2017 Convention
Champions for Justice

2. Ethics Developments in Virginia

James M. McCauley
Virginia State Bar
1111 East Main St.
Suite 700
Richmond VA 23219-3565
Email: mccauley@vsb.org
Website: http://www.vsb.org/

Ethics Update 2017: Hot Topics

James M. McCauley, Ethics Counsel
Virginia State Bar
March 2017

1. Conflicts—Lobbying Firms that employ legislator—LEO 1884

This opinion addresses a situation where a lawyer who is a member of the Virginia General Assembly joins a consulting firm. The consulting firm is owned by a law firm composed of Virginia lawyers and it employs both lawyer and non-lawyer lobbyists and consultants. The lawyer asks whether the lawyers and nonlawyers in the consulting firm would be barred from lobbying the General Assembly if he joined the consulting firm, and further, whether that bar would extend to members of the law firm as well.

In this opinion, the Committee concluded that **both lawyers and nonlawyers in the consulting firm, as well as the lawyers in the law firm that own the consulting firm, would be barred from representing clients or otherwise lobbying before the General Assembly if a lawyer in the consulting firm were a member of the General Assembly.** This conclusion follows from prior legal ethics opinions that establish that a lawyer may not lobby a public body if another member of the lawyer's firm is a member of that public body. For purposes of Rules 1.11(a) and 8.4(d), there is no reason to distinguish between lawyers associated in a law firm and lawyers associated in a consulting firm. Because a lawyer may not circumvent the Rules of Professional Conduct by using others to engage in conduct that he could not personally engage in, a lawyer may not permit his non-lawyer colleagues to appear before the General Assembly under these circumstances.

The opinion further concludes that **the lawyers in the law firm that own the consulting firm are prohibited from appearing before the General Assembly while a member of the consulting firm is also a member of the General Assembly.** To conclude otherwise would be to place form over function and essentially allow the firms to use a screen to avoid the conflict created by the General Assembly member's employment by the consulting firm.

2. Lawyer Impairment—Duty of Supervising Lawyer—LEO 1886[1]

Substance abuse, mental health issues, and other causes of physical or mental impairment can be among the hardest issues for lawyers to acknowledge in themselves or in others, including their partners and colleagues. Lawyers are understandably reluctant to suggest that a colleague is suffering from an impairment, especially when the nature of the impairment is such that the colleague may not be aware of her own issues. However, partners and other lawyers who have

[1] This topic was written by Emily F. Hedrick, Assistant Ethics Counsel, and used with permission.

managerial authority over other lawyers in a firm may not ignore the impairment of another lawyer in the firm.

Legal ethics opinion 1886, approved by the Supreme Court of Virginia on December 15, 2016, makes clear that **Rule of Professional Conduct 5.1 requires a partner or other lawyer with managerial authority in a firm to take precautionary measures before a lawyer's impairment results in serious misconduct or a material risk to client or the public. This means that partners and supervisory lawyers are required to take action when they reasonably believe that another lawyer in the firm may be suffering from a significant impairment. This duty is different from the duty to report another lawyer's misconduct under Rule 8.3(a); there is an independent duty to ensure that the impaired lawyer does not engage in misconduct even if she has not already done so.**

In practical terms, the first step for the firm (acting through its partners or other managing lawyers) when it believes that a lawyer in the firm is suffering from an impairment will be to confront the impaired lawyer and strongly encourage her to seek an appropriate evaluation and/or treatment for her impairment. Lawyers Helping Lawyers, an independent, non-disciplinary and non-profit organization that assists legal professionals and their families dealing with depression, addiction and cognitive impairment, may be able to help with figuring out how best to handle this confrontation and with finding resources to refer the lawyer to for assistance or treatment. LHL or other professionals may be able to assist the firm in determining how to manage an impaired lawyer and how to evaluate what level of involvement by the firm is necessary and appropriate.

Depending on the nature and extent of the impairment, and the nature of the firm's practice, the firm may be able to allow the lawyer to continue to practice with limitations and supervision – for example, a lawyer who has no problem drafting documents when there is no external pressure from short deadlines or other demands, but who cannot maintain composure in an adversarial situation, may be able to limit her practice to research and writing while being removed from any time-sensitive matters or matters involving contact with other parties. On the other hand, the lawyer may be so impaired that she cannot competently practice law at all, and the firm may need to forbid her from working at the firm and insist that she seek appropriate assistance, counseling, therapy, or other treatment as a condition of returning to work at the firm.

In addition to proactively addressing an impairment before clients are affected, the other lawyers in the firm need to evaluate whether the impaired lawyer has already committed misconduct that raises a substantial question as to her honesty, trustworthiness, or fitness to practice law. If so, Rule 8.3(a) requires them to report that misconduct, even if the firm has already taken steps to address the misconduct and prevent it from recurring in the future and even if the impairment has already been reported to Lawyers Helping Lawyers. As the LEO explains: "The report to the lawyer disciplinary agency is necessary to address the misconduct and protect the public. The report to the lawyer assistance program [LHL] is necessary to address the underlying illness that may have caused the misconduct." Note, though, that the duty to report is subject to the duty of confidentiality to the firm's clients,

and a lawyer's misconduct cannot be reported if the client refuses to allow disclosure of confidential information necessary to make the complaint.

3. Lawyer Advertising Rule Amendments

The Standing Committee on Legal Ethics proposed significant revisions to Rules 7.1-7.5, governing lawyer advertising, including the **deletion of Rules 7.4 and 7.5 and the streamlining of Rule 7.1 to a single statement that communications about a lawyer's services may not be false or misleading.**[2] Claims of specialization and the content of firm names, previously addressed by Rules 7.4 and 7.5 respectively, are addressed now by comments to Rule 7.1, since they are just specific examples of the general obligation not to make false or misleading statements. The required disclaimer for statements of case results has been removed from Rule 7.1, again shifting to a general false or misleading standard rather than a mandatory technical requirement. Only minor changes were made to Rule 7.3, on solicitation of clients, to more clearly define the term "solicitation" and to expand the comments to more clearly explain how the Rules apply to paying for marketing services, including paying for lead generation.

The proposed changes to Rules 7.1, 7.4, and 7.5 largely derive from a report and recommendation issued by a committee of the Association of Professional Responsibility Lawyers (APRL) describing the need to simplify and modernize lawyer advertising rules in light of changes caused by the rise of Internet marketing and communications, and in light of increasing concern about the viability of constitutional or antitrust challenges to advertising regulations. Many advertising rules were developed in a time when print advertising was primary, and therefore are unwieldy or impractical when applied to now-common Internet communications. For example, the requirement that a disclaimer must precede each statement of case results makes it impossible to ever mention a case outcome on Twitter, because the disclaimer alone would exceed the character limit of a Twitter post. The cross-border nature of Internet communications also raises difficult issues, as advertising rules vary greatly from state to state and lawyers often find it impossible to comply with all the rules that could possibly apply to their communications.

Surveys conducted by APRL as part of its study of states' approaches to the advertising rules show that the majority of complaints about lawyer advertising come from competing lawyers and involve technical rule violations; consumer complaints about lawyer advertising are rare, and when they are made, generally involve communications or conduct that are clearly false and misleading. These findings suggest that technical requirements, like the specifically required

[2] Rule 7.2 was deleted in 2013 when parts of that rule were merged into Rules 7.1 and 7.3. If the Supreme Court of Virginia adopts the 2017 proposed amendments, Rules 7.1 and 7.3 will comprise all regulation of lawyer advertising and solicitation. This is a significant step toward deregulation and simplification of regulation.

text and placement of the case results disclaimer currently present in Rule 7.1(b), may not be justified by the need to protect clients or the public.

The Committee also considered the APRL committee's analysis of a number of case decisions in the last decade that have struck down lawyer advertising rules, and the fact that restrictions on speech are particularly vulnerable when there is a lack of empirical support for the necessity of the restriction. The recent United States Supreme Court decision in *North Carolina State Board of Dental Examiners v. F.T.C.*, 547 U.S. ___, 135 S. Ct. 1101 (2015), has also raised concerns for regulators about the possibility of increased antitrust scrutiny of regulatory actions, particularly if it appears that the regulation is being carried out by lawyers with a competitive interest in the market.

The Committee determined, based on all of these factors, that the best option is to adopt the APRL committee's recommendation to streamline the rules to focus on the core issue of preventing false or misleading speech, as well as the specific concerns raised by solicitation of clients, and to otherwise remove or relax technical regulations that have no demonstrated connection to public protection.

Comments on the proposed amendments were strongly positive. The only change that the Committee made to the proposed rules in light of the comments was to change "communication" to "solicitation" in Rule 7.3(c), as suggested by Brett Callahan's comment. In response to a comment from Cullen Seltzer that arrived after the Committee approved the proposed rules for submission to Council, the Committee Chair is proposing that Council further revise Rule 7.3(c)(4) so that the rule will read "is contacted pursuant to a court-ordered notification." A court might order a lawyer to send a communication to unrepresented persons in a context that is not a class action, and it should be clear that any such communication is not subject to the rule requiring solicitations to be labeled as "advertising material."

At the VSB Council Meeting on February 25, 2017, Council voted 65-1 to petition the Supreme Court of Virginia to adopt the proposed rule amendments. The Bar's petition is now pending with the Court.

4. Amendments to Rules 1.6 and 3.3—Client Perjury

Effective December 16, 2016, these rule amendments adopted by the Supreme Court of Virginia clarify a lawyer's obligations when a client discloses her intent to commit perjury well in advance of trial, when the lawyer can withdraw from the representation before the client's intended perjury occurs. Under the prior version of Rule 1.6(c)(1), the lawyer was arguably required to report the client's intention to commit perjury once that intention is expressed, even if that occurs long before trial. This interpretation of the rule, however, is inconsistent with the comments to Rule 3.3 that specifically address the issue of client perjury, and indicate that withdrawal before trial is generally a sufficient remedy.

RULE 1.6

After consideration of the apparent conflict between Rule 1.6(c)(1), requiring immediate disclosure, and the comments to Rule 3.3 that provide that **withdrawal is the appropriate remedy when the client's intent is expressed in advance of trial, the Court accepted the Committee's position that Rule 3.3 expresses the correct approach to client perjury.** The Committee has revised Rule 1.6(c)(1) to resolve any doubt about its application and to clarify that Rule 3.3 sets out the lawyer's obligations if the client intends to commit perjury. Rule 1.6(c)(2) was deleted in its entirety, since the lawyer's obligation when a client commits fraud on a tribunal is already addressed by Rule 3.3.

Rule 1.6(c)(1) now requires a lawyer to report only future crimes that are "reasonably certain to result in death or substantial bodily harm to another or substantial injury to the financial interests or property of another," rather than requiring disclosure of a client's intent to commit *any* crime, no matter how minor. On its face, former Rule 1.6(c)(1) required the lawyer to report the client's intent to go fishing without a license or other misdemeanor offense. These revisions better balance the lawyer's duty of loyalty to her client with the lawyer's duty to society.

The amendments do not change the strict requirement in Rule 1.6(c)(1) that before reporting the client's stated intent to commit a future crime, the lawyer must first persuade the client, when feasible, to abandon his/her intent. In this regard, Comment [7c] observes:

> Third, the lawyer may learn that a client intends prospective criminal conduct. As stated in paragraph (c)(1), the lawyer is obligated to reveal such information if the crime is reasonably certain to result in death or substantial bodily harm to another or substantial injury to the financial interests or property of another. Caution is warranted as it is very difficult for a lawyer to "know" when proposed criminal conduct will actually be carried out, for the client may have a change of mind. If the client's intended crime is perjury, the lawyer must look to Rule 3.3(a)(4) rather than paragraph (c)(1).

A strict reading of Rule 1.6(c)(1) suggests that the only time a lawyer *is required* to report the client's intent to commit a crime is only if the client has stated an intent to do so. Suppose a lawyer has information that clearly establishes the client's intent to commit a crime reasonably certain to result in death or substantial bodily harm to another, but the client has not stated his intent to the lawyer? Under newly added paragraph (b)(7), it appears that the lawyer could *permissibly* make the disclosure he or she may not feel obligated to report under paragraph (c)(1).

The amended Rule 1.6 adds a seventh provision to paragraph (b), permitting disclosure when reasonably necessary to "prevent reasonably certain death or substantial bodily harm." This provision mirrors ABA Model Rule 1.6(b)(1), and permits the lawyer to disclose information about actions by the client or third parties that are reasonably certain to lead to death or substantial bodily harm, even if the harm is not the result of a crime. The amendments revised various comments to the Rule to reflect these changes.

RULE 3.3

Comments to Rule 3.3 were revised and added in order to more thoroughly address the lawyer's obligations in cases of false evidence or testimony, now that Rule 3.3 is clearly established as the sole source of the lawyer's obligations in these situations. Paragraph (d) clarifies that the lawyer only has a duty to reveal a third party's fraud upon a tribunal *when that fraud occurs in the course of a proceeding in which the lawyer is representing a client* – a lawyer does not have a general obligation to disclose fraud by third parties when the lawyer is not involved in the case at all.

The adopted rule amendments added paragraph (e) and accompanying comment [15], both from the ABA Model Rule, to establish and explain a definite time limit on the lawyer's duty to disclose and rectify false evidence or false statements made to the Court. The rules require, and will continue to require, that **if a lawyer knows that a client has committed perjury, the lawyer must report that fact to the court promptly. The duty to report client perjury will not apply if the client's perjury is revealed to the lawyer *after* a final order has been entered and the time for an appeal has expired.** This is a departure from the prior rule. The bar and Court concluded that a more sensible time limit on the duty to report is at the conclusion of the proceeding after a final order has been entered and the time for an appeal has run. This time limit strikes a better balance by requiring disclosure of the client's perjury when the matter is still before the Court and there is a greater likelihood that remedial action will be possible and effective, but protecting the client's confidences once the matter is final.

5. Rule 1.6(d)—Cybersecurity and Duty to Protect Client Data

Rule 1.6(d):

> **A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information protected under this Rule**
>
> ***Acting Reasonably to Preserve Confidentiality***
>
> [19] **Paragraph (d) requires a lawyer to act reasonably to safeguard information protected under this Rule against unauthorized access by third parties and 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.** See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of this Rule if the lawyer has made reasonable efforts to prevent the access or disclosure. 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 employment or engagement of persons competent with technology, 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).

[19a] Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other laws, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of this Rule.

[20] Paragraph (d) makes clear **that a lawyer is not subject to discipline under this Rule if the lawyer has made reasonable efforts to protect electronic data, even if there is a data breach, cyber-attack or other incident resulting in the loss, destruction, misdelivery or theft of confidential client information.** Perfect online security and data protection is not attainable. Even large businesses and government organizations with sophisticated data security systems have suffered data breaches. Nevertheless, security and data breaches have become so prevalent that some security measures must be reasonably expected of all businesses, including lawyers and law firms. **Lawyers have an ethical obligation to implement reasonable information security practices to protect the confidentiality of client data.** What is "reasonable" will be determined in part by the size of the firm. See Rules 5.1(a)-(b) and 5.3(a)-(b). The sheer amount of personal, medical and financial information of clients kept by lawyers and law firms requires reasonable care in the communication and storage of such information. A lawyer or law firm complies with paragraph (d) if they have acted reasonably to safeguard client information by employing appropriate data protection measures for any devices used to communicate or store client confidential information.

To comply with this Rule, a lawyer does not need to have all the required technology competencies. The lawyer can and more likely must turn to the expertise of staff or an outside technology professional. Because threats and technology both change, lawyers should periodically review both and enhance their security as needed; steps that are reasonable measures when adopted may become outdated as well.

[21] Because of evolving technology, and associated evolving risks, law firms should keep abreast on an ongoing basis of reasonable methods for protecting client confidential information, addressing such practices as:

(a) Periodic staff security training and evaluation programs, including precautions and procedures regarding data security;

(b) Policies to address departing employee's future access to confidential firm data and return of electronically stored confidential data;

(c) Procedures addressing security measures for access of third parties to stored information;

(d) Procedures for both the backup and storage of firm data and steps to securely erase or wipe electronic data from computing devices before they are transferred, sold, or reused;

(e) The use of strong passwords or other authentication measures to log on to their network, and the security of password and authentication measures; and

(f) The use of hardware and/or software measures to prevent, detect and respond to malicious software and activity.

LEO 1872: Rule 1.6 requires the lawyer to act with reasonable care to protect information relating to the representation of a client. When a lawyer is using cloud computing or any other technology that involves the use of a third party for the storage or transmission of data, the lawyer must arrangements between the law firm and the third-party vendor to follow Rule 1.6(b)(6) and exercise care in the selection of the vendor, have a reasonable expectation that the vendor will keep the data confidential and inaccessible by others, and instruct the vendor to preserve the confidentiality of the information. The lawyer will have to examine the third-party provider's use of technology and terms of service in order to know whether it adequately safeguards client information, and if the lawyer is not able to make this assessment on her own, she will have to consult with someone qualified to make that determination.

Hacker Steals Lawsuit Settlement Funds

Bile v. RREMC, LLC and Denny's Corp, Civ. Action. No. 3:15cv051 (Eastern Dist. Va., J. Payne, Aug. 24. 2016)

Plaintiff and Defendant reached a settlement of an employment discrimination lawsuit. Each side filed motions to enforce the settlement after Defendant's counsel inadvertently delivered to a hacker the settlement proceeds. At a settlement conference, the parties agreed to settle the case for $63,000 and executed a settlement agreement. A hacker obtained access to Plaintiff's e-mail account, obtained knowledge of the pending settlement and sent an e-mail to defense counsel, posing as Plaintiff's counsel, with instructions to wire the settlement funds to an account purporting to be the Plaintiff's account in London. Defense counsel complied and wired the settlement funds to the account as instructed. Two days later Plaintiff's counsel called Defense counsel to inquire about the status of the funds at which point counsel realized that the e-mail with the wire transfer instructions did not originate from Plaintiff's counsel. Defendant's counsel unsuccessfully tried to claw back the wired funds. Plaintiff refused to discontinue the lawsuit and Defendant refused to pay another $63,000.

At issue was the fact that Plaintiff's counsel earlier received an email from an "aoi.com" account that was visually similar to Plaintiff's legitimate aol.com account, with instructions to wire the settlement funds to a particular account in Plaintiff's name at Barclay's in London. Shortly thereafter, Plaintiff's counsel verified that his client did not send that particular email. Plaintiff's counsel deleted the email without alerting Defendants' counsel or the Court to the fact that his client's email account was compromised and that he had received what he considered a fraudulent email. Judge Payne made a finding that Plaintiff and his counsel had actual knowledge a malicious third party was targeting the settlement for a fraudulent transfer to an overseas account that did not belong to Plaintiff.

Judge Payne found that Defendants substantially performed under the settlement agreement and therefore were entitled to substantial performance by Plaintiff under the agreement. Citing UCC law regarding third-party fraud and depositing checks at a bank, the Court noted that a party whose failure to take ordinary care results in loss must be the party to bear that loss. The Court also noted that a blameless party [defendants] is entitled to rely on reasonable representations, even when those representations are made by fraudsters. The Court stated:

> The parties have cited no decision articulating that an attorney has an obligation to notify opposing counsel when the attorney has actual knowledge that a third party has gained access to information that should be confidential, such as the terms of a settlement agreement, or the attorney has knowledge that the funds to be paid pursuant to a settlement agreement have been the target of an attempted fraud. Nor has the Court located such authority. However, the principle is an eminently sensible one . . . that attorneys have an obligation to contact [opposing] counsel when and if they receive suspicious emails instructing [them] to wire settlement funds to a foreign country where such [a] request has never been made during the course of performance of the parties. . . . [Plaintiff's counsel] failed to act with the ordinary care that he, correctly, says should govern this case.
>
> Two days before the fraud was perpetrated on [defense counsel], both [plaintiff's counsel] and [plaintiff] were aware that an unidentified third party had targeted the settlement funds for diversion to a Barclay's account that had nothing to do with [Plaintiff]. Additionally, [both] knew that the email account [for Plaintiff's counsel] was being used in an effort to perpetrate a fraud. [Plaintiff's counsel] failed to pass this information along to Defendants, defense counsel or the Court. This failure substantially contributed to the loss of $63,000 within the meaning of U.C.C. §3-406.

Law Firms Continue to Be Hacked by Cybercriminals

Last year, Cravath, Swaine & Moore and Weil Gotshal & Manges, two of the largest firms in the United States, got caught in a major cybersecurity breach later linked to a $4 million-plus insider-trading scheme. Cybersecurity firm Mandiant estimated that 80 of the largest 100 firms in the country, by revenue, have been hacked since 2011. Other law firms are finding their information systems infected by malware simply because an employee opened a file attachment

to an e-mail. The firm will typically have to take down their entire network, run applications to locate the virus and wipe clean the hard drive where the virus originated. Bottom line: If the source of the e-mail is unknown or even if it is known but it is not expected, the e-mail or file attachment should not be opened until the e-mail is quarantined and inspected. Firewalls should be used to block employees from accessing websites where malware can be inadvertently downloaded.

Clients are forcing law firms to buck up with cybersecurity. The 2016 ABA Legal Technology Survey Report reveals that 30.7% of all law firms and 62.8% of firms of 500 lawyers or more reported that current or potential clients provided them with IT security requirements.

Industry standards give law firms a framework. Some firms are using ISO/IEC 27001 certification. The National Institute of Standards and Technology (NIST) framework from the DOJ also provides guidance for law firms in cybersecurity. The second edition of *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals*, will be published before the ABA Annual Meeting in August 2017.

At the Solo & Small Firm Forum on April 11, 2016 on the Eastern Shore of Virginia, Sharon Nelson commented that there was a time when we may have been capable of preventing cyber-attacks. That time is gone. She acknowledged now that prevention of a cyber-attack is no longer a realistic goal. The best we can do now is have measures in place to "detect" and "react" when there has been a breach of security, and minimize the severity of its consequences, i.e., corruption, theft, destruction of confidential client information. Sharon Nelson reported that successful cyber-attacks on law firms have occurred including large law firms like Weil Gotschal.

A panel of experts made a similar pessimistic assessment at a program on cyber security in Richmond on October 1, 2015 for the Richmond Bar Association.[3] As ethics and technology expert, David G. Ries, author of "Safeguarding Confidential Information: Attorneys' Ethical and Legal Obligations" (January 2016) observes:

> These threats are a particular concern to attorneys because of their duty of confidentiality. Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients. They also often have contractual and regulatory duties to protect client information and other types of confidential information.
>
> Effective information security requires an ongoing, comprehensive process that addresses people, policies and procedures, and technology, including training. It

[3] Cyber Security/Data Breach - Technology and Policy, October 1, 2015, presented by Greg Burkhart: Principal Director, Cyber 4Sight Services, Booz Allen Hamilton; Kevin Minsky: Associate General Counsel, Booz Allen Hamilton;Michael Woods: Vice President and Associate General Counsel, National Security and Public Safety, Verizon Communications

also requires an understanding that security is everyone's responsibility and constant security awareness by all users of technology.

Here are some resources to learn more about IT security:

- Federal Trade Commission, "Start with Security" guidance to businesses (https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf). This is generic guidance drawn from the FTC's recent enforcement cases. It's fairly simple and written in non-technical language, but it provides some insight into what one group of federal regulators are thinking is (or should be) the standard of care for a business.

- NIST Cybersecurity Framework (http://www.nist.gov/cyberframework/). This document was developed through a lengthy consultation process with industry; it is meant to provide a general approach to cybersecurity, and to point businesses toward the relevant existing standards. In many industry contexts, it is becoming the de facto "standard of care."

- NIST Recommendations (http://csrc.nist.gov/publications/PubsSPs.html). These documents are more detailed and technical recommendations developed through the NIST collaborative process with industry. The "800" series are particularly important in cybersecurity. The documents are designed for use by IT professionals responsible for implementing a company's cybersecurity program.

- Verizon Data Breach Report (DBIR) (http://www.verizonenterprise.com/DBIR/) is annual analysis of cyber threats as reflected in actual data breaches and security incidents. The report looks at anonymized data submitted by a broad range of law enforcement agencies, private companies, and cybersecurity providers.

- DHS Information Sharing resources: DHS supports a number of information sharing initiatives. You can find summary information here: http://www.dhs.gov/topic/cybersecurity-information-sharing.

- Steptoe & Johnson Cyberlaw Podcast (http://www.dhs.gov/topic/cybersecurity-information-sharing). Weekly podcast put out by a group of lawyers at Steptoe. They provide a good summary of case law, policy developments, and legislation relating to cyber, data breach, privacy, national security, etc.

Personal Identifying Information (PII)

In addition to the ethical issues of confidentiality, injury can result by misuse or theft of client information, and new statutes in many jurisdictions regarding protecting and securing client information require security breaches to be reported. **To date 46 states have enacted breach notification statutes.** For a list of states and their corresponding notification statute, see the NCSL (National Conference of State Legislatures) website**.**

Virginia statute Va. Code § 18.2-186.6: In addition to **§ 32.1-127.1:05, Breach of medical information notification Va. Code § 18.2-186.6 Breach of personal information notification** requires businesses to report to the A.G.s office any disclosure of a client(s) PII. Virginia law requires a business or state agency to notify any Virginia resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person.

> …(B) If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay. Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

What Should We Be Doing to Exercise Reasonable Care to Protect Client Data from Cyberattack?

What should lawyers be considering as reasonable efforts to protect confidential client information from cyber-attacks? Here is a list of examples:

1. All security patches should be promptly installed.
2. Software which is no longer supported, and therefore not receiving security updates, cannot ethically be used.
3. Authentication – passwords which are used to gain access to law firm data should be a minimum of 14 characters, using capital and lower case letters, numbers as well as special characters.
4. Passwords should not be shared or used in multiple places.
5. Law firms should have a password policy including some of the advice above as well as mandating that passwords be changed regularly (the recommended time period is every 30 days).

6. Where two-factor authentication is available, it should be utilized.

7. All mobile devices should be encrypted and have the ability to be remotely wiped if they are lost or stolen. They should also be protected by security software.

8. We are rapidly reaching the point where e-mails containing confidential data should be encrypted. Several years ago, encryption was cumbersome. Today, it is inexpensive and simple. Lawyers may wish to have an IT professional install and configure their encryption solution.

9. There should be a checklist for departing employees to ensure that all law firm data is returned to the firm and that no further access to the law firm network is technically possible.

10. Law firms should consider annual security assessments.

11. All law firms should have anti-malware software – larger firms should have enterprise grade software. Today's software is not just antivirus software, but can also filter spam, recognize and prevent dangerous components in e-mails and attachments and remove them, and use heuristics to identify potentially dangerous communications.

12. Larger firms will want to explore intrusion detection systems and data loss prevention hardware/software.

13. All firms, of any size, should have an Incident Response Plan, in addition to other security related policies, including disaster recovery plans, BYOD (bring your own device), BYON (bring your own network), etc.

14. Identify all laws and regulations which may apply to your data. Do you hold data which is governed by HIPAA, HITECH or Sarbanes Oxley? Do you hold PII (personally identifiable information)?

15. All firms should have an updated network diagram so it is clear where all data resides and to assist digital forensics experts in the event of a security incident.

16. The security of all third party vendors which hold law firm confidential data (including data in the cloud) should be investigated – again, the standard of reasonableness applies. Lawyers certainly need to read the Terms of Service of anyone who holds their confidential data.

17. Law firms should conduct annual training about data security, including the dangers of phishing and social engineering.

18. As ransomware has evolved, it is now critical that backups be engineered to be impervious to ransomware. In a very small firm, with an external hard drive backup, it may suffice to simply unplug the drive. But more complex backup systems are needed by larger firms.

19. Backups need to be tested on a regular basis.

20. Wireless networks should protected by WPA2 encryption – the only encryption which has not yet been broken.

21. Logging should be enabled on servers whenever possible to aid in the investigation of security incidents.

22. Physical security is also important. Servers should be physically protected. Depending on the size of the law firm, lawyers may include keys, prox cards, alarm codes, video cameras, etc. as part of physical security.

23. If you permit access to your wireless network for guests, their access should be on a properly configured guest network so that they cannot access your confidential data.

24. Make sure there is access control to important data – as an example, there is no reason why a secretary needs to access the firm's financial data.

25. Change all default IDs and passwords – they are freely available on the Internet.

26. Consider a redundant Internet connection, in case your primary connection goes down.[4]

New standards on "cloud computing" have been promulgated the Legal Cloud Computing Association (LCCA), an organization whose purpose is to facilitate adoption of cloud computing technology within the legal profession, consistent with the highest standards of professionalism and ethical and legal obligations. These standards were released just recently in 2016:

- Must disclose where data is housed—physically and geographically
- Must meet certain industry certifications (SOC 2, or ISO 27001 or 27018
- Geographical redundancy—data centers in multiple locations
- Encryption for storage at and transmitting data to and from data center.
- Disclose practices and frequency of testing for hacking and vulnerability
- Disclose policies on limiting access by third parties and request/subpoenas by third parties to obtain customer date, including customer notification
- Data retention policy
- End user authentication (multi-factor, password strength, device authentication, cerficate protocols)
- Addition/Deletion of Authorized users
- Tracking, use of audit logs
- End User's ability to add or delete data

[4] Source: Draft Report of VSB Future of Law Practice Study Committee, Technology Subcommittee Draft Report (April 2016).

- Ability to retrieve data in a non-proprietary format; restoration or back up of inadvertently deleted data
- Terms of Service understandable to end user.
- Privacy policy and restrictions on employee access
- Uptime guaranty or assurance
- Confidentiality of user's data
- Ownership of Data
- Data Breach Notification
- Disaster Recovery

6. Avvo Legal Services and Other Online Lead Generation Companies and Rules 5.4(a) and 7.3(b)

The Virginia State Bar Ethics Committee has yet to issue an advisory opinion on whether the Rules of Professional Conduct permit lawyers to participate in online lawyer-client matching services (ACMS). Some business models place lawyers in violation of the Rules of Professional Conduct while others do not. We have labeled Avvo as an ACMS. Under the business model used by Avvo Legal Services the lawyer

a) accepts a client that has signed up for limited scope legal services[5] advertised to the public by the ACMS for a legal fee set by the ACMS;

b) allows the ACMS to collect the full, prepaid legal fee from the client, and to make no payment to the lawyer until the legal service has been completed;

c) authorizes the ACMS to electronically deposit the legal fee to the lawyer's operating account when she completes the legal service; and

d) authorizes the ACMS to electronically withdraw from the lawyer's bank account a "marketing fee" which, by prior agreement between the ACMS and the lawyer, is set by the ACMS and based upon the dollar amount of the legal fee paid by the client[6].

---

[5] A random sample of services and fees a lawyer agrees to provide through the firm operating this program might be, for example:

Document review: Residential purchase and sale agreement	$495
File for uncontested divorce	$995
Create a parenting plan	$595
Create a living trust bundle (couple)	$1,095

[6] For example, the "marketing fee" might range from $40 for a $149 legal service to $400 for a $2995 service.

The prospective client selects the advertised legal service and chooses a lawyer identified on ACMS's website as willing to provide the selected service. The prospective client pays the full amount of the advertised legal fee to the ACMS. Thereafter, the ACMS notifies the selected lawyer of this action, and the lawyer must call the prospective client within a specified period. After speaking to the prospective client, and performing a conflicts check, the lawyer either accepts or declines the proposed representation.

A lawyer who participates in an ACMS using the Avvo Legal Services model identified herein risks violating the Virginia Rules of Professional Conduct because she

a. cedes control of her client's or prospective client's advanced legal fees to a lay entity;

b. undertakes representation which will result in a violation of a Rule of Professional Conduct;

c. relinquishes control of her obligation to refund any unearned fees to a client at the termination of representation;

d. shares legal fees with a nonlawyer; and

e. pays another for recommending the lawyer's services.

In Opinion 2016-3, the Supreme Court of Ohio Board of Professional Conduct sharply observes, with respect to a similar business model:

> ***the company, not the lawyer, controls nearly every aspect of the attorney-client relationship, from beginning to end. The company, not the lawyer, defines the type of services offered, the scope of the representation, and the fees charged. The model is antithetical to the core components of the client-lawyer relationship because the lawyer's exercise of independent professional judgment on behalf of the client is eviscerated. A lawyer who participates in an ACMS does not violate Rules of Professional Conduct governing limited scope representation, reasonableness of legal fees, and the exercise of independent professional judgment, if she adheres to the Rules governing those aspects of every representation. Avvo Legal Services offers fixed-fee limited scope legal service. A lawyer and client may agree to limit the goals and objectives of the representation. Rule 1.2(b). However, the limitation must not impair the lawyer's ability to provide competent representation and is otherwise consistent with the Rules of Professional Conduct. The client must consent "after consultation" to the limited scope representation. *See,* Rule 1.2(b).

A lawyer does not violate Rule 1.2(b) merely because her contact with a prospective client flows from a proposed limited scope legal representation advertised by a non-lawyer business firm. Indeed, there are several contexts in which a third-party nonlawyer defines the scope of a lawyer's representation of a client. In pertinent part, Comments [6] and [7] to Rule 1.2 state that

> [6] The objectives or scope of services provided by a lawyer may be limited by agreement with the client or **by the terms under which the lawyer's services**

> **are made available to the client**. For example, a retainer may be for a specifically defined purpose. Representation provided through a legal aid agency may be subject to limitations on the types of cases the agency handles. When a lawyer has been retained by an insurer to represent an insured, the representation may be limited to matters related to the insurance coverage. ***.
>
> [7] An agreement concerning the scope of representation must accord with the Rules of Professional Conduct and other law. **Thus, the client may not be asked to agree to representation so limited in scope as to violate Rule 1.1 [Competence]**. [Emphasis supplied throughout.]

In other words, there are circumstances in which a lawyer may agree to allow a nonlawyer to limit the scope of the representation where the lawyer's independent professional judgment is not impaired by the limitation.

The second issue is that the lawyer must assess independently whether the fixed fee for a particular limited scope service *as set by the non-lawyer business firm or ACMS* is a reasonable fee applying the eight factors listed in Rule 1.5. Normally, but not always, the lawyer sets the fee for a legal service.

The third issue arises out of the ACMS holding the fee paid by the client until the lawyer has completed the work. Under Rule 1.15, lawyers are required to place an advanced fee in their trust account and must keep it there until the fee is earned. If the fee is not earned and the client terminated the representation before the service is performed, the lawyer must refund the unearned fee to the client. Rule 1.16(d); LEO 1606. May a Virginia lawyer ethically "opt-out" of the obligations imposed by Rule 1.15 by consenting to a third-party lay ACMS's collection and retention of the client's advanced legal fees? Proponents of the Avvo model argue that the consumer/client is protected when he/she uses their credit card, which enables them to "charge back" or challenge the charge if they are dissatisfied with the service. Further, proponents argue that Rule 1.15 does not apply since the lawyer has not taken custody or control over any client funds until after they have been earned and cannot reasonably be expected to safeguard client funds or property that has yet to come into her possession.

Ethically Impermissible Sharing of Legal Fees with a Nonlawyer

The fourth issue is whether the lawyer is impermissibly sharing legal fees with a nonlawyer as prohibited by Rule 5.4(a).

The North Carolina State Bar has issued a legal ethics opinion which approves a lawyer's participation in an online for-profit service which has both the attributes of a lawyer referral

service and a legal directory[7]. The business model under review in that opinion is described, in pertinent part, as follows:

> A commercial Internet company (the company) operates a website that matches prospective clients with lawyers. A prospective client logs onto the website where he registers and is given an identification number to preserve anonymity. The prospective client posts an explanation of his legal problem on the website and consents to contact from participating lawyers. There is no charge to the prospective client for the standard service but, for more individualized and faster service, there is a fee.
>
> The company solicits lawyers to participate in its service. To participate, a lawyer must be licensed and in good standing with the regulatory agency of his state of licensure. A participating lawyer is charged a **one-time registration fee** that covers expenses for verifying credentials, technical system programming, and other set-up expenses. An **annual fee** is charged to each participating lawyer for ongoing administrative, system, and advertising expenses. The **amount of the annual fee varies by lawyer based on a number of components, including the lawyer's current rates, areas of practice, geographic location, and number of years in practice**. ***
>
> If a client-lawyer relationship is formed between a participating lawyer and a user of the service, it is done without the participation of the company. **The company does not get involved in the lawyer-client relationship or in related financial matters such as fees, retainers, invoicing, or payment.** [Emphasis supplied throughout.]
>
> In answer to the question of whether a lawyer may ethically participate in such a program, the opinion states:
>
> Yes, **provided there is no fee sharing with the company in violation of Rule 5.4(a)**, and further provided the participating lawyer is responsible for the veracity of any representation made by the company about the lawyer or the lawyer's services or the process whereby lawyers' names are provided to a user. [Emphasis supplied.]

A Rhode Island legal ethics opinion[8] specifically approved lawyers' participation in a program run by an Internet company called "Legal Match.com". In addressing whether the arrangement violated the prohibition on fee sharing, the opinion draws the important distinction between ethically permissible advertising costs and impermissible fees charged to a lawyer based upon legal fees generated:

---

7 North Carolina Ethics Op. 2004-1 (2004) **"Participation in On-Line Legal Matching Service"** http://www.ncbar.com/ethics/ethics.asp

8 Rhode Island Supreme Court Ethics Advisory Panel Opinion No. 2005-01 https://www.courts.ri.gov/AttorneyResources/ethicsadvisorypanel/Opinions/2005-01.pdf

> The fee to LM.com is a flat fee which buys advertising and access to requests for legal services posted by consumers. **Unlike the fees in [Rhode Island] Ethics Advisory Opinion No. 2000-04, the annual fee is not a percentage of, or otherwise linked to, a participating attorney's legal fees.** [Emphasis is supplied.]

Rhode Island Ethics Advisory Opinion No. 2000-4, referred to above, found linkage between a consulting company's fee and the attorney's fee to be unethical fee-sharing with a nonlawyer *and* ethically impermissible payment for recommending a lawyer's services:

> In the arrangement proposed by the inquiring attorney, **there is a direct relationship between the consulting fees paid to the consulting company and the attorney's fees earned through the website**. A participating attorney agrees to pay $15,000 to the consulting company for every $100,000 in gross fees he/she earns as a result of the site. In essence, the fee paid to the consulting company is a fifteen percent commission of the gross attorney's fees. As such, **the consulting fee is payment for recommending the lawyer's services** and is violative of Rule 7.2(c).
>
> The proposed arrangement is problematic in other respects. It runs afoul of Rule 5.4(a) **which prohibits attorneys from sharing fees with nonlawyers**.*** [Emphasis supplied.]

In contrast to the business models identified with approval in the North Carolina and first-cited Rhode Island legal ethics opinions, the Avvo model calls for legal fee sharing which some bar opinions hold is ethically impermissible under Rule 5.4(a). A legal fee is shared with a nonlawyer when a fixed portion of it is given by the lawyer to her Internet advertiser, whose entitlement to the fee occurs only when the lawyer has earned her legal fee, and when the amount of the advertiser's fee is based on the amount of that legal fee. Avvo Legal Services calls the fee paid by the lawyer a "marketing fee." Avvo's General Counsel, Josh King, also states that there is no fee-sharing because the lawyer collects the entire fee when the work is finished and pays Avvo the "marketing fee" out of their operating account, as opposed to the trust account, and therefore no fee division has occurred. Calling the online service's entitlement a "marketing fee" does not alter the fact that a lawyer is sharing her legal fee with a lay business. As stated, the amount of the "marketing fee" is itself linked directly to the amount of the lawyer's fee earned on each legal matter obtained by the lawyer through the intermediary ACMS. The larger the legal fee, the larger the "marketing fee" that Avvo collects. Critics argue that the fact that the ACMS executes a separate electronic debit from the lawyer's bank account for its "marketing fee" following the firm's electronic deposit of the full legal fee to the lawyer's bank account does not change the ethically impermissible fee-sharing character of the transaction. If the ACMS were to withhold its "marketing" fee from the legal fee due the lawyer, the "fee sharing" element might appear more pronounced. However, the firm's debiting the lawyer's account following transmission of the full legal fee is but a technical nicety which does not change the substance of the transaction. The form of the transaction cannot mask the substance of it: the legal fees are shared with a nonlawyer in direct violation of Rule 5.4(a).

The Pennsylvania Bar Association's Legal Ethics and Professional Responsibility Committee in Formal Opinion 2016-200 flatly declared that "[a] lawyer who participates in [a program such as is detailed here] in which the program operator collects 'marketing fees' from that lawyer that vary based upon the legal fees collected by the lawyer, violates RPC 5.4(a)'s prohibition against sharing legal fees with a nonlawyer."

The Opinion identifies other jurisdictions' like conclusions on the subject of ethically impermissible fee-sharing with a nonlawyer, stating:

> Ethics opinions that have considered similar compensation arrangements have concluded that marketing, advertising, or referral fees paid to for-profit enterprises that are based upon whether a lawyer received any matters, or how many matters were received, or how much revenue was generated by the matters, constitute impermissible fee sharing under RPC 5.4(a). For example, Ohio Opinion 2016-3, which addresses the same types of FFLS [acronym for "Flat Fee Limited Scope"] programs discussed in this Opinion, states that "a fee-splitting arrangement that is dependent upon the number of clients obtained or the legal fee earned does not comport with the Rules of Professional Conduct." S.C. Opinion 16-06, which also addressed a FFLS program, reached the same conclusion. Other ethics opinions which have, in various contexts, concluded that advertising, marketing, or referral fees calculated on the basis of matters received or legal fees generated violate Rule 5.4(a) include: Arizona Opinion 10-01; Alabama State Bar Ethics Opinion RO 2012-01 ("Alabama Opinion 2012-01"); Indiana State Bar Association Legal Ethics Committee Opinion 1 of 2012 ("Indiana Opinion 1 of 2012"); Kentucky Bar Association Ethics Opinion E-429 and South Carolina Ethics Advisory Opinion 93-09.

A fifth issue is whether the lawyer's payment of a "marketing fee" to Avvo Legal Services is a violation of Rule 7.3(b).

Ethical Restriction on Giving Anything of Value to One Who Recommends the Lawyer's Services

Subject to the exceptions set forth below, Rule 7.3(b) prohibits a lawyer from giving "anything of value" to a person who recommends the lawyer's services. Whether the referring person is a lawyer or nonlawyer is not relevant to an analysis of conduct covered by Rule 7.3(b)[9]. A lawyer may violate Rule 7.3(b) without at the same time violating the fee-sharing prohibition contained

[9] There is one exception: Rule 1.5(e) permits a lawyer to share legal fees, under certain conditions, with *another lawyer* who has referred a case to her. A note to Virginia Legal Ethics Opinion 1130 states:

> **Legal Ethics Committee Notes.** – This LEO was overruled by Rule 1.5(e), which does not require that a lawyer sharing in fees also share responsibility, thus allowing "referral fees" if the client consents after full disclosure.

in Rule 5.4(a) because the source of the compensation given to the referring person need not be a legal fee.

Rule 7.3(b) lists only four specific exceptions under which a lawyer may give something of value to another for recommending a lawyer's services (footnote 9), only two of which are applicable to a lawyer's participation in the for-profit business firm's operations here under review:

1. payment of "the reasonable costs of advertisements or communications"; and/or

2. payment of the "usual charges of a legal service plan or a not-for-profit qualified lawyer referral service".

A "marketing fee" based upon a lawyer's having been actually hired to perform legal services for which a fee has been earned, with the amount of the "marketing fee" based upon the amount of the lawyer's fee is not a reasonable cost of advertisement. It is in form and function the payment of a referral fee to a nonlawyer. Payment of the so-called "marketing fee" is not required unless and until the lawyer finishes a legal matter for a client the lawyer has obtained as a result of the ACMS's efforts. The ACMS which identifies available lawyers on its website is neither a "legal service plan" nor a "not-for-profit qualified lawyer referral service". It is a for-profit lay entity with a business model whose revenue is derived by sharing the lawyers' earnings derived specifically from clients and fees generated to the lawyers by the program.

In discussing a rule analogous to Virginia Rule 7.3(b), the South Carolina bar deemed it a violation of its rule to compensate an Internet service which advertises lawyers' services by paying the Internet service based on fees obtained from clients whom the lawyer receives via participation in the service:

> South Carolina Rule of Professional Conduct 7.2(c)[10] prohibits lawyers from giving "anything of value to a person for recommending the lawyer's services" but includes an exception for the "reasonable cost of advertisements." A lawyer may ethically make payments to an Internet service for advertising the lawyer's services based either on a set monthly or yearly fee or based on the number of hits or referrals from the service to the lawyer. **Lawyers could not ethically pay the service any portion of the fees received from clients obtained through the**

---

[10] RULE 7.2: ADVERTISING

(c) A lawyer shall not give anything of value to a person for recommending the lawyer's services except that a lawyer may

(1) pay the reasonable costs of advertisements or communications permitted by this Rule;

(2) pay the usual charges of a legal service plan or a not-for-profit lawyer referral service, which is itself not acting in violation of any Rule of Professional Conduct; and

(3) pay for a law practice in accordance with Rule 1.17.

> **service.** See S.C. Rule Prof. Cond. 5.4(a). This opinion deals only with services that are open to attorneys generally. Services that restrict or screen attorney participation may violate Rule 7.2(c). [Emphasis is supplied.]

See, South Carolina Bar Ethics Advisory Opinion 01-03.

South Carolina Bar Ethics Advisory Opinion 16-06, issued in 2016, analyzed the ethical implications of a lawyer's participation in a service precisely as described here. It concluded that the marketing fees charged are not the ethically permissible reasonable costs of advertising:

The service, however, purports to charge the lawyer a fee based on the type of service the lawyer has performed rather than a fixed fee for the advertisement, or a fee per inquiry or "click." In essence, the service's charges amount to a contingency advertising fee arrangement rather than a cost that can be assessed for reasonableness by looking at market rate or comparable services.

Presumably, it does not cost the service any more to advertise online for a family law matter than for the preparation of corporate documents. There does not seem to be any rational basis for charging the attorney more for the advertising services of one type of case versus another. For example, a newspaper or radio ad would cost the same whether a lawyer was advertising his services as a criminal defense lawyer or a family law attorney. The cost of the ad may vary from publication to publication, but the ad cost would not be dependent on the type of legal service offered.

PA Formal Opinion 2016-200, cited above, addresses the "reasonable cost of advertisements" issue from the perspective of the differing marketing fees charged, as tethered to the legal fees themselves:

> *** The cost of advertising does not vary depending upon whether the advertising succeeded in bringing in business, or on the amount of revenue generated by a matter. One FFLS [Flat Fee Limited Scope] program charges participating lawyers "marketing fees" ranging from $10 for a $39 "Advice Session" to $400 for a "Green Card Application," which generates $2,995 in legal fees. Clearly, there cannot be a 4000% variance in the operator's advertising and administrative costs for these two services, particularly since the operator does not, and cannot, have any role in the actual delivery of legal services.***

There are a variety of forms in which lawyers may advertise, one being via Internet services which identify lawyers available to handle particular types of legal matters. Comment [4] to Rule 7.3 speaks approvingly of services available to lawyers:

[4] Lawyers are not permitted to pay others for channeling professional work. However, Paragraph (b)(1) allows a lawyer to pay for advertising and communications permitted by this Rule, including the **costs of print directory listings, on-line directory listings, newspaper ads, television and radio airtime, domain-name registrations, sponsorship fees, banner ads, and group advertising**. A lawyer may compensate employees, agents, and vendors who are engaged to provide marketing or client-development services, such as **publicists, public-relations personnel, business-development staff, and website designers**. *** [Emphasis supplied.]

CONCLUSION

A Virginia lawyer may certainly participate in a for-profit lay business firm's Internet advertising platform from which members of the public are matched with Virginia lawyers who are identified as willing and available to handle particular matters for fixed legal fees *if the cost of doing so* complies with Rule 7.3(b)(1) and if the lawyer complies with the other Rules of Professional Conduct discussed above. The "reasonable costs of advertising or communications" may be based on any number of factors which the advertising lawyer may assess for herself: quality of presentation, market exposure, demography, and measurable levels of interest evoked (through Internet "clicks" or "hits"). However, a Virginia lawyer violates Rule 7.3(b) when she pays another—including an Internet marketer—a sum tethered directly to her receipt, and the amount, of a legal fee paid by a client.