disclosure in a federal proceeding is binding only on the parties to the agreement, unless it is incorporated into a court order.

(f) **Controlling effect of this rule.** Notwithstanding Rules 101 and 1101, this rule applies to state proceedings and to federal court-annexed and federal court-mandated arbitration proceedings, in the circumstances set out in the rule. And notwithstanding Rule 501, this rule applies even if state law provides the rule of decision.
Disclosures to Federal Offices and Agencies

- This provision of FRE 502(a) applies even in absence of “federal proceeding.”
- Congress a federal office or agency
- The protections of FRE 502(a) regarding disclosure to federal offices and agencies apply even if the issue is first raised in a state court proceeding, and state law would not otherwise provide the same protection. (See FRE 502(f).)
Disclosures To Federal Agencies

• Before disclosing information to Federal agency in informal investigation, request:
  – Agreement that FRE 502 applies to the disclosures
  – That disclosure of privileged documents does not waive as to undisclosed documents
  – That the company may claw back documents it determines are privileged
  – That the government will seek to have a FRE 502(d) order entered if there is a subsequent federal proceeding

• Request same agreements if responding to subpoena. If no agreement, consider motion to quash or for protective order.

• When disclosing: characterize disclosures as not including privileged or protected information where appropriate.
Implied Waiver – At Issue Waiver

• “At Issue” Waiver occurs where a party raises an issue the effective rebuttal of which requires inquiry into privileged communications.

• Requires affirmative act; just denying allegations typically does not waive privilege.

• Examples of “at issue” waiver:
  – Asserting affirmative defense of “Reasonable Investigation”
  – Asserting reliance on Advice of Counsel
  – Asserting Ineffective Assistance of Counsel
  – Asserting Attorney Malpractice
At Issue Waiver Generally

Different Approaches To “At Issue” Waiver:

• **Broad Approach:** *Hearn v. Rhay,* 68 F.R.D. 574 (E.D. Wash 1975)
  
  (1) Party asserting privilege has taken an affirmative act that
  
  (2) Makes protected information relevant to the case, and
  
  (3) Application of privilege would deny opposing party access to information vital to the defense.

• **Narrower Approach:** *In re Erie County,* 546 F.3d 222 (2d Cir. 2008)
  
  Some showing that opposing party is relying on privileged communications as a claim or defense or as an element of a claim or defense (e.g., where state of mind or good faith are put at issue).
Hypothetical (moderate-sized production)

1 Million Documents

- 50,000 documents produced
- 50,000 documents reviewed for privilege

50 privileged documents produced voluntarily and with intent to waive as to those specific documents

500 privileged emails tagged properly by review team, but inadvertently disclosed by third party vendor

Inadvertently produced 150 sensitive AC privileged emails due to erroneous tagging by review team
UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Rule 502(d) ORDER

ANDREW J. PECK, United States Magistrate Judge:

1. The production of privileged or work-product protected documents, electronically
stored information ("ESI") or information, whether inadvertent or otherwise, is not a waiver of the
privilege or protection from discovery in this case or in any other federal or state proceeding. This
Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence
502(d).

2. Nothing contained herein is intended to or shall serve to limit a party's right to
conduct a review of documents, ESI or information (including metadata) for relevance,
responsiveness and/or segregation of privileged and/or protected information before production.

SO ORDERED.

Dated: New York, New York
[DATE]

Andrew J. Peck
United States Magistrate Judge

Copies by ECF to: All Counsel, Judge
Model Draft Of A Rule 502(d) Order*

Form of Order Implementing Rule 502(d) of the Federal Rules of Evidence When Information Protected by the Attorney-Client Privilege or as Attorney Work-Product is Produced by a Party.

(a) No Waiver by Disclosure. This order is entered pursuant to Rule 502(d) of the Federal Rules of Evidence. Subject to the provisions of this Order, if a party (the “Disclosing Party”) discloses information in connection with the pending litigation that the Disclosing Party thereafter claims to be privileged or protected by the attorney-client privilege or work product protection (“Protected Information”), the disclosure of that Protected Information will not constitute or be deemed a waiver or forfeiture – in this or any other action – of any claim of privilege or work product protection that the Disclosing Party would otherwise be entitled to assert with respect to the Protected Information and its subject matter.

(b) Notification Requirements; Best Efforts of Receiving Party. A Disclosing Party must promptly notify the party receiving the Protected Information (“the Receiving Party”), in writing, that it has disclosed that Protected Information without intending a waiver by the disclosure. Upon such notification, the Receiving Party must – unless it contests the claim of attorney-client privilege or work product protection in accordance with paragraph (c) – promptly (i) notify the Disclosing Party that it will make best efforts to identify and return, sequester or destroy (or in the case of electronically stored information, delete) the Protected Information and any reasonably accessible copies it has and (ii) provide a certification that it will cease further review, dissemination, and use of the Protected Information. Within five business days of receipt of the notification from the Receiving Party, the Disclosing Party must explain as specifically as possible why the Protected Information is privileged. [For purposes of this Order, Protected Information that has been stored on a source of electronically stored information that is not reasonably accessible, such as backup storage media, is sequestered. If such data is retrieved, the Receiving Party must promptly take steps to delete or sequester the restored protected information.]

* This model Rule was drafted by the participants of the Symposium on Rule 502, held on October 5, 2012, at Charleston School of Law in Charleston, South Carolina.
(c) Contesting Claim of Privilege or Work Product Protection. If the Receiving Party contests the claim of attorney-client privilege or work product protection, the Receiving Party must—within five business days of receipt of the notice of disclosure—move the Court for an Order compelling disclosure of the information claimed as unprotected (a “Disclosure Motion”). The Disclosure Motion must be filed under seal and must not assert as a ground for compelling disclosure the fact or circumstances of the disclosure. Pending resolution of the Disclosure Motion, the Receiving Party must not use the challenged information in any way or disclose it to any person other than those required by law to be served with a copy of the sealed Disclosure Motion.

(d) Stipulated Time Periods. The parties may stipulate to extend the time periods set forth in paragraphs (b) and (c).

(e) Attorney’s Ethical Responsibilities. Nothing in this order overrides any attorney’s ethical responsibilities to refrain from examining or disclosing materials that the attorney knows or reasonably should know to be privileged and to inform the Disclosing Party that such materials have been produced.

(f) Burden of Proving Privilege or Work-Product Protection. The Disclosing Party retains the burden – upon challenge pursuant to paragraph (c) – of establishing the privileged or protected nature of the Protected Information.

(g) In camera Review. Nothing in this Order limits the right of any party to petition the Court for an in camera review of the Protected Information.

(h) Voluntary and Subject Matter Waiver. This Order does not preclude a party from voluntarily waiving the attorney-client privilege or work product protection. The provisions of Federal Rule 502(a) apply when the Disclosing Party uses or indicates that it may use information produced under this Order to support a claim or defense.

(i) Rule 502(b)(2). The provisions of Federal Rule of Evidence 502(b)(2) are inapplicable to the production of Protected Information under this Order.

* This model Rule was drafted by the participants of the Symposium on Rule 502, held on October 5, 2012, at Charleston School of Law in Charleston, South Carolina.
The inadvertent production of Privileged Information, shall not waive the attorney-client privilege or the work product protection, provided that the producing party makes a good-faith representation, in writing to the receiving party, that such production was inadvertent or mistaken. In addition, the fact that a document was inadvertently produced shall not be used in any manner as evidence in support of any such alleged waiver.

[Order does not provide that request for claw back be done “promptly”.]
2. NON-WAIVER AND CLAW BACK PROTOCOL (FRE 502(d))

2.1 Non-Waiver By Production. Production of documents and ESI in this case shall be without prejudice to and shall not waive, for purposes of this case or otherwise, any attorney-client privilege or work product protection that otherwise would apply.

2.2 Time For Asserting Privilege And Protection. A producing party may assert privilege or protection over produced documents and ESI at any time by notifying the receiving party(ies) in writing of the assertion of privilege or protection, except that:

(a) Affirmative use of ESI or a document by the producing party in the case waives privilege and protection with respect to it, and of other ESI and documents to the extent provided by Federal Rules of Evidence, Rule 502(a); and

(b) Upon use in the case by another of ESI or a document that was produced by a party, that producing party must promptly assert any claimed privilege and/or protection over it and request return or destruction thereof.
Avoiding Pitfalls In FRE 502(d) Orders

Avoid using FRE 502(b) language in FRE 502(d) orders:

- “Inadvertent”
- “Reasonable”
- “Prompt”

Include provision in FRE 502(d) order that states that provisions of FRE 502(b) are inapplicable to the production of Protected Information pursuant to the FRE 502(d) order.

Provide a clear process for claw backs and challenges that obviates need for motion practice except where the Receiving Party challenges the merits of the Producing Party’s assertion of privilege or protection.
Privilege Logs
Bringing Sanity to the Process

- FRCP 26(b)(5)(A) does not require document-by-document logs.
- 1993 Advisory Committee Note suggests document-by-document logs may be unduly burdensome, particularly “if the items can be described by categories.”
- An increasing number of courts have allowed alternative logging approaches.
Privilege Logs

(b) **Categorical Approach or Document-By-Document Review.**

(1) The preference in the Commercial Division is for the parties to use **categorical designations**, where appropriate, to reduce the time and costs associated with preparing privilege logs. The parties are expected to address such considerations in good faith as part of the meet and confer process (see paragraph (a) above) and to agree, where possible, to employ a categorical approach to privilege designations. The parties are encouraged to utilize any reasoned method of organizing the documents that will facilitate an orderly assessment as to the appropriateness of withholding documents in the specified category.

* Rule 11-b of Section 202.70(g) of Rules of Practice for the New York Commercial Division (adopted July 8, 2014, effective September 2, 2014).
Privilege Logs

(b) **Categorical Approach or Document-By-Document Review***

(2) In the event the requesting party refuses to permit a **categorical approach**, and instead insists on a document-by-document listing on the privilege log, then unless the Court deems it appropriate to issue a protective order pursuant to CPLR 3103 based upon the facts and circumstances before it, the requirements set forth in CPLR 3122 shall be followed. In that circumstance, however, **the producing party, upon a showing of good cause, may apply to the court for the allocation of costs, including attorneys’ fees**, incurred with respect to preparing the document-by-document log. Upon good cause shown, the court may allocate the costs to the requesting party.

* Rule 11-b of Section 202.70(g) of Rules of Practice for the New York Commercial Division (adopted July 8, 2014), effective September 2, 2014).
Practical Approaches to Logging

- Agree on logging protocol at the beginning of the case, ideally at 26(f) conference.
- Agree on what will not be logged:
  - Documents dated after filing of action or some prior date
  - Documents before an agreed upon date
  - Documents relating to specific attorneys, e.g., those who clearly do only litigation work
- Consider logging by category.
- Consider starting with objective privilege logs.
  - Can reserve right to request more detail
- Identify categories of documents that will be logged in more detail, e.g.:
  - In-house attorneys where expect dual business and legal roles
  - Other specific custodians
  - Specific periods of time
Practical Approaches to Logging (cont’d)

• Agree on protocol for testing documents not logged in detail.

• Agree on method for asserting privilege over particular categories, e.g., affidavit support for:
  – Role of in-house counsel
  – Basis for Joint Defense or Common Interest Agreement
  – Basis for date triggering work product protection
    • Consider whether date selected for WP purposes differs materially from date of document preservation/ litigation hold notices.
S14Y0661. IN THE MATTER OF MARGRETT A. SKINNER.

PER CURIAM.

The State Bar of Georgia made a formal complaint against respondent Margrett A. Skinner (State Bar No. 650748), alleging violations of Rules 1.3, 1.4, 1.6, and 1.16 of the Georgia Rules of Professional Conduct. Prior to an evidentiary hearing on the formal complaint, Skinner filed a petition for voluntary discipline, admitting that she violated Rule 1.6 by improperly disclosing confidential information about a former client, and in which she agreed to accept a Review Panel reprimand for the violation. The special master and the State Bar recommended that we accept the petition for voluntary discipline. We rejected the petition, however, noting that a Review Panel reprimand is “the mildest form of public discipline authorized . . . for the violation of Rule 1.6,” In the Matter of Skinner, 292 Ga. 640, 642 (740 SE2d 171) (2013), and noting as well that the petition and accompanying record did not “reflect the nature of the disclosures (except that they concern [unspecified] personal and confidential information) or the actual or potential harm to the
client as a result of the disclosures.” Id. at 642, n. 6. Following our rejection of the petition, the special master conducted an evidentiary hearing, and he made his report and recommendation on December 18, 2013, in which he found that Skinner violated Rules 1.4 and 1.6 but not Rules 1.3 and 1.16.¹ Neither party sought review of the report by the Review Panel, and the matter is again before this Court for decision.

In his report, the special master found that a client retained Skinner in July 2009 to represent her in an uncontested divorce, and she paid Skinner $900, including $150 for the filing fee. For six weeks, the client did not hear anything from Skinner, and after multiple attempts to contact Skinner, the client finally was able to reach Skinner again in October 2009. At that point, Skinner informed the client that Skinner had lost the paperwork that the client had given to Skinner in July. Skinner and the client then met again, and Skinner finally began to draft pleadings for the divorce. The initial drafts of the pleadings had multiple errors, and Skinner and the client exchanged several drafts and communicated by e-mail about the status of the case in October and early

---

¹ Joseph A. Boone was appointed as special master in this matter.
November 2009. Those communications concluded by mid-November, and Skinner and the client had no more communications until March 18, 2010, when the client reported to Skinner that her husband would not sign the divorce papers without changes. In April 2010, both the client and her husband signed the papers.

A disagreement developed about the fees and expenses of the divorce. Skinner asked the client for an additional $185 for certain travel expenses and the filing fee. In April and early May 2010, Skinner and the client exchanged several e-mails about the request for additional money. Then, on May 18, the client informed Skinner that she had hired another lawyer to complete her divorce, and she asked Skinner to deliver her file to new counsel and to refund $750. Skinner replied that she would not release the file unless she were paid. Although Skinner eventually refunded $650 to the client, Skinner never delivered the file to new counsel, contending that it only contained her “work product.” New counsel completed the divorce within three months of her engagement.

Around this time, the client posted negative reviews of Skinner on three consumer Internet pages. When Skinner learned of the negative reviews, she
posted a response on the Internet, a response that contained personal and confidential information about her former client that Skinner had obtained in the course of her representation of the client. In particular, Skinner identified the client by name, identified the employer of the client, stated how much the client had paid Skinner, identified the county in which the divorce had been filed, and stated that the client had a boyfriend. The client filed a grievance against Skinner, and in response to the grievance, Skinner said in August 2011 that she would remove her posting from the Internet. It was not removed, however, until February 2012.

The special master found that Skinner violated Rule 1.4 when she failed between July and October 2010 to keep her client reasonably informed of the status of the divorce, and the special master found that Skinner violated Rule 1.6 when she disclosed confidential information about her client on the Internet. The special master found no violation of Rules 1.3 and 1.16.\(^2\) Turning to the

\(^2\) About Rule 1.16, the special master reported his belief that Skinner technically violated the rule by failing to deliver the file of her client to successor counsel based on a mistaken belief that signed pleadings in the file belonged to her as “work product.” See Formal Advisory Opinion 87-5; Swift, Currie, McGhee & Hiers v. Henry, 276 Ga. 571 (581 SE2d 37) (2003). But the special master did not actually find a violation nor recommend any discipline under Rule 1.16. The special master reported that he made no such finding or recommendation because there was no clear and convincing evidence of prejudice, insofar
appropriate discipline for these violations, the special master noted that Skinner had substantial experience as a practicing lawyer — she was admitted to the Bar in 1987 — which is an aggravating circumstance. The special master also found, however, a number of mitigating circumstances, including that Skinner had no prior discipline, the absence of a dishonest or selfish motive for her improper conduct, that she refunded a substantial portion of her fee to the client even after doing work for the client, that she accepted responsibility for her misconduct by filing a petition for voluntary discipline, that she otherwise was cooperative in the disciplinary proceedings, and that she had expressed remorse for her misconduct. In addition, the special master found as mitigation that Skinner experienced a number of personal problems during her representation of the client and the subsequent time that she posted the confidential information about her client on the Internet, including colon surgery in April 2010, the diagnosis of both her mother and father with cancer (she was their primary caregiver), and the death of her father. For both violations, the special master recommended a public reprimand, with the additional condition that Skinner "be instructed to _______________________

as the client already had the documents contained in the file. As to the retention of unearned fees, the special master found the issue moot in light of the refund of $650 to the client.
take advantage of the State Bar’s Law Practice Management services and recommendations with respect to internal office procedures, client files, and case tracking procedures.”

We have reviewed carefully the record and the very detailed report of the special master, and we agree with his recommendation of a public reprimand, as well as the additional condition that Skinner be instructed to take advantage of the State Bar’s Law Practice Management services and recommendations with respect to internal office procedures, client files and case tracking procedures. See In the Matter of Adams, 291 Ga. 173 (729 SE2d 313) (2012). Although other jurisdictions occasionally have disciplined lawyers more severely for improper disclosures of client confidences, we note that those cases involved numerous clients and violations of other rules, see Office of Lawyer Regulation v. Peshek, 334 Wis.2d 373 (798 NW2d 879 (2011) (60-day suspension), or the disclosure of especially sensitive information that posed serious harm or potential harm to the client, see In re Quillinan, 20 DB Rptr. 288 (Ore. Disp. Bd. 2006) (90-day suspension), available at www.osbar.org/_docs/dbreport/dbr20.pdf. In this case, the improper disclosure of confidential information was isolated and limited to a single client, it does not
appear that the information worked or threatened substantial harm to the interests of the client, and there are significant mitigating circumstances. Accordingly, we hereby order that Skinner receive a public reprimand in accordance with Bar Rules 4-102 (b) (3) and 4-220 (c), and we order that she consult with the Law Practice Management Program of the State Bar as set forth above and implement its suggestions in her law practice.

Public reprimand. All the Justices concur.

Decided May 19, 2014.

Public reprimand.

Paula J. Frederick, General Counsel State Bar, Jenny K. Mittelman, Assistant General Counsel State Bar, for State Bar of Georgia.

William H. Noland, for Skinner.
In the Matter of:

BETTY TSAMIS, Attorney-Respondent, No. 6288664.

Commission No. 2013PR0001

JOINT STIPULATION AND RECOMMENDATION FOR A REPRIMAND BY THE HEARING BOARD

Jerome Larkin, Administrator of the Attorney Registration and Disciplinary Commission, by his attorney, Gina M. Abbatemarco, and Respondent Betty Tsamis, by her attorneys, George B. Collins and Kathryne Hayes, stipulate that Respondent violated Rules 1.6(a), 1.15(d), and 4.4 of the 2010 Illinois Rules of Professional Conduct and, as discipline, recommend that she be administered a reprimand by the Hearing Board, pursuant to Supreme Court Rule 770(h) and Commission Rule 282. In support of that recommendation, the Administrator and Respondent stipulate as follows:

I. STIPULATED FINDINGS OF FACT

A. Count I- Conversion of Klimek settlement

The Administrator and Respondent stipulate that the evidence in Count I of the Administrator's complaint would establish the following facts:

1. In or about February 2008, Respondent agreed to represent Kris Klimek ("Klimek") in a personal injury claim for injuries Klimek sustained arising from a fall that took place on the premises of Malibu East Condominiums in Chicago, Illinois. In August 2011, Respondent settled Klimek's claim for $14,142.68. On or about August 22, 2011, Respondent received three settlement checks from Hartford Insurance Company. The first check was made payable to Respondent in the amount of $4,713.75, and represented payment of her fees pursuant to the fee agreement she had with Klimek. The second check was made payable to
Medicaid/Medicare and Klimek in the amount of $3,942.68 for the purpose of paying claimed liens, with any remaining amount to go to Klimek after the liens had been satisfied. The third check, for $5,486.25, was made payable to Klimek and represented her portion of the proceeds.

2. On September 7, 2011, Respondent deposited the check in the amount of $3,942.68 (which represented the proceeds owed to Klimek and Klimek’s medical providers) into her client trust account at PNC Bank. On December 30, 2011, Respondent disbursed $197.24 to HFS Collections on behalf of Medicaid in satisfaction of its claimed lien. Between September 7, 2011 and February 14, 2012, prior to any disbursement of funds to Medicare or Klimek, Respondent failed to preserve the identity of those funds when she drew the balance in the client trust account below the amount of the check, thereby converting $2,057.54 of the settlement proceeds for her own use. Respondent's bank records show that Respondent's overdraft was the result of her failure to account for credit card fees being charged on the account, and that she had disbursed costs on two client matters in amounts greater than what she had received from those clients. In addition, in January 2012 Respondent deposited a $30,000 settlement check into the account for her client, Linda Griffis. However, on the Griffis settlement statement Respondent incorrectly listed the total she had received as "$33,000." She then disbursed $22,110 to the client and $10,890 to herself in fees, resulting in withdrawal of $3,000 more than had been deposited in connection with that case.

PAGE 3:

3. On April 20, and 26, 2012, respectively, Respondent paid Medicare $717.63 and Klimek the remaining $3,027.81. Klimek’s check for $3,027.81 was later returned due to insufficient funds in Respondent's account. Respondent then deposited $1,000 into the client trust account from her own funds and reissued payment to Klimek.

Count II- Revealing client confidences

4. On September 6, 2012, Respondent agreed to represent Richard Rinehart ("Rinehart") in matters related to Rinehart's securing unemployment benefits from his former employer, American Airlines. American Airlines had terminated Rinehart's employment as a flight attendant because Rinehart allegedly assaulted a fellow flight attendant during a flight. Rinehart paid Respondent $1,500 towards her fee.

5. Between September 6, 2012 and January 16, 2013, Respondent met with Rinehart on at least two occasions and obtained information from Rinehart concerning both his employment history at American Airlines and the alleged incident involving the other flight attendant. Respondent also reviewed Rinehart's personnel file, which she had obtained from American Airlines.


8. On or about February 5, 2013, Rinehart posted a client review of Respondent's services on the
legal referral website AVVO, in which he discussed his dissatisfaction with Respondent's services. On February 7, 2013 and February 8, 2013, Respondent contacted Rinehart by email and requested that Rinehart remove the February 5, 2013 posting about her

from the AVVO website. Rinehart responded that he refused to remove the posting unless he received a copy of his files and a full refund of the $1,500 he had paid Respondent as fees.


10. On April 10, 2013, Rinehart posted a second negative client review of Respondent on AVVO. Respondent replied to his post and revealed confidential information about his case. Respondent's reply to Rinehart's second posting contained information relating to her representation of Rinehart and exceeded what was necessary to respond to Rinehart's accusations.

II. FACTORS IN MITIGATION

11. Respondent was admitted to practice law in Illinois on May 4, 2006 and practices in Chicago where she concentrates her practice in the area of employment and civil rights law. Respondent has no prior disciplinary history. Respondent understands the seriousness of her misconduct and has expressed remorse for it. She has taken steps to more carefully manage her recordkeeping in order to minimize the likelihood of future errors involving her client fund account, so that future overdrafts do not occur. Those steps include reviewing client ledgers and settlement statements with greater detail before issuing checks, and ensuring that she deposits money into the client trust account to account for credit card fees.

12. If this matter proceeded to a hearing, several lawyers and clients would have testified to Respondent's excellent reputation for truth and veracity.

III. RECOMMENDED DISCIPLINE AND LEGAL DISCUSSION

13. The Administrator and Respondent agree and jointly recommend that a reprimand be administered by the Hearing Board pursuant to Supreme Court Rule 770(h) and Commission Rule 282, as the appropriate discipline in this matter. The following cases support that recommendation.

14. In In re Nottage, 2010 PR 00090 (July 20, 2011), the respondent represented a client in a divorce proceeding and negotiated a tentative settlement on behalf of her client. She withdrew while the proceeding was still pending and the client later filed a motion to set aside the settlement, in which she accused the respondent of coercing her to settle the matter. Attempting
to defend herself, the respondent sent the opposing attorney over 500 pages of emails exchanged between herself and the client. The respondent did not seek a court order to release the emails, nor did she take any steps to redact the client's personal information. The hearing board reprimanded the respondent, finding that her conduct had been inconsistent with Rule 1.6. In the instant matter, Respondent also released confidential client information in a public forum in order to counter a client's accusations. Like Nottage, Respondent has expressed remorse for her actions and would present favorable character evidence.

15. In *In re Kreiter*, 95 CH 153 (November 22, 1995) the attorney prepared a personal injury settlement statement which did not disclose the full amount of the fee he was withholding from the settlement proceeds. The Hearing Board found that the statement was neither false nor intentionally misleading. The Board rejected the Administrator's allegation that the respondent had converted funds, but found that the attorney had failed to promptly deliver the funds and that a reprimand was the appropriate sanction for his misconduct. Respondent's conduct is similar to that in *Kreiter*, in that Respondent's errors in properly documenting the amounts of client money she received, as well as her failure to account for the credit card service charges, resulted in her failing to promptly deliver funds to her client. Respondent has also acknowledged her errors as was the case in *Kreiter*.

PAGE 6:

16. Under the circumstances of this case, a reprimand is consistent with prior Hearing Board decisions and is appropriate under the facts and circumstances of this case.

WHEREFORE, the Administrator and Respondent jointly recommend that the Hearing Board issue a reprimand, pursuant to Supreme Court Rule 770(h) and Commission Rule 282.

Respectfully submitted,

Jerome Larkin, Administrator  
Attorney Registration and  
Disciplinary Commission

By: Gina M. Abbatemarco  
Counsel for Administrator  
130 E. Randolph Dr., Suite 1500  
Chicago, IL 60601  
Telephone: (312) 565-2600

Betty Tsamis,  
Respondent

By: George B. Collins  
Counsel for Respondent  
Collins,  
Bargione & Vuckovich  
1 N. LaSalle St., Suite 300  
Chicago, IL 60602
BEFORE THE HEARING BOARD
OF THE
ILLINOIS ATTORNEY REGISTRATION
AND
DISCIPLINARY COMMISSION

In the Matter of:

BETTY TSAMIS,  
Commission No. 2013PR0001

Attorney-Respondent,

No. 6288664.

REPRIMAND

Based upon the agreement and stipulations of the parties, the panel of the Hearing Board hereby makes findings, and reprimands and admonishes you, Betty Tsamis, as follows:

To: Betty Tsamis:

1. You are being reprimanded for mismanaging your client trust account, which resulted in your issuing a check for insufficient funds to your client, Kris Klimek. You are also being reprimanded for revealing confidential information about your former client, Richard Rinehart, in a public forum.
2. Your admitted conduct is inconsistent with Rules 1.6(a), 1.15(d) and 4.4 of the Illinois Rules of Professional Conduct (2010). You are therefore reprimanded not to repeat the conduct which has resulted in the imposition of discipline.

3. You are further advised that while this reprimand is not formally presented to the Supreme Court, it is not to be taken lightly. You are admonished not to engage in such misconduct in the future and to strictly comply with the Rules of Professional Conduct. You are

PAGE 2:

further admonished that this disciplinary action is of public record and will be considered in the event of any future disciplinary proceedings relating to you.

Respectfully submitted,

Patrick M. Blanchard,
Chair

Cynthia A. Cohan

David C. Rudd

CERTIFICATION

I, Kenneth G. Jablonski, Clerk of the Attorney Registration and Disciplinary Commission of the Supreme Court of Illinois and keeper of the records, hereby certifies that the foregoing is a true copy of the Reprimand, approved by the Hearing Panel, entered in the above entitled cause of record filed in my office on January 15, 2014.

Kenneth G. Jablonski, Clerk of the
Attorney Registration and Disciplinary Commission of the Supreme Court of Illinois