

**THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK
COMMITTEE ON PROFESSIONAL ETHICS**

Formal Opinion 2015-3: LAWYERS WHO FALL VICTIM TO INTERNET SCAMS

TOPIC: Internet-based scams targeting law firms

DIGEST: An attorney who discovers that he is the target of an Internet-based trust account scam does not have a duty of confidentiality towards the individual attempting to defraud him, and is free to report the individual to law enforcement authorities, because that person does not qualify as a prospective or actual client of the attorney. However, before concluding that an individual is attempting to defraud the attorney and is not owed the duties normally owed to a prospective or actual client, the attorney must exercise reasonable diligence to investigate whether the person is engaged in fraud. In addition, because Internet-based trust account scams may harm other firm clients, a lawyer who receives a request for representation via the Internet has a duty to conduct a reasonable investigation to ascertain whether the person is a legitimate prospective client before accepting the representation. A lawyer who discovers he has been defrauded in a manner that results in harm to other clients of the law firm, such as the loss of client funds due to an escrow account scam, must promptly notify the harmed clients.

RULES: 1.1, 1.4, 1.6, 1.15, and 1.18

QUESTION: What are the ethical duties of a lawyer upon suspecting or discovering that he is the target of an Internet-based trust account scam?

OPINION:

I. INTRODUCTION

Internet-based scams targeting lawyers are not new and appear to be on the rise.¹ Since 2009, email scams have swindled lawyers out of an estimated \$70 million.² These scams are often highly sophisticated, involving parties that appear to be representing legitimate international corporations and using high-quality counterfeit checks that can take a bank weeks

¹ See, e.g., Jennifer Smith, *In Email, Scammers Take Aim At Lawyers*, Wall St. J., Aug. 5, 2012, <http://www.wsj.com/articles/SB10000872396390443517104577571453933076304>; James McCauley, *Increasingly Sophisticated Internet Scams Continue to Target Lawyers*, Va. State Bar, Dec. 2, 2013, <http://www.vsb.org/site/news/item/increasingly-sophisticated-internet-scams-continue-to-target-lawyers>; Todd C. Scott, *Scammed! Sophisticated Check Fraud Scheme Targets Lawyers*, Am. Bar Ass'n Law Trends & News, Fall 2010, Vol. 7, No.1., available at http://www.americanbar.org/content/newsletter/publications/law_trends_news_practice_area_e_newsletter_home/10_fall_pm_feat1.html.

² Smith, *supra* note 1.

to discover. One experienced ring obtained \$29 million over a two-year period from seventy lawyers in the United States and Canada.³ Once an attorney falls victim to a scam, his problems have just begun. Banks have sued attorneys for lost funds caused by counterfeit checks, and some malpractice insurers have refused to indemnify affected lawyers. *See e.g., Lombardi, Walsh, Wakeman, Harrison, Amodeo & Davenport, P.C. v. American Guarantee and Liab. Ins. Co.*, 924 N.Y.S.2d 201 (3d Dep't 2011) (coverage litigation between insurer and attorney, arising from settlement of bank's lawsuit against attorney as a result of an overdraft caused by a counterfeit check); *O'Brien & Wolf, L.L.P. v. Liberty Ins. Underwriters Inc.*, No. 11-cv-3748, 2012 WL 3156802 (D. Minn. Aug. 3, 2012) (holding that insurance company was required to cover losses from attorney trust account due to counterfeit check scheme); *Attorneys Liab. Protection Soc., Inc. v. Whittington Law Assocs., PLLC*, 961 F.Supp.2d 367 (D. N.H. 2013) (denying insurance coverage for losses due to "Nigerian check scam").⁴ On top of that, a law firm that suspects or knows that it is a victim of an Internet scam faces serious questions about its ethical obligations. This opinion addresses some of those ethical issues and offers guidance to attorneys who believe they are (or have been) the target of an Internet scam.

II. A TYPICAL SCAM⁵

A common example of the internet-based scam begins with an email from an individual requesting assistance with an urgent transactional or litigation matter (the "email sender"). This email sender is generally located abroad, whereas the counterparty or adversary is usually located in the attorney's jurisdiction. The email sender often proposes a contingency fee arrangement whereby the attorney would receive a percentage of the transaction total or litigation settlement. If the attorney sends a draft engagement letter, the email sender swiftly executes it. Soon thereafter, the email sender notifies the attorney that transaction has been consummated or the litigation has settled. As a result, the attorney performs little or no work before the engagement ends.

³ McCauley, *supra* note 1.

⁴ A determining factor in lawyer-insurer litigation surrounding scams is often whether or not the activity was related to the firm's "professional" services. *See, e.g., Bradford & Bradford, P.A. v. Attorneys Liab. Prot. Soc'y, Inc.*, No. 0:09-CV-02981-CMC 2010 WL 4225907 (D.S.C. Oct. 20, 2010) (no duty to defend law firm against lawsuit by bank to recover funds lost due to trust account fraud). In New York, however, at least one appellate court has held that handling a client's funds is part of the legal services provided, even when the client is an imposter. *Lombardi*, 924 N.Y.S.2d 201 (insurance company required to defend law firm against lawsuit by bank for lost funds). We highlight these cases merely to alert attorneys to the insurance coverage issues; whether or not losses caused by Internet-based scams are covered by legal malpractice insurance is outside the Committee's jurisdiction, which is limited to interpreting the New York Rules of Professional Conduct.

⁵ This description of the typical scam and the "red flags" identified in Sections II and III are derived from case law, articles, and ethics opinions cited throughout this opinion.

The attorney receives the closing or settlement check quickly. The attorney then deposits the check in the law firm's trust account and, once the check has "cleared," the attorney transfers his contingent fee into his operating account and wires the remainder of the funds to a foreign bank account designated by the email sender. Unfortunately, the attorney might not realize that a bank can "clear" a check and make the funds available before the bank actually *collects* the funds. The bank may take weeks or even months to discover that the check is fraudulent. When that happens, the bank will notify the attorney that the check was fraudulent.

If the trust account contains the funds of other clients, then those clients may be harmed because the bank may use those funds to cover all or part of the wire transfer. If the trust account contains no other client funds (or if the client funds are insufficient to cover the full amount of the wire transfer), then the bank will notify the attorney that his trust account is overdrawn, and will look to the attorney or the law firm to make up the deficiency.

III. RED FLAGS WHICH MAY ALERT AN ATTORNEY TO AN INTERNET SCAM

Before we discuss an attorney's ethical options and obligations upon receiving a scam communication, we will identify some of the elements that may alert an attorney to the scam. A lawyer's suspicion should be aroused by any one or more of these common "red flags" indicating a scam:

- The email sender is based abroad.
- The email sender does not provide a referral source. (If the email sender is asked how he found the firm, he may respond that it was through an online search. If prospective clients rarely approach the recipient attorney based on an Internet search, this should be an immediate red flag.)
- The initial email does not identify the law firm or recipient attorney by name, instead using a salutation such as "Dear barrister/solicitor/counselor."
- The email uses awkward phrasing or poor grammar, suggesting that it was written by someone with poor English or was converted into English via a translation tool.
- The email is sent to "undisclosed recipients," suggesting that it is directed to multiple recipients. (Alternatively, the attorney recipient may be blind copied on the email.)
- The email requests assistance on a legal matter in an area of law the recipient attorney does not practice.
- The email is vague in other respects, such as stating that the sender has a matter in the attorney's "jurisdiction," rather than specifying the jurisdiction itself.
- The email sender suggests that for this particular matter the attorney accept a contingency fee arrangement, even though that might not be customary for the attorney's practice.
- The email sender is quick to sign a retainer agreement, without negotiating over the attorney's fee (since the fee is illusory anyway).
- The email sender assures the attorney that the matter will resolve quickly.
- The counterparty, if there is one, will also likely respond quickly, settling the dispute or closing the deal with little or no negotiation.

- The email sender insists that his funds must be wired to a foreign bank account as soon as the check has cleared. (The sender often claims that there is an emergency requiring the immediate release of the funds.)
- The email sender or counterparty sends a supposed closing payment or settlement check within a few days. The check is typically a certified check or a cashier's check, often from a bank located outside of the attorney's jurisdiction.

IV. DUTIES OF A LAWYER WHO SUSPECTS OR LEARNS THAT HE IS THE TARGET OF AN INTERNET SCAM

When an attorney receives an email from what appears to be a prospective client, it may not be immediately obvious whether it is a legitimate inquiry or an Internet scam. The email sender may provide contracts or other legal documents that look completely genuine; the companies involved in the transaction or litigation may have realistic websites; and the closing or settlement check that the attorney receives may be so authentic looking that even a bank has difficulty detecting that it is fraudulent.

Consequently, if an email or the course of dealing with the client contains one or more of the red flags described above, the safest course may be to delete it. As the California State Bar Association Committee on Professional Responsibility and Conduct ("COPRAC") has noted: "The best approach is to ignore such solicitations altogether." COPRAC Ethics Alert: *Internet Scams Targeting Lawyers* (Jan. 2011). An attorney has no ethical obligation to respond to an unsolicited email inquiry from a prospective client. See NYSBA Ethics Op. 833 (2009) ("An attorney is not ethically required to respond to unsolicited letters from incarcerated individuals requesting legal representation."). If the attorney responds to the email, however, he should be mindful of certain ethical obligations that arise once he engages in those communications.

A. Ethical Duties Owed to the Email Sender

Even before an attorney-client relationship has formed, an attorney owes certain duties to prospective clients, including the duty to preserve confidential information. See Rule 1.18(b). Those duties do not apply, however, to someone who is merely posing as a "prospective client" but whose purpose is to defraud the attorney. The Committee on Professional Ethics of the New York State Bar Association ("NYSBA") has noted:

[A] person who communicates with a lawyer seemingly for the purpose of forming a relationship to obtain legal services is presumptively a "prospective client" entitled to protections of confidentiality under the Rules. However, **if the purported prospective client is actually seeking to defraud the lawyer rather than to obtain legal services, then the person is neither an actual nor a prospective client and is not entitled to those confidentiality protections.**

NYSBA Ethics Op. 923 (May 18, 2012) (emphasis added). In light of these principles, an attorney must exercise diligence in investigating prospective clients before concluding that they

are not genuine and thus not owed any ethical obligations. “The presumption of confidentiality gives way only if and when the lawyer reasonably concludes that the purported client was not actually seeking legal services.” *Id.*

While an attorney is investigating the validity of a potential new matter, he is still bound by his duties to a legitimate prospective client. In particular, Rule 1.18(b) prohibits the disclosure of any information learned in the consultation with the prospective client. If the attorney has not yet determined that the prospective client is trying to defraud the attorney, then the attorney is prohibited from disclosing confidential information about the client, including to banking and law enforcement authorities. If the attorney concludes after investigating the matter that the email sender is attempting to defraud him, then the attorney “may report the scheme to affected banks or law enforcement authorities, and may supply information and documents to those investigating the scheme, without violating any duty of confidentiality that would be owed to persons genuinely seeking legal services.” *Id.*

B. Ethical Duties Owed to Other Clients of the Firm

When an attorney falls victim to the type of Internet scam described above, it could place other clients of the firm at risk. For example, if an attorney’s trust account holds funds from multiple clients, then any funds that are transferred from the trust account to the email sender most likely belong to other clients of the firm. This would place the firm in violation of Rule 1.15(a), which imposes a fiduciary duty upon the attorney to preserve client funds. The loss of those client funds triggers other ethical obligations, including a duty to immediately notify all affected clients. *See* Rule 1.4(a)(1)(iii) (lawyer must “promptly inform the client of . . . material developments in the matter”).

In addition to suffering the reputational damage and financial losses that may come with falling victim to a scam, a lawyer may have violated the duty of competence. Rule 1.1 requires a lawyer to provide competent legal representation to a client and not to “intentionally . . . prejudice or damage the client during the course of the representation except as permitted or required by these Rules.” Rule 1.1(a), 1.1(c)(2). In our view, the duty of competence includes a duty to exercise reasonable diligence in identifying and avoiding common Internet-based scams, particularly where those scams can harm other existing clients. Since depositing a counterfeit check into a firm’s trust account can negatively impact an attorney’s other current clients whose funds are in the same account, an attorney who fails to exercise reasonable diligence to identify and avoid an Internet scam may violate Rule 1.1. *See Iowa Sup. Ct. Att’y Disciplinary Bd. v. Wright*, 840 N.W.2d 295 (Iowa 2013) (attorney violated duty of competence by failing to conduct a cursory Internet search, which would have revealed the existence of a commonplace internet scam that resulted in financial loss to attorney’s other clients).

Thus, an attorney who receives an email solicitation from an unknown individual should conduct a reasonable investigation to ascertain that the email sender is a legitimate prospective client. The due diligence may include verifying the accuracy of the information provided by the email sender, such as names, addresses, telephone numbers, website addresses, and referral sources. The attorney should resist the temptation to depart from his customary intake procedures, such as performing conflict checks, verifying the prospective client’s business and

financial status, executing a retainer agreement, and obtaining an advance retainer. The attorney should also take reasonable steps to ensure that all funds deposited into the trust account are held until the bank confirms that the funds have been honored or collected, not merely that a check has “cleared.” As noted above, pressure from the email sender to wire the funds immediately on the basis of an emergency or urgent need is a red flag that should be scrutinized more closely.

V. CONCLUSION

An attorney who discovers that he is the target of an Internet-based trust account scam does not have a duty of confidentiality towards the individual attempting to defraud him, and is free to report the individual to law enforcement authorities, because that person does not qualify as a prospective or actual client of the attorney. However, before concluding that an individual is attempting to defraud the attorney and is not owed the duties normally owed to a prospective or actual client, the attorney must exercise reasonable diligence to investigate whether the person is engaged in fraud. In addition, because Internet-based trust account scams may harm other firm clients, a lawyer who receives a request for representation via the Internet has a duty to conduct a reasonable investigation to ascertain whether the person is a legitimate prospective client before accepting the representation. A lawyer who discovers he has been defrauded in a manner that results in harm to other clients of the law firm, such as the loss of client funds due to an escrow account scam, must promptly notify the harmed clients.