2015 Mendrazycki Essay Competition Winner

Battling a Hack Attack: What to do in the Event a Firm’s Confidential Client Information is Breached

Rikkilee Moser
Northern Illinois University College of Law
DeKalb, IL
MEMORANDUM

TO: Goods, Sterns and Selie, LLP Management Committee
FROM: General Counsel
DATE: February 20, 2015
RE: Potential breach of firm’s confidential material

I. INTRODUCTION

GSS is currently working with an outside IT team to investigate a possible breach of the firm’s networks, and the potential subsequent access to confidential client information. At this time, no determinations have been made, but the following memorandum provides an evaluation of how GSS should respond to several possible outcomes of the investigation. Additionally, the purported information leaked to the media involves several GSS clients as well as one potential client that was never retained by the firm. GSS owes a duty of confidentiality to both current clients and past potential clients per Model Rule of Professional Conduct 1.18. As indicated in the rule: “Even when no client-lawyer relationship ensues, a lawyer who has learned information form a prospective client shall not use or reveal that information.” Model Rules of Prof’l Conduct R. 1.18(a) (2014). Thus, the following analysis pertains to both GSS’s current clients as well as previous potential clients.

I. QUESTIONS PRESENTED

A. OBLIGATIONS WITH KNOWLEDGE OF A BREACH: What obligations does GSS have in the event that it is determined its networks were illegally accessed, but cannot determine what information was accessed?
Short Answer: GSS must contact each client whose information was potentially compromised and notify them that GSS’s system was breached.

B. OBLIGATIONS WITHOUT KNOWLEDGE OF A BREACH: What obligations does GSS have in the event that it cannot be determined whether its networks were illegally accessed?

Short Answer: Even if GSS cannot determine if its networks were breached, it should still contact each client whose information could have potentially been compromised and inform them of the possibility.

C. LIABILITY: What liability does GSS face if it is determined that its networks were illegally accessed, and what can GSS do to minimize that liability?

Short Answer: GSS may be subject to disciplinary action as a result of the breach, as well as action brought by the Attorney General or by a civil claim as a result of failing to notify clients of the breach. In order to minimize liability, GSS should inform its clients of the breach as soon as possible.

D. MINIMIZING FUTURE LIABILITY: What policies can GSS implement to minimize future liability?

Short Answer: GSS can and should strengthen its security and network accessibility with updated servers, password protection, and encrypted data. GSS should also obtain consent from clients to store information on a network as well as secure a waiver of liability, and invest in cyber liability insurance.
II. DISCUSSION

A. OBLIGATIONS WITH KNOWLEDGE OF A BREACH

If the IT team discovers that GSS’s networks were hacked and personal information was accessed, regardless of whether it is able to determine what specific information was compromised, there is no doubt that GSS needs to notify its clients. All but three states (Alabama, New Mexico, and South Dakota) have adopted some form of a data security breach notification law. E.g., 815 Ill. Comp. Stat. 530/1 (West 2015); Kan. Stat. Ann. § 50-7a01 (West 2015). These laws, although each slightly unique, essentially all pronounce that when personal information has been compromised the party who has been breached must notify the victim as expediently as possible. E.g., Ariz. Rev. Stat. § 44-7501 (West 2015). The majority of the laws define a breach as an unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information. E.g., Mich. Comp. Law § 445.72 (West 2015). It is also important to note that even if a breach has occurred, many states have provided an exception to the notice requirement if there is a reasonable belief that substantial harm will not result from the breach. E.g., La. Rev. Stat. § 51:3071 et seq (West 2015).

However, it is improbably that this exception would apply to the present situation. The information leaked to the media about GSS’s clients resulted in withdrawn sponsorships, refusals of contracts, and internal investigations for discrimination. There is no doubt that those circumstances constitute substantial harm, and even if it remains undetermined whether the information leaked to the media was stolen from GSS’s networks, the probability is remarkably high that it was.
Furthermore, the duty of confidentiality owed to a client encompasses any information relating to the representation of that client. Model Rules of Prof’l Conduct R.1.6 cmt. 3 (2014). Thus, if GSS’s networks were hacked it is impossible to deny a correlation between the breach and representation—even if the information accessed is unknown.

In tandem with the duty of confidentiality is the duty of an attorney to properly communicate with his or her clients. A lawyer is required to keep clients informed and provide reasonable explanations so that each is able to make knowledgeable decisions about their representation. Model Rules of Prof’l Conduct R.1.4 (2014). The fact that a breach occurred which likely compromised confidential information is no small matter, and surely is necessary information for a client to possess when making determinations about their case and the representation they are receiving.

Therefore, it is best for GSS to communicate with each client regarding the breach. State statutes require either written or electronic (sometimes telephonic) notice as soon as possible after learning of the breach, unless immediate notice would interfere with a criminal investigation. E.g., Colo. Rev. Stat. § 6-1-716 (West 2015). Thus, assuming that a criminal investigation is not ongoing, in order to comply with Just Win’s Model Rules of Professional Conduct, as well as the theme of the 47 statutes from other states, GSS ought to immediately contact its clients, inform them of the breach the firm experienced, and notify them that their confidential information may have been accessed. If however, law enforcement does pursue an investigation, GSS would be permitted to delay notification until given the all clear by the investigating authorities. See e.g., Tenn. Code Ann. § 47-18-2107 (West 2015).
B. OBLIGATIONS WITHOUT KNOWLEDGE OF A BREACH

In the event that the IT team is incapable of determining whether or not GSS’s networks were illegally accessed, the firm should still inform its clients of the possibility that their personal information was compromised. First and foremost, an “attorney owes the highest fiduciary duty to his or her client.” People v. Martinez, 47 Cal. 4th 399, 420 (Cal. 2009). Most jurisdictions recognize that this encompasses the duty to provide complete disclosures of material facts pertaining to the client’s representation. E.g., Willis v. Maverick, 760 S.W.2d 642, 645 (Tex. 1988). Courts further state that the fiduciary duty between an attorney and client triggers integrity, fidelity, candor, openness, and honesty, while avoiding concealment and deception. E.g., Floyd v. Hefner, 556 F. Supp. 2d 617, 661 (S.D. Tex. 2008).

The 9th Circuit has furthered this idea by holding that even when a fiduciary only has a suspicion that the beneficiary may be harmed, they still have a duty to notify the client. Barker v. American Mobil Power Corp., 64 F.3d 1397, 1404 (9th Cir. 1995). In Barker a fiduciary had suspicions that his client’s funds were being misappropriated, yet failed to notify them or investigate further. Id. at 1402-03. The court held that this was a breach of his obligation to protect his clients. Id. at 1404. Thus, GSS may have a common law duty to inform its clients merely that it suspects a breach occurred.

Along the same lines, it is beneficial to note that Alaska addresses the issue of suspicion in its data security breach notification law. The state requires that notice be given in the event of a breach, or with reasonable belief of a breach. Alaska Stat. § 45.48.090 (West 2015). Thus, if Just Win was to err on the side of caution and mirror Alaska’s
conservative approach to this issue, notification would be necessary despite IT’s failure to
determine one way or another whether GSS has been hacked.

Furthermore, as discussed in the previous section, the state of Just Win requires that
attorneys “keep the client reasonably informed about the status of the matter,” Model Rules
of Prof’l Conduct R. 1.4(a)(3) (2014), as well as “explain a matter to the extent reasonably
necessary to permit the client to make informed decisions regarding the representation.”
Model Rules of Prof’l Conduct R. 1.4(b) (2014). Both of these regulations require that the
attorney keep an open line of communication and inform the client of anything that might
be pertinent to their case. The potential theft of confidential information undoubtedly
p pertains to the case of a client, and is something that the clients ought to be advised of as a
result of GSS’s fiduciary obligations.

C. LIABILITY

If the IT team determines that GSS’s networks were illegally accessed, it will be
prudent to prepare for the consequences. In determining what GSS’s liability would be, it is
first necessary to ascertain the duty owed. It is the well recognized duty of an attorney to
“make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or
unauthorized access to, information relating to the representation of a client.” Model Rules
of Prof’l Conduct R. 1.6(c) (2014). In determining the reasonableness of the attorney’s
actions factors considered include “the sensitivity of the information, the likelihood of
disclosure if additional safeguards are not employed, the cost of employing additional
safeguards, the difficulty of implementing the safe-guards, and the extent to which the
safeguards adversely affect the lawyer’s ability to represent clients.” Model Rules of Prof’l
Conduct R. 1.6 cmt. 18 (2014). The information compromised is clearly sensitive, thus liability may hinge on the likelihood that GSS was going to face a breach, and whether reasonable safeguards were taken to protect the client information. Additionally, the obligation to keep a client’s property safe and secure is also a duty imposed by Just Win state law. Model Rules of Prof’l Conduct R. 1.15 (2014). Property includes any contracts, documents, etc. that the client has entrusted to the attorney. See N.J. Advisory Comm. on Prof’l Ethics, Opinion 692 (2001). In this case, team or sponsorship contracts, as well as employee files would fall into the category of client property.

Furthermore, many states recognize that these duties “[extend] beyond deliberate revelations of client information and [require] a lawyer to protect client information against all disclosure.” Wash. State Bar Ass’n, Advisory Op. 2215 (2012). At least eighteen states have issued advisory opinions pertaining to a firm’s use of cloud computing or online data storage. E.g., id.; N.Y. State Bar Ass’n Comm. On Prof’l Ethics, Opinion 842 (2010). While each state addressing the issue opined that this advance in technology is a permissible practice for a firm or attorney, they each also outlined specific factors to consider when determining whether reasonable care was used when storing information outside of the traditional office setting.

In the event that GSS is found to have failed to comply with these duties, disciplinary action may (but not automatically will) ensue. Furthermore, if a client takes action against GSS he or she will first have to prove an actual injury. If a client who has suffered as a result of the leaked information sues, GSS would have to defend itself against malpractice or negligence. However, if a client attempted to bring suit that had not been directly affected by the breach, GSS would not be liable to them since no injury occurred. See Guin v. Brazos
Higher Educ. Serv. Corp., 2006 U.S. Dist. LEXIS 4846 (holding that threat of harm is not enough to satisfy the injury element in a negligence case).

However, GSS may face additional liability if it fails to respond to this situation in a timely manner. Looking back to the state data breach notification laws—if notice is not provided within the most expedient time possible, the breached party may face action initiated by each state’s respective Attorney General. E.g., W. Va. Code § 46A-2A-104 (West 2015). Additionally, seventeen states also permit civil action to be brought against the party failing to provide notice. S.C. Code Ann. § 39-1-90 (West 2015).

**D. MITIGATING FUTURE LIABILITY**

In order to prevent future attacks on firm networks, GSS ought to implement three simple changes that will increase security and reduce the possibility of liability after a breach. First, GSS should strengthen its network security. This can be done by updating its server system to the most current version. Old server systems lack technical support from the server company and thus are more frequently targets of hacking. Security Matters: The Safekeeping of Case and Client Data, Abacus Law, http://abacuslaw.com/sites/default/files/files/white-papers/Security%20Matters%20-%20The%20Safekeeping%20of%20Case%20and%20Client%20Data.pdf (last visited Feb. 20, 2015). Additionally, security can be strengthened with password protection and encrypted data. If the practice is not already in place, GSS should have unique passwords that are only shared with authorized personnel. Jonathan P. Adams et al., The ABA Cybersecurity Handbook 119 (Jill D. Rhodes & Vincent I. Polley eds., 2013. Moreover, the network clients are given access to should be completely separate from the main network, and should have its own unique password. Id.
Furthermore, GSS should invest in encryption software so that information stored on the network is essentially “scrambled” until the designated user accesses it. Id. at 121. Thus, even if another breach occurred, the attacker would be very unlikely to actually obtain any information.

Second, GSS should inform its clients of our data storage policies, and obtain their consent to store personal information or any data relating to their representation on our networks. It would also be prudent to include that information in the contract with the client and have them acknowledge the risks associated with network data storage. Id. It is very unlikely that a client would wish to have GSS forgo use of technology when the alternatives are slower and more costly, but if they so choose, then GSS would be required to use an alternative method of data storage. See id. This process would limit liability for future breaches since the client would have already waived the risks.

Lastly, GSS should consider purchasing cyber liability insurance. The average cost to respond to a data breach is $3.5 million dollars, and that number is on the rise from last year. Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis, Ponemon Institute (May 5, 2014, 10:15 AM), http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis. GSS’s general liability insurance is unlikely to cover costs associated with a data breach, which would place significant financial strain on the firm it were to suffer another hacking attack. See, Adams et al., supra, at 193. A cyber liability insurance plan would offset numerous incidental costs of another breach, including notification expenses. Id. at 194.
III. CONCLUSION

For the aforementioned reasons, GSS ought to disclose the situation to its clients, whether IT ultimately is able to conclude a breach occurred or not. Timely notice not only ensures that GSS is abiding by its ethical obligations and the law, but it also reduces the chances that GSS will be faced with additional liability via suit brought by the Attorney General or by civil action. Additionally, by taking further precautions regarding network security, client waivers, and cyber liability insurance, GSS will be protecting not only its future clients but the firm’s name and assets as well.