NEW YORK STATE BAR ASSOCIATION
Journal
NYSBA
MAY 2018
VOL. 90 | NO. 4

Trading Client Trust

CONNECT WITH NYSBA
VISIT NYSBA.ORG/BLOG

A Glimpse Into Insider Trading Within the Legal Profession

Devika Kewalramani, Jason Canales and Amanda Kane

GUARDIANSHIP AND INVOLUNTARY ADMISSIONS

PREPPING WITNESSES FOR DEPOSITIONS

SECOND AMENDMENT MEETS #NEVERAGAIN

LAW PRACTICE MANAGEMENT: PROJECT MANAGEMENT RED FLAGS

Trading Client TRUST

"Ex-BigLaw Patent Attorney Convicted of Insider Trading for Tipping off Friend About Client Merger"

"Ex-Partner Denies Insider Trading Charges Amounting to $1 Million in Illicit Trading Profits"

"Husband of BigLaw Associate Denies Insider Trading Charges for Trading on Non-Public Merger Information"

"BigLaw Employee Charged in $5.6 Million Insider Trading Scheme"

Have you seen these recent headlines? They highlight a disconcerting increase in the number of insider trading charges against lawyers. The irony is that trust and confidentiality are the pillars on which a client-lawyer relationship stands. Insider trading allegations against a lawyer have the effect of ripping away at the very core of that relationship. The legal profession is regulated by rules of professional conduct that set high ethical and professional standards for lawyers. Moreover, lawyers and law firms are bound by their duty of confidentiality owed to clients. This requirement to protect client information is not a new obligation. So, how can this happen? Could it be because sensitive client information is more readily available at law firms via electronic means such that improper access and use may go undetected or unreported? Whatever the possible causes may be for the proliferation of insider trading activities by lawyers, it seems that there may be a much darker problem facing the legal profession that may need to be looked at and addressed.

Part I of this article will examine recent cases involving insider trading committed by lawyers, their friends and family, non-legal staff and hackers. Part II will highlight the ethical issues that surround the alleged misconduct. Part III aims to lay out some practical tips and guidelines to aid lawyers and law firms on how to keep insider trading issues outside the firm.

PART I: RECENT CASES: EMERGING PATTERNS

A growing number of insider trading cases involving lawyers and law firms generally seem to fall within three sets of categories: the first involves lawyers who are alleged to

A Glimpse Into Insider Trading Within the Legal Profession

By Devika Kewalramani, Jason Canales and Amanda Kane

have traded on client information for their own benefit. The second involves lawyers who dole out tips to friends, family and colleagues who then trade on that information. The third involves law firms that may have unwittingly left their client information vulnerable to attack and use by third parties, such as hackers and family members, who then steal the information and trade on it.

Lawyers Directly Making Illicit Trades

The first group of cases involves the most egregious examples of lawyer misconduct – lawyers who themselves unlawfully trade on and profit from confidential client information. Recently, an attorney was convicted and sentenced to 30 months in jail for his role in a large insider trading scheme and was subsequently disbarred by consent by the New Jersey Supreme Court.[1] That attorney, along with a fellow associate, leaked information to a hedge fund about an upcoming client merger through prepaid cell phones in exchange for envelopes of cash.[2] They allegedly made a profit of $32,500.[3] The hedge fund founder and manager who traded on the information was also found guilty of securities fraud and conspiracy, and was fined $92.8 million.[4]

In another instance, a former law firm associate was convicted and subsequently disbarred because of his part in a 17-year, multimillion-dollar insider trading scheme.[5] The associate began the scheme as a young summer associate, feeding non-public client information to traders, and followed it through his early years as a licensed attorney at various large law firms until his arrest.[6] The D.C. Court of Appeals that ultimately disbarred the associate concluded that his insider trading habit was a "crime of moral turpitude."[7]

Another recent case involved an ex-law firm partner accused of using confidential merger information to make trades amounting to $1 million in profits. The partner was alleged to have improperly accessed

Devika Kewalramani is a partner at Moses & Singer LLP and co-chair of its Legal Ethics & Law Firm Practice. LinkedIn: www.linkedin.com/in/devikakewalramani. Website: www.mosessinger.com/attorneys/devika-kewalramani.

Jason Canales is a partner in Moses & Singer LLP's Litigation Practice Group. Website: www.mosessinger.com/attorneys/jason-canales. LinkedIn: www.linkedin.com/in/jasoncanales/.

Amanda Kane is an associate at Moses & Singer LLP. Website: www.mosessinger.com/attorneys/amanda-kane. LinkedIn: www.linkedin.com/in/amanda-kane.

documents related to pending merger announcements belonging to at least 11 firm clients (none of which he personally advised) before tipping off his neighbor and making trades for himself.[8] Likewise, a real estate partner was sentenced to a six-month imprisonment and was fined for purchasing stock in a firm client on the eve of a merger announcement.[9]

Lawyers as Tippers

The second category of cases involves lawyers who breach the fiduciary duties owed to their clients by consciously revealing confidential client information to others, who then use that information to unlawfully trade. For example, a former patent attorney was convicted of insider trading charges by a Brooklyn federal jury for tipping off his friend about a client merger after drinking several glasses of wine and becoming intoxicated during dinner.[10] The friend bought $585,000 worth of stock in the company for himself and clients, netting an illegal $400,000 in profits.[11]

Another insider trading case involved a young transactional lawyer who inadvertently tipped off her father about an upcoming client merger while she was working from home during the holidays.[12] Her father, also an attorney, saw his daughter's transaction documents in the house, including disclosure schedules which identified one of the merging parties to the transaction by name.[13] He then purchased shares in the merging company early on the day the merger was scheduled to be announced.[14] After the announcement, the father sold his shares, earning a small profit.[15] The SEC charged the father with misappropriating his daughter's material, nonpublic information by breaching his family duty of loyalty and confidentiality.[16] The case was ultimately settled.[17] Situations like this exemplify just how vigilant lawyers need to be, even at home where family members are present, with handling paper documents having critically sensitive client information.

Hackers, Husbands and Others

The third category of cases involves hackers, friends and family members of lawyers, and law firm employees who breach law firm security protocols, steal confidential client information and trade on it. Recently, three foreign citizens were criminally charged in the United States for trading on confidential corporate information related to upcoming mergers obtained by hacking into a law firm network and email servers.[18] The hackers were charged with conspiracy, insider trading, wire fraud and computer intrusion. The prosecutors on the case stated that the intruders made more than $4 million in profits through the scheme.[19] Following this case, U.S. officials have continued to warn that law firms are prime targets for hackers given the highly sensitive and valuable client information they hold.[20] Given the potential negative publicity, reputational injury and disciplinary implications that could haunt a firm and its lawyers, a deeper look may be warranted into how information security breaches are occurring at law firms and what law firms and lawyers can do to make sure that they are properly securing confidential client data now and in the future.

Lawyers are obligated to forever protect and preserve the information and documents their clients entrust to them.

Sometimes, people whom lawyers trust (and share a bed with) can also go rogue. Recently, the husband of a now-suspended law firm associate admitted to insider trading charges after using confidential merger information he gleaned from conversations with his wife, information which he then used to trade on in an account set up in his mother's name.[21] The associate's husband is accused of making $120,000 in profits from the information he learned.[22]

Law firm employees have also become entangled in insider trading scandals. In 2015, a systems engineer who scanned his law firm's computer system for merger information was sentenced to two years in prison.[23] In 2016, a managing clerk of a New York law firm tipped his friend off about upcoming mergers his law firm was involved with. He allegedly discovered the information by rummaging through his law firm's computer system using search terms such as "merger agreement," "bid letter" and "due diligence."[24] His sentence was 46 months in prison.[25]

In other instances, non-legal staff in law firms have gone to great lengths to attempt to cover up their indiscretions. For example, the managing clerk of a law firm, together with a trader and a middle man, created a scheme whereby the middle man would transfer material non-public information gleaned by the managing clerk to the trader, who would then use the information to trade for himself and his customers.[26] The managing clerk faced charges by the SEC stemming from an insider trading operation that amounted to $5.6 million in profits.[27] According to the SEC's complaint, the scheme was structured to "avoid detection" by sharing information on post-it notes

and napkins at specified meeting places – usually coffee shops or Grand Central Station.[28] Once the post-it or napkin was transferred, the recipient would rip up or swallow the piece of paper.[29] Not only was information conveyed about what companies were merging, but information about the timing of such mergers was also

conveyed. That, in turn, was used to create fake paper trails of memos and email exchanges that purportedly contained research and analysis on why the trades should be made. In fact, these emails were fabricated in order to create the false appearance that the trades were being made legitimately based on actual research, rather than improperly based on material non-public information.[30]

PART II: ETHICS: A LAWYER'S STOCK-IN-TRADE

A lawyer who may be targeted by the government for insider trading violations could potentially face more than civil and criminal penalties – the lawyer's professional conduct involving potential confidentiality breaches and other ethical transgressions may also be under disciplinary scrutiny. Given that New York's Rules of Professional Conduct (the "Rules")[31] apply equally to lawyers and law firms (including legal departments of organizations),[32] the lawyer's firm may also be potentially impacted by the alleged misconduct of the lawyer for possibly failing to make reasonable efforts to ensure that firm lawyers conform to the ethical rules.[33] Below is a brief discussion of some of the key ethical issues surrounding insider trading by lawyers that may be implicated under the Rules.

Duty of Confidentiality

Lawyers are obligated to forever protect and preserve the information and documents their clients entrust to them. Because a lawyer who engages in insider trading may be liable for misappropriating material-non-public client information, his or her conduct strikes at the very crux of the confidentiality obligation. The duty of confidentiality contained in Rule 1.6(a) provides that "[a] lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person," unless the client gives informed consent or the disclosure is impliedly authorized to advance the best interests of the client or is permitted by the Rules.[34] Moreover, Rule 1.8(b) states that "[a] lawyer shall not use information relating to the representation of a client to the disadvantage of the client unless the client gives informed consent," except as permitted or required by the Rules.[35] The definition of "confidential information" is contained in Rule 1.6(a) which "consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential." The definition excludes a lawyer's legal knowledge, legal research and information that is generally known in the local community, trade, field or profession to which the information relates. Notably, not only is the definition of confidentiality broad, even information not directly received from the client, but from others in the course of the representation, may fall within the protection of the rule.

In addition, Rule 1.6(c) states that:

> A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).[36]

This rule places an additional responsibility on lawyers to take reasonable security measures to prevent confidential client information from being accidentally disclosed to outsiders or improperly accessed by others without the firm's or client's authorization.[37]

If a lawyer breaks his or her oath of silence by sharing any confidential client information – even innocently and without knowledge of the other person's intentions – he or she may still breach his or her duty of confidentiality to clients, regardless of whether he or she is found to be liable under the insider trading laws. It is also important to remember that while lawyers and non-lawyers can get into trouble for violating the insider trading laws, only lawyers are subject to regulation by the ethical rules and can be disciplined by the appropriate grievance committees for unethical conduct.

Duty of Technological Competence

Recent technology amendments to the comments accompanying a lawyer's duty of competence signify how closely the duty of confidentiality is tied to the duty of competence: lawyers need to act competently to protect client confidentiality. While traditionally the elements

of competent representation of a client required "legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation,"[38] the competency criteria for the modern practitioner has been upgraded to include "technological" competence. Specifically, Comment [8] to Rule 1.1 elaborates on lawyer competence, emphasizing the interplay between the duty of confidentiality and the use of technology in law practice:

> To maintain the requisite knowledge and skill, a lawyer should…keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information . . . [39]

Lawyers and law firms are ethically obligated to take reasonable precautions to protect client data, both electronically and physically. To comply with the techno-competency requirement of Rule 1.1, they need to ensure that adequate cyber security measures are taken to protect against client data breaches from the inside and outside. Also, the broad confidentiality obligation of Rule 1.6, coupled with recent insider trading security breach cases discussed above, demonstrate just how critical it is for lawyers to be equally careful with sharing information with others, guarding physical client documents from being improperly accessed and used by outsiders (and insiders), and holding, transmitting and storing electronic client information.

In addition, lawyers and law firms have an ethical duty to stay on top of technological developments and to reasonably assess the potential security risks posed by the technology they use to make sure confidentiality breaches can be avoided. Failure to do so could be an invitation for disaster. A recent study by a technology consultant reported that approximately two-thirds of U.S. law firms have experienced data breaches. A more detailed study by the same consultant showed that in a survey of over 200 law firms, only 34 percent have adopted comprehensive policies and procedures to protect confidential client documents, only 30 percent have an information security officer (or equivalent position), and 18 percent perform data penetrability and vulnerability tests on their systems. Of the firms surveyed, 66 percent faced security breaches and approximately 40 percent of firms failed to realize that breaches had occurred.[40]

To illustrate this, take one simple example: an M&A lawyer working on a merger could potentially risk committing ethical violations in the following scenario:

- Sending confidential client information to an unsecure personal email account, thereby allowing it to be stored and transmitted in an unsecured manner
- Creating the risk that others will view or have access to confidential client information, which can then be freely and widely disseminated to unintended recipients

Note, lawyers not only have a duty to not disclose confidential client information, but under Rule 1.6(c), to proactively make "reasonable efforts" to prevent the unauthorized disclosure of client information. Comment [17] to Rule 1.6 demonstrates the applicability of Rule 1.6(c) to situations like these, stating that "[w]hen transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[41] However, Comment [16] to Rule 1.6 clarified that:

> Unauthorized access to, or the inadvertent or unauthorized disclosure of, information protected by

> Rules 1.6, 1.9, or 1.18, does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the unauthorized access or disclosure.[42]

Currently, there are no established standards for law firms that identify exactly what constitutes "reasonable efforts," and many lawyers and law firms around the country are trying to grapple with the guidance issued by various state bar association ethics committees that shed light on compliance with the ethical duties while using evolving technology in law practice. The lack of clarity surrounding the "reasonable efforts" standard highlights the complex and intertwined relationship between the use of technology in law practice and protecting client confidentiality, while attempting to implement effective law firm data security practices. Lawyers and law firms need to keep up with rapidly changing technology in order to protect client information effectively. These types of efforts could also possibly root out any potential insider trading issues that may be lurking within the firm.

Firm-Wide Duty to Ensure Ethical Compliance

Under Rule 5.1, law firms as well as lawyers in management and supervisory roles are under a duty to: Make reasonable efforts to ensure that all lawyers in the firm conform to these Rules.[43]

This overarching supervisory duty of law firms and senior lawyers incorporates many of the other ethical duties, such as confidentiality and competence that need to be exercised by lawyers to ensure firm-wide ethical compliance.[44] Many firms take steps to comply with Rule 5.1 by, for example, conducting ethics and confidentiality training programs and CLEs and instituting data security policies and practices to ensure protection of client information.

Firms and their senior lawyers also have a duty to make sure that the conduct of junior lawyers and non-lawyers who assist with client matters is compatible with the professional obligations of lawyers.[45] However, junior lawyers under the guidance of senior lawyers are not shielded from responsibility for their own ethical conduct and are independently bound by the Rules, the same way supervisory lawyers are.[46] A chain of command is no excuse for ignorance or noncompliance with the profession's ethical rules and lawyers at every level at a law firm should be aware of these duties to ensure that their conduct and that of non-lawyers (employed or retained by the firm) do not lead to any violations of the ethical rules. Building greater internal firm sensitivity and awareness of the fundamental importance of client confidentiality could probably go a long way to wipe out any possible instances of unprofessional conduct involving use or disclosure of client information, such as tipping, trading or innocent blabbing.

Duty to Report Misconduct

Insider trading violations by a lawyer can raise serious concerns about the lawyer's honesty, trustworthiness or fitness. Rule 8.3 provides that if a lawyer within a firm knows that another lawyer "has committed a violation of the Rules of Professional Conduct that raises a substantial question as to that lawyer's honesty, trustworthiness or fitness as a lawyer" he or she has a duty to report such knowledge to the appropriate authorities empowered to investigate or act upon such ethical violations.[47] While there is no duty to self-report ethical misconduct under Rule 8.3,[48] lawyers are members of a self-regulated profession, and therefore have an ethical obligation to report professional misconduct of others (barring disclosure of confidential information protected by Rule 1.6).[49] It is possible that failure to report attorney misbehavior where it meets the standards of Rule 8.3 could potentially put the firm or its lawyers at risk of violating the duty to report professional misconduct, something that lawyers should always keep at the back of their minds.

Duty to Avoid Misconduct

A lawyer is also prohibited under Rule 8.4 from engaging in "illegal conduct that adversely reflects on the lawyer's honesty, trustworthiness or fitness as a lawyer," "conduct involving dishonesty, fraud, deceit or misrepresentation," or "any other conduct that adversely reflects on the lawyer's fitness as a lawyer."[50] Rule 8.4 reflects the close connection between illegal activity and unethical behavior – a lawyer can be disbarred if convicted of a crime.[51] It is also important to be aware that Rule 8.4 is a stand-alone rule on misconduct, and could apply even if the alleged misconduct by the lawyer or law firm is unrelated to the practice of law or the representation of clients.

Stealing sensitive client data, sharing with a friend, or trading to profit on it are the types of attorney behavior that do not live up to the fundamental tenets that underlie the legal profession. Law firms and lawyers may need to more closely understand not just how insider trading violations may occur within their organizations, but more important, why they are happening more frequently, and what they can do to stop it.

PART III: PRACTICAL (NOT IMPROPER) TIPS

So, what more can lawyers and law firms do to avoid breaches of confidentiality stemming from lawyer misconduct or improper use of technology? Some simple starting-off points for consideration in deciding how to best protect against nefarious behavior that may compromise confidential client information are discussed below:

- Create and maintain a restricted securities policy and list of securities that can be sent to the *entire* firm to confirm which securities cannot be traded. It should be regularly updated to add or delete

items, as needed. Consider firm-wide training sessions to explain the purpose and importance of the policy, the need to review the list, how to comply, and consequences of non-compliance.

- Design special secure data storage rooms for merges and acquisitions that have strict security protocols and can only be accessed by the lawyers working on the matters and the clients.
- Avoid directly referencing the companies involved in upcoming (especially, highly sensitive) deals, wherever possible. This is a basic precaution that can help prevent the dissemination of information that could potentially lead to insider trading issues.
- Establish internal controls to monitor computer network activity to identify and prevent unauthorized or unusual access to client-related data.[52] Some law firms may be subject to clients' outside counsel guidelines that may require law firms that receive non-public information to certify compliance with applicable restrictions on insider trading, including taking appropriate steps to limit firm lawyers, non-legal employees and third party consultants, if any, from accessing or using such information.
- Develop and regularly conduct internal ethics and confidentiality training programs to educate and build awareness within the firm regarding the types of activities that could create potential risks to client confidentiality and privilege, and the possible consequences when ethical duties may be violated, even accidentally.

NO TRADE-OFFS

Improper tipping or illegal trading present no trade-offs for lawyers. They risk potential ethical violations and possibly disciplinary charges. Trading client trust tramples over the professional boundaries of the client-lawyer relationship.

---

1. Jeannie O'Sullivan, *Ex-Ropes & Gray Atty Jailed for Insider Trading Disbarred,* Law360, Sept. 8, 2016, https://www.law360.com/articles/837757/ex-ropes-gray-atty-jailed-for-insider-trading-disbarred.
2. *Id.*
3. *Id.*
4. Peter Lattman, *Rajaratnam Ordered to Pay $92.8 Million Penalty*, N.Y. Times, Nov. 8, 2011, https://dealbook.nytimes.com/2011/11/08/rajaratnam-ordered-to-pay-92-8-million-penalty/.
5. Zoe Tillman, *Lawyer Convicted in Insider Trading Scheme Disbarred*, The American Lawyer, Nov. 21, 2013, http://www.americanlawyer.com/id=1202629205940/Lawyer-Convicted-in-Insider-Trading-Scheme-Disbarred.
6. *Id.*
7. *Id.*
8. *Law Firm Partner and Neighbor Charged in $1 Million Insider Trading Scheme*, SEC Press Release, May 11, 2017, https://www.sec.gov/news/press-release/2017-100.
9. Nate Raymond, *Pennsylvania lawyer gets six months in prison for insider trading*, Reuters, July 22, 2016, http://www.reuters.com/article/us-usa-insidertrading-idUSKCN1022JY.
10. Stewart Bishop, *Ex-Hunton Patent Atty Convicted of Insider Trading,* Law360, March 15, 2017, https://www.law360.com/articles/902137/ex-hunton-patent-atty-convicted-of-insider-trading.
11. *Id.*
12. Dixie L. Johnson and Robert Greffenius, *Insider Trading by Friends and Family: When the SEC Alleges Tipping*, ABA Bus. L. Today, June 30, 2011, http://apps.americanbar.org/buslaw/blt/content/2011/08/article-johnson-greffenius.shtml; *SEC v. Goetz*, No. 3:11-CV-01220-IEG-NLS (S.D. Cal. Jun. 3, 2011).
13. *Id.*
14. *Id.*
15. *Id.*
16. *Id.*
17. *Id.*
18. Nate Raymond, *U.S. accuses Chinese citizens of hacking law firms, insider trading,* Reuters, Dec. 27, 2016, https://www.reuters.com/article/us-cyber-insidertrading/u-s-accuses-chinese-citizens-of-hacking-law-firms-insider-trading-idUSKBN14G1D5.
19. *Id.*
20. *Id.*
21. Pete Brush, *Husband of Ex-Linklaters Associate Cops to Illegal Trades*, Law360, Oct 30, 2017, https://www.law360.com/articles/979750/husband-of-ex-linklaters-associate-cops-to-illegal-trades.
22. *Id.*
23. Sara Randazzo, *Ex-Wilson Sonsini Employee Sentenced to Two Years for Insider Trading*, Wall St. J.: L. Blog, July 29, 2015, https://blogs.wsj.com/law/2015/07/29/ex-wilson-sonsini-employee-sentenced-to-two-years-for-insider-trading.
24. Jeannie O'Sullivan, *Ex-Simpson Thacher Clerk Gets Prison for Insider Trading*, Law360, Sept. 14, 2016, https://www.law360.com/newyork/articles/839864/ex-simpson-thacher-clerk-gets-prison-for-insider-trading.
25. *Id.*
26. *SEC Charges Brooklyn Man for Facilitating Insider Trading Scheme Via Post-It Notes at Grand Central Terminal*, SEC Press Release, Sept. 19, 2014, https://www.sec.gov/news/press-release/2014-204.
27. *Id*
28. *Id.*
29. *Id.*
30. *Id.*
31. New York Rules of Professional Conduct, 22 N.Y.C.R.R. Part 1200.
32. *See* definition of "firm" or "law firm" in Rule 1.0(h).
33. *See* Rule 5.1.
34. *See* Rule 1.6(a).
35. *See* Rule 1.8(b).
36. While Rule 1.6 is the general duty to protect confidential information of current clients, Rule 1.9(c) addresses the confidentiality duty owed to former clients, and Rule 1.18(b) addresses the confidentiality duty owed to prospective clients.
37. *See* Cmt. [16] to Rule 1.6.
38. *See* Rule 1.1.
39. *See* Cmt. [8] to Rule 1.1.
40. Melissa Daniels, *How to Stay Safe in a World of Law Firm Data Breaches*, Law360, June 22, 2017, https://www.law360.com/articles/937681?scroll=1ogle.com; *see also Law Firm Cyber Security Scorecard*, Logicforce, 2017, http://marketing.logicforce.com/acton/attachment/21751/f-0058/1/-/-/-/-/lf_cyber_security_scorecard_060317.pdf.
41. *See* Cmt. [17] to Rule 1.6.
42. *See* Cmt. [16] to Rule 1.6.
43. *See* Rule 5.1.
44. *Id.*
45. *See* Rule 5.1; See Rule 5.3, Cmt. [3].
46. *See* Rule 5.2, Cmt. [2].
47. *See* Rule 8.3(a).
48. Note: New York's Judiciary Law § 90(4)(c) requires a lawyer to report his or her criminal conviction by a federal or state court to the Appellate Division of the New York State Supreme Court.
49. *See* Rule 8.3.
50. *See* Rule 8.4.
51. Under New York's Judiciary Law § 90(4)(a), a lawyer convicted of a felony under New York law, or convicted of a crime in another jurisdiction that would constitute a felony in New York, is automatically disbarred.
52. Recently, three hackers broke into several prominent New York law firms and stole M&A information for improper trading purposes. Bob Van Voris, *Chinese Hackers Must Pay $8.9 Million in Law Firm Data Theft*, Bloomberg, May 10, 2017, https://www.bloomberg.com/news/articles/2017-05-10/chinese-hackers-must-pay-8-9-million-for-law-firm-data-theft.