George Mason University School of Law
17TH ANNUAL ETHICS UPDATE
October 12, 2016
9:30-11:30 AM

Ryan A. Brown, Esq.
Arlington Law Group
703-842-3025 x40
rbrown@arlingtonlawgroup.com

Anti-Money Laundering & Counter Terrorist Financing

I. Lawyers and AML/CFT Requirements **(50 Minutes)**
Rules: 1.1, 1.2, 1.4, 1.6, 1.8, 1.16, 1.18, 1.9

a. The CBS News program, 60 Minutes, aired a program in January, 2016 entitled "Anonymous, Inc." which was based upon an undercover operation by a group called Global Witness. A script was created about a fictional African government minister who had received several hundred million dollars in bribes and who wanted to bring that money into the United States to invest in real estate, a private jet and real estate. The Global Witness investigator then took meetings at a dozen Manhattan law firms, saying that he represented the African minister, that the funds were from bribery, and asking how they could be brought into the United States. All but one of the firms provided detailed information on how the funds could be brought into the United States, and many were eager to hold follow on meetings to discuss the potential representation. Several went as far as to quote legal fees, and only a few of the firms expressed reservations as to the source of the funds. One of the attorneys suggested using his attorney trust account to receive and transmit the funds, bypassing bank scrutiny.

The episode quoted a study that the United States is the second easiest place to form an anonymous company, after Kenya. While there is noting wrong or illegal about setting up shell companies to protect privacy, doing so to protect criminals or launder money is illegal. Global Witness put out a report of the under cover operation in early 2016[1].

b. Background/Overview

i. What is Money Laundering?

[1] See: https://www.globalwitness.org/en/reports/loweringthebar/

The Bank Secrecy Act Anti-Money Laundering Examination Manual defines money laundering as "the criminal practice of filtering ill-gotten gains, or 'dirty' money through a series of transactions; in this way the funds are 'cleaned' so that they appear to be proceeds from legal activities." So, in layman's terms money laundering is a process by which individuals take money gained from illegal transactions and convert it into legitimate currency to hide the illegal source of the money. [2]

The Money Laundering Control Act of 1986[3] made money laundering a federal offense. See next tabbed section for full statute.

There are three stages of money laundering: 1) Placement; 2) Layering; and 3) Integration.[4]

During placement, the illegal funds are introduced into the financial system by moving them away from direct association with their illegal source. At the layering stage, the individuals further disguise the source of the money though a series of often complex financial transactions. Finally, in integration, the money becomes available to the criminal with the initial source hidden from detection. [5]

A 2009 study estimated that the amount of money laundered worldwide added up to $1.6 trillion in US currency, roughly 2.7% of the world GDP. [6]

Further, the ABA suggested practices are designed to aid lawyers who are unknowingly assisting clients in money laundering/terrorist financing.

ii. What is Terrorist Financing?

---

[2] Bank Secrecy Act Anti-Money Laundering Examination Manual, Federal Financial Institutions Examination Council (2007), *available at* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_002.htm.

[3] 18 U.S.C. §§ 1956-57.

[4] *The Money Laundering Cycle*, United Nations Office on Drug and Crime, *available at* https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html.

[5] Am. Bar Ass'n, VOLUNTARY GOOD PRACTICES GUIDANCE FOR LAWYERS TO DETECT AND COMBAT MONEY LAUNDERING AND TERRORIST FINANCING, 4-5 (2010) [hereinafter known as "Good Practices Guidance], *available at* http://www.americanbar.org/content/dam/aba/publishing/criminal_justice_section_newsletter/crimjust_taskforce_gtfgoodpracticesguidance.authcheckdam.pdf.

[6] United Nations Office on Drug and Crime, Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Crimes, at 5 (October 2011), *available at* http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

Also targeted by this legislation is financing of individual terrorists, terrorist organizations, and any terrorist acts. A "terrorist" is defined by the FATF as "any person who commits, participates in, organizes, or contributes to the commission of terrorist acts." [7]

"Terrorist acts" are acts "intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."[8]

A "terrorist organization" is a "group of terrorists that: (a) commits, or attempts to commit, a terrorist act by any means, directly or indirectly, unlawfully and willfully, (b) participates as an accomplice in terrorist acts, (c) organizes or directs others to commit terrorist acts, or (d) contributes to the commission of terrorist acts by a group of persons acting wit ha a common purpose when the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.[9]

It is more difficult to detect terrorist financing than money laundering because often times the transactions involve small amounts of money, are made to non-profit organizations, or stem from a host of sources.[10]

c. How do these issues impact Lawyers?
    i. FATF-40+9 Recommendations (Lawyers as Designated Non-Financial Businesses & Professions)[11]

        1. Relevant Recommendations
            a. **22-Customer Due Diligence** (Incorporates Lawyers into to Recs. 10-12, 15, 17)

        DNFBPs: customer due diligence

        The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to

---

[7] *See* GOOD PRACTICES GUIDANCE *supra* note 5 at 6.
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] All relevant language pertaining to the 40+9 Recommendations found at Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations, (Feb. 2012), *available at* http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

designated non-financial businesses and professions (DNFBPs) in the following situations:

(d) Lawyers, notaries, other independent legal professionals and accountants – when they prepare for or carry out transactions for their client concerning the following activities:
- buying and selling of real estate;
-managing of client money, securities or other assets;
-management of bank, savings or securities accounts;
-organization of contributions for the creation, operation or management of companies;
-creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

b. **23-Other Measures** (Incorporates Lawyers into Recs. 18, 21)

DNFBPs: Other Measures

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial
businesses and professions, subject to the following qualifications:
(a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

c. **10-Customer Due Diligence**

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Financial institutions should be required to undertake customer due diligence (CDD) measures when:
(i) establishing business relations;

(ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

(iii) there is a suspicion of money laundering or terrorist financing; or

(iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:
(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.
(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.
Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as

reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business. Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer. These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

d. **11-Record Keeping**

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

e. **12-Politically Exposed Persons**

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

(a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
(b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
(c) take reasonable measures to establish the source of wealth and source of funds; and
(d) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs

f. **15-New Technology**

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

g. **17-Reliance on 3rd Parties**

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is

permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

(a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.

(b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(b) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

(d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programs against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programs is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group program, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

h. **18-Internal Controls and Foreign Bodies and Subsidiaries**

Financial institutions should be required to implement programs against money laundering and terrorist financing. Financial groups should be required to implement group-wide programs against money laundering and terrorist financing,

including policies and procedures for sharing information within the group for AML/CFT purposes. Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programs against money laundering and terrorist financing.

i. **21-Tipping Off and Confidentiality (especially relevant in conjunction with Rule 1.6)**

Financial institutions, their directors, officers and employees should be:

- (a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and
  (b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

d. Good Practices Guidance & Risked-Based Approach (April 2010)
   i. **Purpose/Goal of ABA GPG**

The purpose of the risk-based approach under the GPG is to help enable lawyers in identifying the biggest threats of money laundering/terrorist financing and efficiently allocate limited time and resources to combating these problems. Those sources of money that pose the greatest risks/warning signs receive more attention and a greater level of scrutiny. Inversely, situations that pose a lesser amount of risk may receive a lower level of scrutiny than what is normally suggested.

The GPG suggests lawyers create protocol to decide what specific actions to take depending upon the level of risk involved with the client's situation.

For example, Attorney in Fairfax County dealing with a long term client asking to form an LLC in order to conduct a local business need not take high-priority measures to ensure the legitimacy of the request. However, if a new, unknown client

comes in with a large source of money and asked for the same thing, a good protocol will probably dictate an enhanced level of research before deciding to move forward with the work.

How does a lawyer go about determining whether a client's motives and money are "pure?"

ii. **Client Due Diligence ("CDD")-What is it?**

Client Due Diligence is the process by which the GPG suggests lawyers should research a client in order to allow them to form a reasonable belief that they know the identity of the client and the actual purpose of the act they are being asked to perform for the client.

A lawyer should perform CDD at intake, but it should also be done throughout the term of representation whenever a situation arises that would warrant its use.

For "basic" CDD, a lawyer is expected to take 3 steps: 1) timely identify and verify the identity of client(s); 2) identify the beneficial owner and verify her identity to a degree of reasonable satisfaction; and 3) depending on the nature of the representation, gather information about the client(s) business situation.

1. **Specified Activities when CDD is Necessary**

   The "Specified Activities" covered by the Lawyer Guidance include five categories: 1) buying and selling real estate; 2) managing of client money, securities, or other assets; 3) management of bank, savings or securities accounts; 4) organization of contributions for the creation of the operations or management of companies; and 5) creation, operation, or management of legal persons or arrangements, and buying and selling of business entities.

2. **Risk Categories**
   a. Country/Geographic Risk
      The lawyer should look at the interrelationship between the client's domicile, the location of the transaction, and the geographic source of the funding. With this information, the lawyer should then identify the profile of the country/countries involved. Countries subject to

sanctions, embargos, or similar measures by a credible body (e.g. the U.N.) or identified by a credible source to have high levels of corruption and criminal activity are a higher risk and may require higher levels of CDD.

b. **Service Risk**
    i. **"Touching the Money"**
    Any time a lawyer acts as a financial intermediary for his client handles the funds in the act of closing or facilitating a transaction through accounts controlled by the lawyer. When this situation arises, a lawyer should find out the source and destination of the money.

    ii. **Performing Services Outside Area of Expertise**
    When a client knows lawyer does not have much experience in a certain area but asks the lawyer to do perform a service on that subject matter anyway. The lawyer should refer to another lawyer with expertise for advice if going through with the request.

    iii. **Accelerated Real Estate Transfers**
    Unusually short turnaround for real estate transfers with no legal, tax, business, economic or other legitimate reason.

    iv. **Cash Payments/Payments from Other Sources**
    When a lawyer receives payment from an unknown third party or in cash when paying in cash is unusual. (If getting $10,000+ in cash in one transaction or 2 or more related transactions, the lawyer needs to file Form 8300 with IRS)

    v. **Inadequate Consideration**

Any transaction where there appears to be inadequate consideration and the client gives no legitimate reason for this disparity.

vi. **Extraordinary Legal Fees**
Whenever a client offers to pay a lot more money for a service than the normal rate, especially if client wants this to be quick and anonymous. (Contingency fees not included here)

vii. **Unclear Source of Funds/Wealth**
The "source of the funds" is the activity that generated the funds for the client. The "source of the wealth" is the activities that generated the overall net worth of the client. If either of these sources cannot be identified, it should be a red flag to a lawyer.

viii. **Out of Character Transactions**
Typically smaller profile clients who then ask to make unusually large transactions should be treated at a higher level of risk.

ix. **Shell Companies**
Companies with ownership through nominee shareholding and control through nominee and corporate directors are often used to conceal beneficial ownership, making them higher risk clients.

x. **Estate Administration-Convictions for Proceeds Generating Crimes**
Any administrative arrangements dealing with estates where the decedent had been convicted of proceeds generating crimes. If the lawyer had knowledge of, or if the client was known by reputation to be involved in this criminal activity, the representation is higher risk. Further, if the client is involved with casinos, bars, strip clubs, or dealers in pornography, assuming a higher risk level is warranted.

xi. **Hard to Identify Trust Beneficiaries**
Situations where is more difficult to identify actual beneficiaries of the trust (such as discretionary trusts giving the trustee power to name beneficiaries within a class and distribute funds) may be higher risk representation.

xii. **Anonymity**
Services that purposefully provide for or depend upon more anonymity in client identity than normal, without a legitimate explanation could be higher risk.

xiii. **Trust Services**
Firms that offer, as a separate business, Trust and Company Service Provider ("TCSP") services should look to TCSP Guidance even if owned an operated by lawyers.

c. Client Risk

i. **Politically Exposed Persons ("PEP")**
PEPs are individuals entrusted with prominent functions in a foreign country such as heads of state, senior politicians, senior government, judicial, or military officials. Working with a client who is a PEP or beneficially owned by one is often subject to a higher level of risk.

ii. **Unusual Activity**
When a client begins acting in a way or requesting services which are unusual or unconventional for that client. This is a broad category that should be looked at by considering the totality of a lawyer's professional relationship with a client.

iii. **Masking of Beneficial Ownership**
Whenever the structure or nature of the client entity makes it difficult to determine the true beneficial owner or

controlling interests in the entity, the client is higher risk.

iv. **Cash Intensive Businesses**
Clients such as money services, casinos, and businesses that generate large amounts of cash (e.g., bars/restaurants) are higher risk because of the large amounts of cash flow. The risk of representing these clients may be mitigated if they are already subject to Anti Money-Laundering/Combating the Financing of Terrorism (AML/CFT) requirements under the 40+9 Recommendations.

v. **Charities and NPOs**
Those charities and NPOs operating on a "cross-boarder" basis and not subject to some acceptable form of supervision could be higher risk.

vi. **Financial Intermediaries Not Subject to AML/CFT Laws**
Clients using these types of financial intermediaries who are not supervised by competent measures should be more heavily scrutinized.

vii. **Clients with Certain Criminal Convictions**
Clients who have been convicted of financial crimes may be higher risk.

viii. **Clients with No/Multiple Addresses**
Any client without an address, or who has multiple addresses without a legitimate reason is a higher risk because it may be done to conceal the client's identity.

ix. **Unexplained Changes in Instructions**
Clients who (especially at the last minute) change instructions regarding the receipt and delivery of funds without further explanation are higher risk.

x. **Structures with No Legal Purpose**
If a client uses legal persons and arrangements without legitimate tax, business, economic, or other reason, they are higher risk. For example, the purpose of creating a legal entity with seemingly no legitimate reason could be for use in illegal activity.

3. Variables Affecting Risk
    a. **Nature of Client Relationship**
    If representation of a particular client is regular and the type of representation is typical of that client, reduced CDD may be allowed.

    b. **Existing Regulation**
    The level of regulation or oversight/governance regime to which client is subject may be taken into account when assessing risk. If a client is already subject to AML/CFT guidelines, the risk may be less.

    c. **Reputation and Publically Available Information**
    If client is a transparent or well known and has operated for an extended period of time without convictions for similar financial crimes, they pose a lower risk of money laundering.

    d. **Regularity/Duration of Relationship**
    A lawyer may consider the length and regularity of representation with specific clients in determining risk.

    e. **Familiarity with Country/Laws**
    If lawyer knows the local laws/regulations overseeing foreign entities, she can better assess the risk level of the client.

    f. **Duration/Magnitude of Lawyer-Client Relationship**
    A lawyer should assess the relationship between the magnitude and longevity of the client's business operations and its use of the lawyer for its legal needs when assessing the risk of representation.

g. **Local Counsel**
A lawyer providing limited legal services as local or special counsel may mitigate the level of risk associated with representation.

h. **Geographic Disparity**
An unexplained substantial geographic distance between the lawyer and the client without some type of relationship between that distance and the work being done could increase risk.

i. **"One Shot" Transaction**
If a client asks the lawyer to perform only one transaction-based service and another risk factor is present, this could be a higher risk representation.

j. **Technological Developments Favoring Anonymity**
The use, or insistence upon use by a newer client, of technology that promotes non-face to face interaction could be a higher risk. The use of such technology with an existing client will not constitute a higher risk representation, especially if no other risk factors are present.

k. **Client Origination/Referral Source**
A prospective client referred by a trusted source subject to AML/CFT regulations may pose less risk than a one who contacted the lawyer in an unsolicited manner.

l. **Structure of Client/Transaction**
A structure with no legal, tax, business, economic, or other legitimate risk may be a higher risk client.

m. **Pension Funds**
Trusts that are pensions may be lower risk.

iii. Basic Protocol for Client Intake and Assessment
1. Standard CDD-Generally applied to all clients
a. **Identifying the Client**
Basic Identification—A lawyer needs to review the client's driver's license or other government

ID, verify their address, and check any financial and business records. Further, the lawyer should check with the Office of Foreign Assets Control[12] (an "OFAC Scan") to make sure the client's name does not appear on the Specially Designated Nationals List ("SDN List")[13]. This is a list of individuals and entities with whom persons in the U.S. may not do business.

b. **Identifying the Beneficial Owner**
A lawyer should identify the beneficial owner and verify its identity so that the lawyer has a reasonable belief he knows the beneficial owner.

c. **Purpose and Nature of Business**
A lawyer should get information on the purpose and intended nature of the client's business.

d. **Ongoing Due Diligence**
A lawyer should continue to conduct due diligence throughout the relationship with the client in order to make sure the transactions taking place are consistent with a legitimate purpose.

2. Reduced CDD
   a. **When to Conduct Reduced CDD**
   A lawyer does not need to conduct Standard CDD in every situation. Reduced CDD may be applied in situations where the risk of money laundering and terrorist financing are lower. Examples of these situations include: 1) publicly listed companies and majority owned subsidiaries; 2) financial institutions subject to a AML/CFT regime, including all U.S. banks; and 3) government authorities and state run enterprises from non-sanctioned countries.

   b. **Process of Conducting Reduced CDD**
   The only information a lawyer needs to gather when conducting Reduced CDD is the purpose

[12] https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx
[13] https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

and nature of the matter or business relationship necessary for the lawyer to perform his duties.

3. Enhanced CDD
    a. **When to Conduct Enhanced CDD**
    When a lawyer reasonably determines a certain client is higher risk, that lawyer should perform Enhanced CDD. When making this determination, the lawyer should look at the factors discussed earlier, such as client's business activity, ownership structure, and service offered.

    b. **Process of Conducting Enhanced CDD**
    Enhanced CDD consists of a more in depth, systematic background check into the client and its ownership and business activities. The lawyer should make sure that the client and its ownership are legally legitimate and that no criminal activity is involved.

4. **Timing**
    The risk assessment should be conducted during the client intake process. A lawyer should not perform any work for a prospective client until after the risk assessment process.

5. **Unacceptable Risk**
    After the lawyer has performed the risk assessment of the prospective client and the proper level of CDD, the lawyer may feel conducting a business relationship with the prospective client is too risky. If this is the case, the lawyer should comply with the steps required under Rule 1.16 of the Virginia Ethics Requirements and decline or withdraw from representation if the situation meets those requirements.

e. ALM and the Relationship to VA Ethics Requirements
    i. **Rule 1.1 (Competence)**
    A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for representation.
    In many situations, the Virginia Ethics Rules do not allow reporting as mandated by the FATA's 40+9 Recommendations. However, when those situations arise, even though reporting

may not be allowed, a lawyer should still engage in CDD in order to learn more about the client and the representation. After undertaking the necessary CDD, a lawyer should be able to gather the information necessary to decide whether representation of the client could be in violation of the law or ethics rules. Under Rule 1.1, a situation may present itself where the lawyer has a duty to gather more information in order to ensure that the representation of a client does not violate the law.

ii. **Rule 1.2(c) (Scope of Representation)-May not aid or counsel in activity lawyer knows is criminal or fraudulent**.
(c) A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent, but a lawyer may discuss the legal consequences of any proposed course of conduct with a client and may counsel or assist a client to make a good faith effort to determine the validity, scope, meaning, or application of the law.
This rule is critical for when a lawyer finds out that his client is engaging in money laundering. If the attorney knows that her client is planning to use her services to launder money or finance terrorism, the lawyer has a duty under Virginia Ethics Rule 1.2(c) to not offer her services to further these goals. In the event her client is engaging in illegal activity, asking the right questions and conducting the necessary CDD may help the lawyer identify a problem and cease representation per Rule 1.16. Further, even if the lawyer does not identify through the process any traces of illegal activity, the lawyer may use her documented procedure in order to defend herself from accusations that she "knowingly" aided or counseled her client.

iii. **Rule 1.4(a) (Communication)**
(a) A lawyer shall keep a client reasonably informed about the status of a matter and promptly comply with reasonable requests for information.
Keeping a client "reasonably informed" of the status of the representation includes letting a client know that you must, and are, informing authorities about his intent to engage in an illegal activity.[14] This goes against the FATF's goal of keeping the client/criminal unaware of the fact that the authorities

[14] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 463 (2013), *available at* http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/formal_opinion_463.authcheckdam.pdf.

know about his illegal activity and could lead to the client taking measures to avoid detainment and prosecution.

iv. **Rule 1.6 (Confidentiality)-"Shall reveal" client intent to commit any crime.**

Current Version

(a) A lawyer shall not reveal information protected by the attorney-client privilege under applicable law or other information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).

…

(c) A lawyer shall promptly reveal:

(1) the intention of a client, as stated by the client, to commit a crime and the information necessary to prevent the crime, but before revealing such information, the attorney shall, where feasible, advise the client of the possible legal consequences of the action, urge the client not to commit the crime, and advise the client that the attorney must reveal the client's criminal intention unless thereupon abandoned, and, if the crime involves perjury by the client, that the attorney shall seek to withdraw as counsel; …

New version effective December 1, 2016

(c) A lawyer shall promptly reveal:

(1) the intention of a client, as stated by the client, to commit a crime ***reasonably certain to result in death or substantial bodily harm to another or substantial injury to the financial interest or property of another*** *and the information necessary to prevent the crime, but before revealing such information, the attorney shall, where feasible, advise the client of the possible legal consequences of the action, urge the client not to commit the crime, and advise the client that the attorney must reveal the client's criminal intention unless thereupon abandoned, and, if the crime involves perjury by the client, that the attorney shall seek to withdraw as counsel; …*

Under the current version of Rule 1.6, a lawyer is obligated to reveal a client's intent to commit **any** crime. Therefore, if a client expresses to his lawyer an intent to launder money or finance terrorism, the lawyer must report this to the proper authority, but only after urging the client not to commit the

crime and advising the client that the attorney has a mandatory reporting obligation. As things stand under the current rule, the mandatory reporting standards from the FATF do not conflict with Rule 1.6 since, under 1.6, it is already mandatory in Virginia for a lawyer to report to the proper authorities any crime her client expresses an intent to commit.

The amended Rule 1.6, effective December 1, 2016, creates a conflict between the AML/CTF Recommendations and the Virginia ethics requirements. No longer is the lawyer mandated to report potential crimes if they do not rise to the threshold of "***reasonably certain to result in death or substantial bodily harm to another or substantial injury to the financial interest or property of another."*** Furthermore, there is a question of whether a harm to a government (e.g. tax evasion) would constitute as a "substantial injury to the financial interest … of another."

v. **Rule 1.8(f) (Conflict of Interest: Prohibited Transactions)**
(f) A lawyer shall not accept compensation for representing a client from one other than the client unless:
(1) the client consents after consultation;
(2) there is no interference with the lawyer's independence of professional judgment or with the client-lawyer relationship; and
(3) information relating to representation of a client is protected as required by Rule 1.6.
According to the Good Practices Guidance, receiving payment from a third party is a situation that may pose a higher risk. When receiving a payment from a third party, the lawyer should make sure to understand how and why the payment is being made in such a way. Comment [11] dealing with 1.8(f) states that the lawyer must make sure payment from a third party does not conflict with Rules 1.6, 1.7, or 5.4(c). A certain amount of CDD may be necessary under the current requirements of 1.8(f), so further inquiry regarding the identity and purpose of the third party paying for the lawyer's services is only a slight, but logical extension.

vi. **Rule 1.16(b)(1) & (2) (Declining or Terminating Representation)**
(b) Except as stated in paragraph (c), a lawyer may withdraw from representing a client if withdrawal can be accomplished without material adverse effect on the interests of the client, or if:

(1) the client persists in a course of action involving the lawyer's services that the lawyer reasonably believes is illegal or unjust;
(2) the client has used the lawyer's services to perpetrate a crime or fraud;
Rule 1.16 allows a lawyer to withdraw from representation if the client demands the lawyer act illegally or in violation of the Rules of Ethical Conduct. It further permits a lawyer to withdraw from representing her client if the client definitively wishes to continue on a course of action the lawyer "reasonably believes" is illegal or unjust, or where the action insisted upon by the client is repugnant to the lawyer. If a lawyer reasonably believes the client is laundering money or financing terrorism, the lawyer has the option of withdrawing from representation. There is no obligation to withdraw unless the lawyer knows that her client insists upon the lawyer acting illegally or that further representation on the lawyer's part would result in a violation of the ethics rules.

vii. **Rule 1.18(b) (Duties to Prospective Client)**
(b) Even when no client-lawyer relationship ensues, a lawyer who has had discussions with a prospective client shall not use or reveal information learned in the consultation, except as Rule 1.9 would permit with respect to information of a former client.

A lawyer has a duty to a prospective client to keep the information she hears in consultations confidential. This has the potential to conflict with the FATA 40+9 Recommendations that mandate reporting a client who appears to be laundering money or participating in financing terrorists. Therefore, even if a lawyer does sufficient CDD and finds that a prospective client may be acting illegally through the consultation, the lawyer may not reveal this information. In this rule, however, there is a provision allowing a lawyer to reveal information obtained in a consultation if it is allowed under Rule 1.9, which references rule 1.6, so if the lawyer knows the prospective client committed or is committing a crime, the lawyer must reveal that information.

viii. **Rule 1.9 (Former Client)**
(c) A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter:
(1) use information relating to or gained in the course of the representation to the disadvantage of the former client except as Rule 1.6 or Rule 3.3 would permit or require with respect to a client, or when the information has become generally known; or

(2) reveal information relating to the representation except as Rule 1.6 or Rule 3.3 would permit or require with respect to a client.
Rule 1.18(b) references Rule 1.9 for when a lawyer may reveal information gained from a prospective client. Rule 1.9(c)(2) states that a lawyer may only reveal former client information when revealing the information is allowed or mandated under Rule 1.6.

f. Pending Legislation and Rule 1.6
    i. Incorporation Transparency and Law Enforcement Assistance Act, S 2489; HR 4450 and Stop Tax Haven Abuse Act, S 174; HR 297 would subject lawyers to the AML and suspicious activity reporting requirements of the Bank Secrecy Act when helping clients set up trusts, companies or other specified entities. This would require lawyers to make "beneficial ownership" info available to law enforcement.[15] In late May, the ABA wrote a letter to Congress stating its opposition to the bills.

    In the letter, the ABA specifically mentioned its strong disapproval of the requirement for lawyers to make beneficial ownership available to law enforcement. According to the ABA, that requirement would likely conflict with the lawyer's duty of confidentiality with regards to certain client information, undermining the lawyer-client relationship. Further, the duty to report beneficial ownership would impose an unnecessarily harsh and costly burden on lawyers to dig deep for information regarding all "substantial" owners of companies.

    As of October, 2016, these bills had not moved out of committee, but they have been reintroduced in the past, so they may appear again.

II. Updates on Technology and the Law **(40 Minutes)**
Rules: 1.1, 1.3, 1.6, 1.15, 3.3, 3.4, 3.6, 7.1, 7.3, 8.4

a. Privacy
    i. Cyber Attacks on Law Firms
        1. **Hackers targeting law firms for insider trading Info**
        In a June 2016 email sent to its members, the D.C. Bar warned of possible phishing attacks targeting the D.C. Bar and its members. The email mentioned similar attacks directed toward several bars across the country,

15

and warned that these attacks often have a generic subject line and advised its members to be on the lookout for suspicious email activity.

This warning is closely related with a more general cyber-security problem affecting law firms around the country. In an alert send out March 4, 2016, the FBI discussed an ad on a website soliciting hackers to break into law firms to steal non-public information to be used for insider trading.[16] At least six big firms at that time were found to have recently been the targets of similar attacks.[17]

2. **Attacks come from outside and inside a firm**
In these six instances, the perpetrators of the attacks happened to be lawyers and other staff members employed by the firms who took advantage of their inside access to the firm's servers.[18] However, the FBI alert warns of attacks coming from outside the system.[19]

3. **Law firms "soft underbelly" of financial system**
According to a 2015 study by CitiGroup, cyber-security at law firms is below the standard for other industries.[20] As evidence to this, in early 2016, news broke about two big firms whose security systems had been breached by outside sources hacking into the servers.[21] But these firms are not alone. It has been reported that, of the 15 most prestigious law firms in the U.S., 13 have been targeted by outside hackers.[22] Similarly to the attacks on the six firms by employees, authorities believe the purpose of the invasions is to gain information to be used in insider trading.[23]

---

[16] Gabe Friedman, *FBI Alert Warns of Criminals Seeking Access to Law Firm Networks*, BLOOMBERG LAW (March 11, 2016), *available at* https://bol.bna.com/fbi-alert-warns-of-criminals-seeking-access-to-law-firm-networks/
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL STREET JOURNAL, (March 29, 2016), *available at* http://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.
[22] David Lat, *Beware of Big Hacking in Big Law*, ABOVE THE LAW (March 30, 2016), *available at* http://abovethelaw.com/2016/03/beware-of-big-hacking-in-biglaw/?rf=1.
[23] *Id.*

Many big law firms represent big Wall Street banks and Fortune 500 companies in not only lawsuits, but billion dollar merger negotiations as well.[24] Tellingly, the only two of the 15 firms mentioned above not targeted by hackers focused strictly on already public litigation.[25]

It is speculated that law firms are attacked because they are thought of as the "soft underbelly of the financial sector."[26] This may be because of the perceived lack of technological expertise possessed by lawyers when compared to other professionals that deal with this information.[27]

Another reason may be, as noted before, cyber-security in big law is not as stringent as that of members of the financial service industry. In October 2015, an Israeli cyber-security firm tested the network of a prestigious law firm in order to see how susceptible it was to an outside attack.[28] According to the Israeli firm's CEO, it took less than 48 hours to gain complete control of the law firm's entire network.[29] Specifically the Israeli firm's CEO said that they used three vectors to gain control of the law firm's network: "(1) we broke their WiFi encryption, (2) we used social engineering against the receptionist to run our malware, and (3) we used social engineering against one of the partners where he was convinced to open a malicious file sent via email." Compared to the same firm's test aimed at a top ten technology company, which took over three weeks just to obtain information, this attack took no time at all.[30]

Importantly, these types of technological attacks have an effect, not only on a firm's business prospects, but also on individual lawyer's ethical obligations to her client.

---

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Kevin Townsend, *Why Are Law Firms Targeted by Cyberattacks?*, SECURITYWEEK, (April 1, 2016), *available at* http://www.securityweek.com/why-are-law-firms-targeted-cyberattacks.
[29] *Id.*
[30] *Id.*

4. **Updated Rule 1.1 Comment [6]- know the benefits and risks of relevant technology used by a lawyer**
Newly added to Rule 1.1 in Virginia is a comment that deals directly with lawyers and technology. Comment [6] states, in part, "To maintain the requisite knowledge and skill, a lawyer should engage in continuing study and education in the areas of practice in which the lawyer is engaged. Attention should be paid to the benefits and risks associated with relevant technology."

   According to the ABA (referring to its Model Rule with the same relevant language), lawyers can no longer turn a blind eye to changes and updates in technology when it comes to their ethical obligations.[31] In order to represent a client competently, a lawyer must be aware of what risks the use of different technological advances pose to a client's confidential information. As Comment [6] mentions, a lawyer needs to educate herself in order to update technological safeguards and better protect client information.

5. **Updated Rule 1.6(d)-take reasonable efforts to prevent inadvertent disclosure of information (Comments [19]-[21] expand)**
As mentioned, keeping client information confidential is of the utmost importance with advances in technology. Because of this, Rule 1.6 is implicated as the technological tides continue to change. In response to this change, subsection (d) was recently added to Rule 1.6. 1.6(d) provides, "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information protected under this rule." Added in conjunction with subsection (d) were Comments [19]-[21].

   Comment [19] discusses what constitutes a reasonable attempt to safeguard client information. When determining the reasonableness of a lawyer's actions to safeguard client information, several factors should be considered, such as the sensitivity of the information, the likelihood of disclosure without more safeguards,

---

[31] Jody R. Westby, *Cybersecurity & Law Firms: A Business Risk*, 39 Law Practice Magazine 4 (July/August 2013), *available at* http://www.americanbar.org/publications/law_practice_magazine/2013/july-august/cybersecurity-law-firms.html.

employing or working with individuals competent with technology, cost and difficulty of adding safeguards, and how difficult those safeguards make it for a lawyer to interact with a client.

Comment [20] informs lawyers that perfect data security is not possible, and if information is compromised by a data breach or cyber-attack, a lawyer is protected as long as she has taken reasonable measures in attempt to protect the information. The comment does mention, however, that since attacks of this kind are so commonplace now, there are certain protective measures a lawyer or firm must take to safeguard client information. That being said, a firm is not obligated to take every single technological measure to protect client information, but should stay updated about the availability and necessities of evolving technological shields.

Comment [21] gives several ways in which lawyers should keep themselves up to date with evolving technological methods to safeguard client information.

Under a lawyer's obligations to inform a client (Rule 1.4), in the event of a data breach it is likely the lawyer would have an obligation to inform their client about the problem. This also echo's Virginia's statutory requirements to notify clients when their personal identification is breached[32].

ii. **Supreme Court Approved Rule Change Allowing Law Enforcement to Remotely Search Computers Around the World**

The Supreme Court approved changes to Rule 41 of the Federal Rules of Criminal Procedure that allows a magistrate judge to issue a warrant to remotely access a computer outside of its own jurisdiction.[33] Before the change, warrants could only be issued for remote searches taking place within the same jurisdiction.[34] The Department of Justice believes this change

---

[32] Virginia Code § 18.2-186.6. Breach of personal information notification

[33] Seung Lee, *Supreme Court Allows FBI to Hack Any Computer Anywhere With A Warrant*, Newsweek, (May 1, 2016), *available at* http://www.newsweek.com/supreme-court-allows-fbi-hack-any-computer-anywhere-if-warrant-454278.

[34] U.S. Supreme Court Approves Expanding Hacking Powers, BBC, (April 29, 2016), *available at* http://www.bbc.com/news/technology-36169019.

is necessary because, in an age where maintaining one's anonymity online is becoming easier, criminals are able to hide from authorities when committing crimes online.[35] Department of Justice officials also insist that, although they wish to expand the jurisdictional breadth of remotely accessing computers, there is no change to the legal requirement of probable cause and notice.[36]

Backed by rights groups, several members of Congress have proposed a bill opposing the changes.[37] Opponents of the change cite the fact that many of the computers potentially subject to government access would be those belonging to the victims of attacks, not the wrongdoers.[38] Congress has until December 1 of this year to overrule these changes.[39]

iii. **Apple Declines to Access iPhone for Law Enforcement**

In a widely publicized dispute between Apple and the FBI, the tech company refused to unlock the iPhone of one of the San Bernardino shooters. In February, a Federal magistrate ordered Apple to aid the FBI in accessing information from the iPhone of one of the San Bernardino shooters for its investigation. Apple refused to comply with the order because it categorized the FBI's request as a government "overreach."[40]

Eventually, the FBI found an alternative way to obtain the information from the phone and dropped the case against Apple.

iv. **Virginia Senate Passed Bill Allowing Police to Access Cellphones Without Warrant**

On March 3, 2016, the Virginia Senate passed a bill that would require cell phone companies to provide certain information to law enforcement agencies allowing police to track people in

---

[35] *Id.*

[36] *Id.*

[37] Community Reports, *Poe, Conyers Lead Bipartisan House Coalition to Stop Government Surveillance and Hacking*, Lake Houston Observer (May 25, 2016), *available at* http://www.yourhoustonnews.com/lake_houston/opinion/poe-conyers-lead-bipartisan-house-coalition-to-stop-government-surveillance/article_b91eabd0-5120-5fe6-93d2-10c8cb23fe82.html.

[38] U.S. Supreme Court Approves Expanding Hacking Powers, BBC, (April 29, 2016), *available at* http://www.bbc.com/news/technology-36169019.

[39] *Id.*

[40] Alice Truong, *Apple is Refusing FBI Demands to Hack the iPhone of One of the San Bernardino Shooters*, Quartz (Feb. 17, 2016), *available at* http://qz.com/618151/apple-has-been-ordered-to-help-break-into-the-iphone-of-one-of-the-san-bernardino-shooters/.

emergency situations.[41] In cases where the situation involves someone being in immediate danger, the police would be able to gain access to the location data from the service providers.[42] Although some legislators and rights activist groups believe the bill to be unconstitutional under the Fourth Amendment to the United States Constitution, others liken the expanded access to police action in exigent circumstances.[43]

v. **No Warrant Needed to Obtain Cell Tower/Cell Phone Provider Records Under Third-Party Exception (4th Cir.)**
In a 12-3 vote, the Fourth Circuit held that law enforcement officials may obtain location information from cell phone providers without a warrant.[44] The court applied the third-party doctrine, holding that accessing this information without a warrant is not a search under the Fourth Amendment.[45] Under the third-party doctrine, an individual who knowingly and willingly consents to reveal information to a third party cannot have a reasonable expectation of privacy in that information, regardless of the nature of the information surrendered.[46]

Since customers of the cell phone companies willingly give the companies access to, among other things, their location, law enforcement may obtain this information from the companies for the purposes of investigation without running afoul of the Fourth Amendment. The decision by the 4th Circuit brings it in line with decisions from the 5th, 6th and 11th Circuits.[47] Reconsidering the case en banc, the 4th Circuit overturned an earlier panel decision holding there was a search because of the breadth of the information obtained by law enforcement.[48]

---

[41] Laura Vozzella, *Cell Companies Would Have to Share Tracking Data in Emergencies Under Va. Bill*, Washington Post (March 3, 2016), *available at* https://www.washingtonpost.com/local/virginia-politics/cell-companies-would-have-to-share-tracking-data-in-emergencies-under-va-bill/2016/03/03/380fe9ca-e186-11e5-846c-10191d1fc4ec_story.html.
[42] *Id.*
[43] *Id.*
[44] Jenna McLaughlin, *Appeals Court Deals Devastating Blow to Cellphone-Privacy Advocates*, THE INTERCEPT (May 31, 2016) *available at* https://theintercept.com/2016/05/31/appeals-court-delivers-devastating-blow-to-cell-phone-privacy-advocates/.
[45] United States v. Graham, 2016 U.S. App. Lexis 9797 (4th Cir. 2016).
[46] Smith v. Maryland, 442 U.S. 735, 744 (1979).
[47] Jenna McLaughlin, *Appeals Court Deals Devastating Blow to Cellphone-Privacy Advocates*, THE INTERCEPT (May 31, 2016) *available at* https://theintercept.com/2016/05/31/appeals-court-delivers-devastating-blow-to-cell-phone-privacy-advocates/.
[48] United States v. Graham, 796 F.3d 332, 344 (4th Cir. 2015).

While the decision upon reconsideration eliminated a circuit split, there is still much opposition to this application of the third party doctrine from rights groups and legal scholars. Each circuit court decision had strong dissents, and there is much support for the idea that the third party doctrine as it is does not fit in with the technological age.[49] Many judges joining the majority in these opinions also believe, given the advances in technology, the Supreme Court should weigh in on this issue again.[50]

b. Interaction of Technology and the Law

i. **What Laws Apply to U.S. Tech Firms Abroad and for Information in the Cloud?**

With the increase in global reliance on technology comes an increase in interaction between tech companies and the governments of different nations. The legal ramifications of this globalization are quickly becoming realized. Along with the international nature of the tech world come the questions of what country's laws apply to who and when.

Similarly to Apple's fight with the U.S. government about access to iPhone data, U.S. tech companies find themselves in situations where foreign governments ask them to provide information that may help local law enforcement investigations.[51] When this happens, there is often much confusion as to what laws apply to the tech companies in what situation.[52] Under U.S. law, an American company in a foreign country may not directly give that foreign body information stored within the U.S., but the foreign government may go through certain diplomatic processes to get the information.[53] For other countries, this process poses a problem, because it takes and extended period of time for the information to go through this process, severely hampering investigations.[54]

---

[49] Jenna McLaughlin, *Appeals Court Deals Devastating Blow to Cellphone-Privacy Advocates*, THE INTERCEPT (May 31, 2016) *available at* https://theintercept.com/2016/05/31/appeals-court-delivers-devastating-blow-to-cell-phone-privacy-advocates/.

[50] *Id.*

[51] Martin Kaste, *For U.S. Tech Firms Abroad and for Data in the Cloud, Whose Laws Apply?*, NPR (March 3, 2016), *available at* http://www.npr.org/sections/alltechconsidered/2016/03/03/469066176/for-u-s-tech-firms-abroad-and-data-in-the-cloud-whose-laws-apply.

[52] *Id.*

[53] *Id.*

[54] *Id.*

Because of the length of this process, judges in different countries (including the U.S.) often order companies to disclose information directly to law enforcement, bypassing the diplomatic processes.[55] With the wide variety of laws and the clouding of jurisdictional authority, it is difficult to determine with whose laws companies comply. A potential solution to this problem would be for the U.S. to individually craft deals with different countries allowing foreign courts quick access to the information on servers located within its borders. Currently, the U.S. has already begun negotiating such a deal with the U.K.

Earlier this year, Brazil requested access to WhatsApp user information from Facebook, owner of WhatsApp. Facebook didn't comply, and Brazil went so far as to arrest a key Facebook employee, and Brazil further blocked WhatsApp from operating in Brazil. This was overturned by a Brazilian Supreme Court decision which said that the complete block of WhatsApp was overreaching[56].

Some countries are considering legislation requiring that servers for technology companies be located within the borders of the country so that they have local jurisdiction over the data. Other countries have taken the tack of blocking entire social media networks to suppress dissention[57].

ii. **Is Compelled Decryption Testimonial for 5th Amendment Purposes?**

A Pennsylvania man has been held in prison since September 2015 for failure to comply with a court order to decrypt two computer hard drives. Authorities suspect the computers contain pornographic images of children, but the man has yet to be charged with that crime. A Pennsylvania court held the man would not be compelled to decrypt the hard drives, but the case was then taken to federal court where a warrant was issued for the information. After his failure to give the passwords to the external hard drives, the man was held in contempt and has been held in jail since. He appealed his case to the 3rd Circuit Court of Appeals on, among other things, his Fifth Amendment right against self-incrimination.

---

[55] *Id.*

[56] *WhatsApp in Brazil back in action after suspension, BBC News, July 20, 2016, available at:* http://www.bbc.com/news/world-latin-america-36836674

[57] *Africa cracks down on social media, BBC News, September 10, 2016, available at:* http://www.bbc.com/news/world-africa-37300272

The 11th Circuit has ruled on a similar case. In 2012, the 11th Circuit held that the "foregone conclusion" doctrine negating Fifth Amendment immunity did not apply to a defendant who refused to decrypt his hard drive. Under that doctrine, if the government can show with "reasonable particularity" that it knew of the existence of certain testimony, that testimony is not protected by the Fifth Amendment. According to the court, since the government did not really know that the materials they were looking for were on the hard drive with "reasonable particularity" the doctrine did not apply.

It has been argued, however, that the 11th Circuit's treatment of the foregone conclusion doctrine in this context was incorrect and should not be applied by the 3rd Circuit. This argument treats the knowledge of the password as the testimony implicit in the court order, not the information on the hard drive. If the government knows that a certain individual knows a password, then the self-incrimination of admitting that one knows a password is not protected by the Fifth Amendment because it is a foregone conclusion that the individual knows the password.[58]

While another court has allowed a government to compel an individual to access a phone using thumbprints, that same court held that password protection could not be compelled because of the Fifth Amendment.[59]

c. Social Media in Litigation

i. **Pulaski County Judge Denied Motion for Analysis of Social Media Comments to Determine if Defendant Unable to Receive a Fair Trial.**

A Pulaski County woman asked a judge to review messages and comments from Facebook in order to determine whether or not they impacted the court's ability to conduct a fair trial for her. The defendant claimed that the posts on Facebook (according to the defendant "thousands" of them) show that locally, her case is extremely public and it is unlikely she will receive a fair trial in Pulaski.[60]

---

[58] Orin Kerr, *The Fifth Amendment Limits on Forced Decryption and Applying the "Foregone Conclusion" Doctrine*, The Volokh Conspiracy (June 7, 2014), *available at* https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine/.

[59] Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. Ct. 2014).

[60] Tonia Moxley, *Noah Thomas Case: Judge Denies Motion for Social Media Analysis*, ROANOKE TIMES (Dec. 16, 2015),

The defendant based this claim on the nature of the Facebook posts, many of which were threatening. Worried that these posts were indicative of local opinion, the defendant moved for change of venue and also moved to have the court use an expert witness to analyze the Facebook posts in support of her motion to change venue. The judge, however, denied the request to use the expert witness.[61]

The judge eventually decided to attempt to seat a jury in Pulaski, however, during the process over 60% of the potential jurors were dismissed for their inability to remain impartial.[62] Because of this, the judge ruled in favor of the motion to change venue, eventually leading to the proceedings being conducted as a bench trial.[63]

ii. **Snapchat Sued for Encouraging Reckless Driving.**
The victim of a high-speed crash is suing Snapchat for contributing to the speed of a car that rear-ended and injured an individual in Georgia. The teen driver of the speeding vehicle was allegedly using Snapchat at the time of the accident in order to send a picture using the application's speed filter. This filter measures the speed at which a person using the app is traveling and displays this speed when the picture is sent to friends.

The driver denied using Snapchat at the time leading up to the crash, and Snapchat, after looking at the driver's Activity Log, claims the application was not being used at the time. These accounts differ from statements made by the three passengers of the vehicle who claim the driver was driving at speeds close to or exceeding 100 MPH and using Snapchat.

The suit against Snapchat not only cites this incident, but also claims Snapchat was aware of other similar accidents caused by people using the application while operating a vehicle. The complaint alleges that even with this knowledge, Snapchat did not remove the filter, which ultimately encouraged the driver to travel at such a high rate of speed leading to the accident.[64]

---

[61] *Id.*
[62] Jacob Demmitt, *Ashley White Case Shifts to Bench Trial in Pulaski County*, ROANOKE TIMES (Feb. 9, 2016), *available at* http://www.roanoke.com/news/crime/pulaski_county/ashley-white-case-shifts-to-bench-trial-in-pulaski-county/article_4b6eef31-717a-5e6d-921a-bede136e1705.html.
[63] *Id.*
[64] Tobias Salinger, *Georgia Teen Sued Over Snapchat Use in High-Speed Car Crash Now Facing Criminal Charges*, N.Y. Daily News (June 1, 2016), *available at*

The teen driver has been criminally charged for her role in the accident.

d. Social Media in Your Practice

i. **Lawyer Posts Pictures of Evidence During Trial on Twitter**
While observing an October trial held in U.S. District Court, a Chicago lawyer took pictures of evidence and posted them to twitter. The lawyer posted at least nine times from his twitter account during the trial, specifically referencing the evidence and its use in the trial. An FBI agent in attendance noticed the actions and brought it to the attention of authorities. The lawyer was eventually fined $5,000, ordered to do 50 hours of pro bono work, and to attend a seminar on legal ethics and social media.

An attorney in Louisiana was disbarred as a result of comments posted on social media regarding the handling of a child custody case. In what the Louisiana Supreme Court described as "a social media blitz," the attorney posted on Twitter and other places online misrepresenting the situation and even advocated circulating petitions asking the judges to decide the case in a certain way. The Louisiana Supreme Court found that the attorney violated several Rules of Professional Conduct, including improper ex parte communication, disseminating false information, and engaging in conduct detrimental to the administration of justice.

ii. **LinkedIn as Advertising**
Early in 2015, the New York County Lawyer's Association issued an opinion warning lawyers to be careful about what they include on LinkedIn profiles, making sure no one is endorsing them as a "specialist" in a certain area of practice, which may violate the rules against attorney advertising. The NYCLA also said that anything other than educational background and former employment should include the words "Attorney Advertising" and have the necessary disclaimers attached to it.

Later in the year, an Ethics Opinion was released by the Committee on Professional Ethics of the Association of the Bar of the City of New York disagreed with the NYCLA's broad categorization of elements of a LinkedIn profile as attorney

---

http://www.nydailynews.com/news/crime/georgia-teen-sued-snapchat-crash-criminally-charged-article-1.2657829.

advertising. The City Bar with on to further describe what, in its opinion, constituted advertising. According to the Opinion, these five specific criteria must be met in order to qualify LinkedIn content as advertising:

a) "it is a communication made by or on behalf of the lawyer;
b) the primary purpose of the LinkedIn content is to attract new clients to retain the lawyer for pecuniary gain;
c) the LinkedIn content relates to the legal services offered by the lawyer;
d) the LinkedIn content is intended to be viewed by potential new clients; and
e) the LinkedIn content does not fall within any recognized exception to the definition of attorney advertising."[65]

The Bar explains that the intent element in subsection (b) is subjective, but may be inferred by other elements within the profile. However, a post cannot be considered advertising unless evidence clearly shows that the primary purpose of the post is to attract clients.[66]

III. 2015-2016 Virginia Legal Ethics Opinions **(10 Minutes)**

a. **LEO 1884 (Pending)- Conflict arising from lawyer/legislator working for a consulting firm owned by a law firm.** Applicable ethics rules-1.11(a) (Special Conflicts of Interest for Former and Current Government Officers and Employees); 5.3 (Responsibilities Regarding Nonlawyer Assistants); 8.4(a), (d) (Misconduct)

Related LEO-419, 537, 1278, 1718

"This proposed opinion generally addresses a situation where a lawyer who is a member of the Virginia General Assembly joins a consulting firm. The consulting firm employs both lawyers and non-lawyers who lobby the state and federal legislatures; the consulting firm is owned by a law firm composed of Virginia lawyers. The lawyer asks whether the lawyers and non-lawyers 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."

---

[65] NYCBA Committee on Prof'l Ethics, Formal Op. 2015-7 (2015).
[66] Catherine Foti, *LinkedIn for Lawyers: Newly Issued Ethical Guidance Makes Social Media Use Less Risky*, FORBES (Jan. 15, 2016), *available at* http://www.forbes.com/sites/insider/2016/01/15/linkedin-for-lawyers-newly-issued-ethical-guidance-makes-social-media-use-less-risky/2/#672f81813ce5.

The proposed opinion states that lawyers and non-lawyers working for the consulting firm, along with lawyers from the owning law firm, may not represent a client or lobby the General Assembly if a member of the consulting firm is a member of the GA. (1.11(a); 8.4(a), (d)). According to the opinion, there is no reason to distinguish between lawyers in a law firm and in a consulting firm, and lawyers may not get around the Rules of Professional Conduct by using a non-lawyer to act in such a way in which the attorney is prohibited from acting. (5.3)

b. **LEO 1886 (Draft Opinion) – Duty of Partners and Supervisory Lawyers in a Law Firm when Another Lawyer in the Firm Suffers from Significant Impairment.** Applicable Ethics Rules**:** Rule 5.1 – Responsibilities of Partners or Supervisory Lawyers. Rule 8.3 – Reporting Misconduct.

In this advisory opinion, the Committee analyzes the ethical duties of partners and supervisory lawyers in a law firm to take remedial measures when they reasonably believe another lawyer in the firm may be suffering from a significant impairment that poses a risk to clients or the general public. Two separate hypothetical situations of lawyer impairment are outlined and opined upon by the committee. This opinion delves into the responsibilities of partners and supervisory lawyers at the respective firms where these two practice, and their obligations to prevent serious misconduct and risks to clients or the public.

The first situation describes a lawyer experiencing severe substance abuse issues. A junior associate informs a managing partner at the firm that a senior associate has been coming to work smelling of alcohol and clients have been complaining about unreturned phone calls and missed court dates. The committee determined that as a managing partner at the firm, the lawyer informed of the impaired lawyer must make reasonable efforts to ensure the impaired lawyer does not engage in unethical conduct or cause harm to the firms clients. Only violations that effect honesty, trustworthiness, or fitness as a lawyer must be reported however.

In the second situation involving the aging attorney, a partner has observed that the attorney has slowed down in recent months. His memory isn't as sharp as it once was, he exhibits confusion, referring to the partner by his ex-wife's name and not her own. The committee opined that while it is certainly concerning, the attorneys condition has not made it readily apparent that an ethics violation has taken place. His impairment absent misconduct, is not subject to being reported to the bar. It would however require the partner to take

reasonable efforts to prevent any risk or harm to the firm's clients due to the attorney's impairment.

IV. Other Rule Changes **(20 Minutes)**

a. Adopted

i. **New Rule: Provision of legal services following determination of major disaster**

A new rule, Rule 10, was approved by the Virginia Supreme Court and became effective on January 1, 2016. Rule 10 covers the determination of a major disaster by judges in a jurisdiction and when a lawyer may practice outside a jurisdiction in which she is allowed because of a disaster.

According to subsection (a) of the Rule, the Chief Justice of the Virginia Supreme Court shall decide when there is an emergency that affects the justice system due to a major disaster. This determination may be made regarding Virginia or another state if a state of emergency has already been declared by the highest court in that other state.

Further, subsections (b) and (c) state that lawyers not authorized to practice in Virginia but authorized in other jurisdictions may practice pro bono in Virginia if a state of emergency is declared by the Chief Justice in Virginia. A lawyer authorized to practice in another state may also practice in Virginia if a state of emergency is declared in the state where that lawyer is authorized to practice.

Subsection (d) states that a Foreign Lawyer may practice in Virginia until the Chief Justice decides a state of emergency no longer exists in Virginia or the other state. The Foreign Lawyer may continue to represent any client until the conclusion of that representation, but may not take on new clients or an unrelated matter from an existing client after the emergency status is lifted.

Subsection (e) states that a Foreign Lawyer may not appear in court unless it is under a court's *pro hac vice* rule or if the Chief Justice gives permission to all Foreign Lawyers appear in court. Subsection (f) holds that a Foreign Lawyer practicing in Virginia under Rule 10 is subject to the disciplinary authority of Virginia.

ii. **New ABA Rule 8.4(g) – Anti-Discrimination**

The American Bar Association has adopted a new subsection (g) to Rule 8.4 regarding misconduct. The rule is adopted to

replace a footnote to Rule 8.4. Where footnotes are only considered guidelines to the rules, an actual codified rule is arguable and enforceable in disciplinary proceedings. The text of new subsection (g) is as follows:

[It is professional misconduct for a lawyer to:]

(g) Engage in conduct that the lawyer knows or reasonably should know is harassment or discrimination on the basis of race, sex, religion, national origin, ethnicity, disability, age, sexual orientation, gender identity, marital status, or socioeconomic status in conduct related to the practice of law. This paragraph does not limit the ability of a lawyer to accept, decline, or withdraw from a representation in accordance with Rule 1.16. This paragraph does not preclude legitimate advice or advocacy consistent with these Rules."

iii. **Amendments to paragraph 10 Section IV of the Rules for Integration of the Virginia State Bar**

10-2. ADVISORY OPINIONS OR RULES. …
C. Notice and Comments. The Committee shall provide Notice and opportunity for public comment on proposed Advisory Opinions or proposed Rules. Public comments shall be directed to the Executive Director of the Virginia State Bar. For proposed Advisory Opinions, the Committee will consider any comments received and either ~~publish~~ adopt, modify or withdraw the opinion as an Advisory Opinion. If the Advisory Opinion is adopted or modified, the Committee shall or ask for Council review in accordance with section 10-3. Advisory Opinions express the judgment of the Committee and are not binding on any judicial or administrative tribunal. In the case of a Rule, the Committee will consider any comments received and then submit the Rule to Council for consideration in accordance with section 1

0-3. … 10-3. ADVISORY OPINION OR RULE CONSIDERATION BY COUNCIL. A. Review. After considering all materials and written comments, Council may approve, modify, or disapprove any Advisory Opinion or Rule by a majority vote of those present and voting. If Council approves or modifies an Advisory Opinion or Rule, it ~~may~~ shall be published as an Advisory Opinion of the Bar and have the ~~same legal effect as a Committee-issued opinion. Council may determine to submit the Advisory Opinion or Rule~~ sent to the Court for review along with copies of all public comments.

iv. **Amendments to Rule 5.5 Comment [1a], and Rule 8.3(e)**

RULE 5.5. Unauthorized Practice of Law; Multijurisdictional Practice of Law.
[Ia] For purposes of paragraphs (a) and (b), "Lawyer" denotes a person authorized by the Supreme Court of Virginia or its Rules to practice law in the Commonwealth of Virginia including persons admitted to practice in this state *pro hac vice*.
* * *
Amend Part Six, Section II, Rule 8.3, adding a new section (e) that reads as follows:
RULE 8.3. Reporting Misconduct.
* * *
(e) A lawyer shall inform the Virginia State Bar if:
(1) the lawyer has been disciplined by a state or federal disciplinary authority, agency or court in any state, U.S. territory, or the District of Columbia, for a violation of rules of professional conduct in that jurisdiction;
(2) the lawyer has been convicted of a felony in a state, U.S. territory, District of Columbia, or federal court;
(3) the lawyer has been convicted of either a crime involving theft, fraud, extortion, bribery or perjury, or an attempt, solicitation or conspiracy to commit any of the foregoing offenses, in a state, U.S. territory, District of Columbia, or federal court. The reporting required by paragraph (e) of this Rule shall be made in writing to the Clerk of the Disciplinary System of the Virginia State Bar not later than 60 days following entry of any final order or judgment of conviction or discipline.

v. **Amendments to Rules 1.1 (Competence) and 1.6 (Confidentiality) relating to use of technology in a law practice**
Relevant discussion found in Section II(a)(5) of these materials, above.

vi. **Amendments to Paragraph 13-11 (Limited Right to Discovery), 13-25 (Reinstatement), and 13-30 (Confidentiality)**
The Supreme Court of Virginia approved changes to Paragraphs 13-11, 13-25, and 13-30 of the Rules for Integration of the Virginia State Bar.
The amendments added language to Paragraph 13-11(b)(3), updated the language on reinstatement after revocation in

Paragraph 13-25, and added language in Paragraph 13-30 referencing 13-11 in A. Confidential Matters.

For the full text of the revised rules visit: http://www.vsb.org/docs/2015_12_17_part%206_Sect.%20IV_Para%2013_11_13_25_13_30.pdf

vii. **Supreme Court of Virginia amends rule regarding unauthorized practice of law**
The revisions to Part 6, §IV, paragraph 10 of the Rules of the Supreme Court of Virginia, provide a more efficient and independent review and investigation of unauthorized practice of law complaints. The amendments to Paragraph 10 clarify the mechanism for the VSB ethics counsel to review and dispose of a complaint of Unauthorized Practice of Law. The amendments also provide for supervision and an independent review and disposition of the complaint by the clerk of the disciplinary system.

For the full text of the revised rule visit: http://www.vsb.org/pro-guidelines/index.php/bar-govt/promulgation-of-legal-ethics-and-upl.
(Rule prohibitively long for inclusion in its entirety)

b. Proposed
   i. **Amendments to Paragraph 13.1 regarding suspension for failure to complete professionalism course**
   The amendments authorize the Virginia State Bar executive director to grant, for good cause, an extension request from a member who fails to complete the Professionalism Course by the deadline. Requests for extension often come from lawyers who have scheduled the course for the end of the year and, for unforeseen reasons, are unable to take it. Currently, the members are suspended until they complete the course, unless they obtain a waiver from the Executive Committee, which must hold an emergency meeting to consider the request. The amendments would grant the executive director the authority to consider requests for extension, subject to the limitations set forth in the rule as outlined.

The Executive Committee unanimously approved the proposed revision to the Professionalism Course Rule, as follows:

13.1 Suspension for Failure to Complete Professionalism Course—
Each person admitted to the Virginia State Bar on or after July 1, 1988, as an active member shall complete the course of study prescribed by the Executive Committee of the Virginia State Bar and approved by the Supreme Court of Virginia on the Rules of Professional Conduct and the lawyer's broader professional obligations, and any active member who fails to complete the course shall be suspended unless an ~~waiver~~ extension is obtained for good cause shown. Such course of study shall be funded by attendance fees paid by those attending the course.
Any active member licensed after June 30, 1988, and any other member who changes his or her membership to active status shall complete the required course within twelve months of becoming an active member. Failure to comply with this Rule shall subject the active member to the penalties set forth in Paragraph 19 herein.
"Good cause shown" as used herein shall include illness, hospitalization or such other cause as may be determined by the Executive Committee, whose determination shall be final. The Executive Director of the Virginia State Bar is authorized to grant extensions for compliance with this paragraph until the next Executive Committee meeting. Any determination by the Executive Committee or the Executive Director may be reviewed by the Supreme Court on request of the member seeking an ~~waiver~~ extension.

ii. **Amendments to Rule 1.6 and 3.3 (Approved with Effective Date of 12/1/2016)**
The adopted changes deal with client perjury. Currently, Rule 1.6(c)(2) includes a client's stated intent to commit perjury with other crimes a client intends to commit which a lawyer must report. Under the current rule, even after a lawyer no longer represents a client, she must report this stated intent. Also, the lawyer must report the intent to commit perjury at some point before the client testifies, but the rule is not specific as to when this must be done.

The current rule is inconsistent with Rule 3.3 dealing directly with fraud on a tribunal. The proposed rule removes perjury from Rule 1.6 (more specifically it deletes the current

1.6(c)(2)), making that crime to fall exclusively under Rule 3.3, which indicates withdrawal before trial to be a sufficient remedial measure. This change, however, would not change the requirement that a lawyer speak with her client about the possible consequences of perjury, try to convince the client not to commit perjury, and warn the client of the lawyer's obligation to disclose the client's intent to commit perjury.

The additional approved change to Rule 1.6 modifies the obligation to disclose intent to commit any crime to those crimes "reasonably certain to result in death or substantial bodily harm to another, or substantial injury to financial interests or property of another." This changes the requirement from obliging the lawyer to disclose intent to commit any crime, regardless of how minor, to only those potentially more serious offenses.

Finally, the obligation to report client perjury would be limited to the conclusion of the proceedings, meaning after a final order has been entered and time for an appeal has run.

iii. **Amendments to Rules 7.1 – 7.5 (Pending with Council; Comments Due by November 4, 2016)**

After making significant changes to the advertising rules just a few years ago, the Virginia State Bar's Standing Committee on Legal Ethics (the "Committee") has 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[67]. Claims of specialization and the content of firm names, previously addressed by Rules 7.4 and 7.5 respectively, are now addressed 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 have been 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.

---

[67] For more information or to make public comment, see: http://www.vsb.org/pro-guidelines/index.php/rule_changes/item/amendments_rules_7_2016-09-30

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 as a result 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.

Public comment on these proposed rule changes are due by November 4, 2016.

iv. **Paragraph 13-24 regarding disbarment, revocation, or suspension in another jurisdiction (Comments due August 6, 2016. Pending consideration by Council)**
The Standing Committee on Lawyer Discipline has approved the proposed revisions to Paragraph 13-24. The purpose of the amendments is to clarify what qualifies as another jurisdiction for reciprocal discipline purposes, to clarify the Board's authority to impose the same, equivalent, or lesser discipline as another jurisdiction, to allow for leniency as appropriate, and to remove the default provision.

Proposed subparagraph 13-24.A defines "Jurisdiction" to include other state licensing or disciplinary authorities and federal courts and agencies, including the military. This definition is in keeping with the rules and precedent of the majority of other states and with most prior Board decisions imposing reciprocal discipline. Subparagraph A distinguishes a state licensing or disciplinary authority from other jurisdictions, as orders from state licensing or disciplinary authorities are treated differently than orders from other jurisdictions in proposed subparagraph 13-24.B.

Proposed subparagraph 13-24.B introduces the term "equivalent discipline," which is intended to provide the Board with authority to impose reciprocal discipline available in Virginia when the other jurisdiction has imposed a sanction not provided for in the Rules of Court, such as an indefinite suspension.

Proposed subparagraph 13-24.B eliminates the automatic suspension of the respondent's law license upon issuance of the rule to show cause when the other jurisdiction is not a state licensing or disciplinary authority. This change is intended to address concerns that a suspension from another jurisdiction that is not a state licensing or disciplinary authority may not warrant a suspension of the respondent's law license in Virginia.

Proposed subparagraph 13-24.B also eliminates the automatic suspension of the respondent's law license upon issuance of the rule to show cause when the other jurisdiction's suspension order has been suspended or stayed. This change is intended to address fairness concerns that a respondent's law license in Virginia should not be suspended prior to the Paragraph 13-24 proceeding if the respondent remains authorized to practice law in the other jurisdiction that imposed the suspension.

Proposed subparagraph 13-24.C removes "return receipt requested," as such service is not required to be effective under Part 6, Section IV, Paragraph 13-12.C of the Rules of Court.

Proposed subparagraph 13-24.C includes an additional ground of defense that specifically provides that a respondent may present argument and evidence supporting the imposition of lesser discipline than was imposed in the other jurisdiction. This option is not specifically provided in the existing rule.

Proposed subparagraphs 13-24.D and 13-24.E contain revisions that are intended to clarify the language and do not change the substance.

Proposed subparagraph 13-24.F gives bar counsel the authority to present evidence and argument of the existence of one or more of the grounds enumerated in subparagraph 13-24.C. Under the existing rule, bar counsel lacks authority to present evidence and argument against the imposition of the same discipline as ordered by the other jurisdiction.

Proposed subparagraph 13-24.F also removes the automatic default provision of the existing rule, which denies the respondent the opportunity to put on a defense if the respondent has failed to submit a written response to the rule to show cause within 14 days of service. The result under the current rule is that the Board has no option but to impose the same discipline as the other jurisdiction. The proposed revision instead provides the Board with discretion to decide whether to allow the respondent to put on evidence despite the respondent's failure to file a timely written response. If after proffer the Board is willing to hear the respondent's full evidence and argument, bar counsel may move for a continuance of the hearing to investigate the respondent's defenses.

Proposed subparagraph 13-24.G replaces former subparagraph 13-24.F and provides that the burden of proof is clear and convincing evidence. This is not a change. This burden lies with the respondent, but may also lie with bar counsel if bar counsel seeks to prove the existence of one or more of the grounds found in subparagraph 13-24.C. The sharing of the burden is new.

Proposed subparagraph 13-24.G also provides that absent clear and convincing evidence of the existence of any of the grounds specified in subparagraph 13-24.C, the Board will adopt the findings of the other jurisdiction and conclude that the respondent was afforded due process. The purpose of this addition is to underscore that absent sufficient proof to the contrary, the Board will give full faith and credit to the order of the other jurisdiction.

Proposed subparagraph 13-24.H gives the Board discretion to dismiss the case or impose lesser discipline if it finds clear and convincing proof of the existence of any of the grounds specified in subparagraph 13-24.C. Under the existing rule, the respondent alone may bear the burden of proof, and if the respondent fails to prove one or more of the grounds of defense by clear and convincing evidence, the Board must impose the same discipline as the other jurisdiction.

v. **Mandatory Reporting of Pro-Bono**

On July 1, 2016, the Virginia Access to Justice Commission sent a proposal to the Virginia State Bar Council requesting a change to the Virginia Rules of Professional Conduct and the Rules of the Supreme Court of Virginia to require mandatory reporting of pro-bono activities by Virginia attorneys – both hours served and financial contributions[68]. The proposal states that it is not a step towards mandatory pro-bono, but rather a tool to measure pro-bono activities within the bar, and that attorneys could comply with the rules by simply reporting zero dollars in contributions and zero hours served if they so chose.

Many small firms are concerned about the record keeping that would be required to properly report pro bono activities. The current comments to Rule 6.1 and the proposed new comments to Rule 6.1 define a specific set of activities that constitute "pro bono" work, including, for example, serving on the board of a bar association or promoting law day activities, but not including volunteering to teach a continuing legal education class that raises funds for pro bono activities or scholarships. Thus, attorneys will have to compare every activity against the list of "approved" pro-bono activities to determine what to report to the bar. Many attorneys may find it more convenient to simply make a monetary contribution to established pro-bono programs. The Virginia State Bar Council has not reached a final determination on this proposal, and there is still time to make public comment on it.

c. Disciplinary Cases

i. **Attorney Arrested for Timeshare Fraud**

In October of 2015, a Virginia attorney was arrested by federal authorities and charged with multiple counts of fraud. The attorney allegedly took part in a timeshare scheme designed to

[68] http://www.vsb.org/docs/access-reporting-2016/VATJ-VSB-prop-probono-report-070116.pdf

take advantage of timeshare owners who no longer wanted the timeshares and charges associated with them.

As part of the scheme, the timeshare holders paid a fee to unload the timeshare. Since there were few buyers for these available timeshares, the individuals participating in the scheme would transfer the timeshares to straw buyers or stolen identities. The perpetrators would then reassure the resorts and creditors that there were no problems through deception, but would never pay the fees or taxes that went along with the timeshares.

The accused lawyer handled the real estate loan transactions, transferring the timeshare ownership to the names of the straw owners and stolen identities. This scheme led to $1.3 million in losses to the affected resorts. Three other individuals have already pled guilty for their roles in the scheme, and the attorney in question faces up to 22 years in prison for fraud. The trial was set for September.[69]

ii. **Mishandling Client Funds**

A Virginia lawyer lost his law license after comingling and converting client funds. The lawyer used his office trust account for his own benefit and for the security of his own money instead of safeguarding client funds. The trust account had overdraft protection, a feature that the lawyer used quite often. Using money in the trust account, the lawyer bought liquor, theater tickets, and services from hotels and restaurants.

The complaints were filed by five of the lawyer's clients. One was given a refund check for advanced payments, but had to go to the bank four separate times before the bank was able to cash the check. The Disciplinary board found that the bar had proven the lawyer committed eight different rules violations.

iii. **Lawyer Disciplined for Sarcasm**

The Virginia State Bar issued a public reprimand and subsequently a 90-day suspension to a lawyer for repeated rude behavior and sarcasm directed toward judges and opposing counsel. The lawyer was already on probation from

[69] Adrienne Mayfield, *Williamsburg Attorney Accused in $1.3 Million Timeshare Scheme to Face Trial in September*, Virginia Gazette (March 25, 2016), *available at* http://www.vagazette.com/news/va-vg-federal-timeshare-20160325-story.html.

the Bar following an incident in 2013 with a judge before this most recent occurrence.

The incident triggering the 90-day suspension happened at the deposition of an alleged accident victim. The offending lawyer, counsel for the defendant, made several sarcastic comments to opposing counsel as well as being unnecessarily abrasive towards the plaintiff during the deposition. After a disagreement with opposing counsel, the lawyer sarcastically stated, "I'm sorry if I hurt your feelings," then offered opposing counsel water to make him feel better. The plaintiff's attorney reported the incident to the Bar, which found the lawyer's conduct violated rules against harassment and intentional embarrassment of others.

iv. **Repeat Incompetence**
In December, the Disciplinary Board of the Virginia State Bar suspended a lawyer for 60 days after it found he was repeatedly incompetent in his representation of a client. The lawyer represented the same client in a products liability and a home warranty case.

In the products liability case, the lawyer continuously postponed discovery meetings and never disclosed any expert witnesses, so the defense attorneys asked the Federal District Court judge to sanction the lawyer. The judge instead dismissed the case commenting on the fact that the lawyer had amended the complaint six times and had never fixed existing problems in the complaint and mentioned the lawyer's "incompetence."

The same client paid around $20,000 in legal fees and $13,450 in arbitration costs to get and award of only $1,500. Like the judge in the products liability case, the judge who dismissed subsequent civil suit on the matter also negatively commented on the lawyer's performance. The Disciplinary Board took those comments into account when deciding on the 60 day suspension.

d. Other Updates
   i. **Veterans Legal Service Clinic**
   Virginia Attorney General Mark Herring announced the first pro bono Veterans Legal Services Clinics in Virginia are taking place starting this year. In conjunction with the Virginia Department of Veterans Services and the Virginia State Bar, the AG office is providing certain free legal services to veterans.

These services include the drafting of wills, powers of attorney and advanced medical directives.

In order for an individual to qualify for the free services, they must:

a) be a veteran or the spouse/partner of a veteran;
b) present official documentation showing military service;
c) be a Virginia resident; and
d) show that their income, assets, expenses, and geographic location show they do not have access to representation and estate planning.[70]

ii. **Court Revises Process for Lawyer Reinstatement**

In December of 2015, the Virginia Supreme Court approved revisions to the procedures for rejoining the Virginia State Bar. The initial request should now be sent to the VSB, not the Virginia Supreme Court. The threshold requirements for reinstatement includes 60 hours of pro bono work, a score of at least an 85 on the MPRE, and any reimbursement of any payments, costs, and fees relating to the disbarment. The initial phase also requires $5,000 in cash bond.

The changes will also list the factors for reinstatement considered by the Disciplinary Board. After taking a case, the Board will send a recommendation to the Virginia Supreme Court with the record of the proceeding. The Court will then ultimately decide the lawyer's fate.

Along with the alterations to the reinstatement process, the Supreme Court also approved amendments to regulations clarifying the duty of prosecutors to disclose any information that could potentially exculpate a lawyer in a disciplinary matter. This duty would trump the prosecutor's duty to confidentiality in those situations.

iii. **Third Party Beneficiaries of a Will May Sue Drafting Attorney for Malpractice**

In June of this year, the Virginia Supreme Court held that an intended residuary beneficiary of a will has standing to sue the drafting attorney for malpractice in the event of a drafting error. In *Thorsen v. Richmond SPCA* the testator intended for her attorney to draft a will leaving her entire estate to her

[70] http://ag.virginia.gov/index.php/veteranslegalservices

mother, but if her mother predeceased her, to the Richmond SPCA.

By the time the testator died, her mother had predeceased her. The attorney who drafted the will notified the RSPCA that they were the sole beneficiary of the testator's estate, but was notified by the insurance company that, by the language of the will, the RSPCA was only entitled to the tangible estate, not the real property. A Circuit Court found the language of the will to unambiguously give only the tangible property to the RSPCA, leaving the real property to pass via intestacy.

The RSPCA brought suit against the attorney for the value of the real property the testator intended to give it, just over $600,000. The RSPCA argued that, through the contractual duty to incorporate the testator's intent through the will, the attorney also had a duty to the RSPCA as an intended beneficiary through the will.

The Court held that the intent of the deceased testator can only be enforced by allowing the beneficiary a way to redress the error of the attorney. The Court limited the application of this cause of action by requiring the nonparty to be a "clearly and definitely intended beneficiary" to the oral contract between the attorney and the testator. Further, the Court held that contingent and residuary beneficiaries can be clearly intended beneficiaries and may sue if the facts show the clear intent of the testator to make the third party a beneficiary was understood by the attorney.

iv. **Sanctions for Intimidation**

The Virginia Supreme Court upheld sanctions levied against and attorney and his client for bringing claims for an improper purpose. The parties initiated suit by bringing 17 claims against the defendant, the plaintiff's former girlfriend. Throughout the process, the plaintiff continued to amend his complaint, changing facts and adding/dropping claims depending upon the circumstances. After four years of this, the court dismissed most of the claims. Those that were not were either nonsuited or voluntarily dropped by the plaintiff.

The plaintiff admitted in court that the claims were brought in order to intimidate the defendant. In the end, the Court stated that, although intimidation is a part of the adversarial process, when intimidation and imposing costs are the goals of an action (as opposed to actually prevailing on the merits of one's

claim), the claim was filed for an improper purpose. In this case, the Court found the plaintiff's purpose was only to intimidate the defendant and knew how much the drawn out process cost his opponent, so concluded it was done for an improper purpose. The Court awarded over $80,000 in sanctions to the plaintiff, and over $60,000 to the plaintiff's attorney who had withdrawn from representation earlier due to the plaintiff's inability to pay fees.

V. Q&A **(5 Minutes)**