2019 Cyber, Management and Professional Liability Conference
July 10-12, 2019
Boston, MA

Avoiding Malpractice and Bad Faith in an Electronic World

The pitfalls and perils facing claims handlers and lawyers because we practice in an electronic world are legion. Consider: electronic document collection that collects too much or not enough; inadvertent production and inadvertent withholding, either of which can be related to sheer volume; misdirected e-mail because of a "reply all" or autopopulate; informal chatter via e-mail; attaching a draft to an e-mail; incompletely scrubbed template (perhaps sharing HIPAA protected information); data shared via a "shoulder surfer"—and the list goes on.

The rules about managing these electronic risks are fairly minimal. There is the ABA Model Rule 1.1 on competence. Comment 8 to that rule says:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, and engage in continuing study and education and comply with all the continuing legal education requirements to which the lawyer is subject.

As of the end of 2018, 35 states had formally adopted this version of the Model Rule comment. (Alabama, California, Georgia, Hawaii, Maine, Maryland, Michigan, Mississippi, Nevada, New Jersey, Rhode Island, South Carolina, South Dakota, Texas, and Oregon have not). Robert Ambrogi, *Tech Competence*, LS LawSites blog, www.lawsitesblog.com/tech-competence/. Even in those states where technology is not mentioned, though, lawyers are expected to be competent and to remain current in their education and training. St. B. Calif Formal Opinion No. 2015-193 (acknowledging obligation to be educated in relevant technology); Ga. St. B. Rule 1.1, comment 6; Tx. St. B. Rule 1.01, comment 8.

While there is not a similar rule imposed on insurance companies, they are, without exception, held to at least a reasonableness standard in everything they do. From claims handling (Fla. Stat. §624.155; *Seto v. State Farm Ins. Co.*, 855 F. Supp. 2d 424 (W.D. Pa. 2012)), to coverage decisions (*Griffin Dewatering Corp. v. Northern Ins. Co. of New York*, 176 Cal. App. 4th 172, 97 Cal. Rptr. 3d 568 (2009)), to decisions about whether to continue to offer coverage (*Columbia Universal Life Ins. Co. v. Miles*, 923 S.W.2d 803 (Tx. Ct. App. 1996)), claims handlers and insurance companies are expected to act reasonably and in good faith. A fair reading of that obligation includes a duty to keep abreast of current technologies and to both use them and protect against their misuse. This means that claims handlers need to keep in

mind their own interaction with the electronic world, their insureds' interaction with the electronic world, and their defense counsel's interaction with the electronic world.

As noted above, the possibilities for error are almost endless. Given our limited time and space, we mention several of them, simply to raise awareness, and then discuss in greater detail five situations in which electronic errors are common and have led to or can lead to claims. In addition to the situations noted in the opening paragraph, consider:

- Lost or stolen electronic devices or laptop (Model Rule 1.15 regarding safeguarding client property);
- Potential loss of privilege if a client uses company e-mail (American Bar Association Formal Opinion 11-459);
- Claims of unauthorized practice of law because internet makes interstate and global practice possible; and
- Performing a full data collection in a case will cost thousands of dollars and the adjuster must decide whether to authorize the expenditure.

While opportunities for error abound, maintaining awareness and implementing fairly simple solutions can help adjusters and lawyers avoid many potential mistakes.

For example, confirming by telephone can avoid e-mail spoofing. A lawyer who failed to do that will most likely suffer serious consequences. Claimant was a client of Montunui Firm (with apologies to Walt Disney). During the course of the representation, Montunui received wiring instructions from opposing counsel's (Maui) e-mail address and a signed stipulation of dismissal. On January 13, Montunui wired the funds per the e-mail's instructions. On January 19, Maui advised Montunui that he had not signed the wiring instructions, the signature on the stipulation of dismissal had been fraudulent, and his client had not received the funds.

Montunui reported this matter to the FBI. It appears that Maui's e-mail address was hacked. The FBI was able to recover $100,000 of the stolen funds. Even though at no point was Montunui's computer system compromised, and it appears that the issue was strictly on Maui's side, Claimant is seeking the remaining $300,000 as well as costs and has filed suit against Montunui. The opposing counsel whose e-mail was hacked, Maui, was also in the lawsuit. He has since been dismissed, and the grounds for his dismissal and operation of state law mean it is unlikely that Maui will be on the verdict form. This means the jury will only allocate fault between Montunui and the criminal hacker who, predictably, has limited assets.

Despite this ultimately happening because of the criminal acts of a third party, there were serious issues with the Insured Montunui's conduct surrounding the e-mail. The opposing attorney predominantly communicated via letter and fax, not e-mail. There had been a letter from Maui several days prior to his e-mail explicitly rejecting the offer the e-mail purported to accept. Thus, the e-mail wasn't just wiring instructions, it also included a forged signature on a settlement agreement that essentially came out of the blue and was contrary to prior representations made by Maui. In addition to this, the Insured did not call Maui to discuss it with him or verify his acceptance of the offer. The forged settlement agreement also did not include any of Maui's clients' signatures, which meant that it was not completely executed at the time the Insured wired the funds. Any of these precautions could have prevented the fraudulent transfer and a jury may find that the lawyer should reasonably have taken one or more of them.

It is also vitally important that we stay vigilant in warding off the hacking of our own systems. Not doing so led to disaster for a company and its lawyers. Over the course of many years, Law Firm served as risk manager for its client, XYZ Company. It this capacity, Law Firm submitted and managed all claims for losses that were covered under an insurance policy issued by World's Best Insurance Company. All of Law Firm's communications with Insurance Company were via e-mail. Client sustained severe property damage in a summer windstorm and sought to recover insurance proceeds from Insurance Company. On behalf of Client, Law Firm submitted the claim to Insurance Company via e-mail. Insurance Company accepted the electronically submitted claim.

While adjusting the claim, Insurance Company was in frequent communication with Law Firm through its e-mail account and relied on Law Firm to provide instructions on how and where to send settlement funds. Law Firm provided wire instructions to Insurance Company via e-mail and Insurance Company processed the first partial settlement disbursement with the wire instructions provided by Law Firm.

At some point after the first settlement disbursement was made and received, Law Firm's e-mail and/or computer was hacked and its security was compromised. Beginning in October, this hacker monitored and reviewed e-mails being sent to Law Firm's e-mail account and also sent e-mails from Law Firm's e-mail account.

In December, Insurance Company was ready to make a second settlement disbursement on behalf of Client. As with the initial payment, Insurance Company relied upon Law Firm to provide payment instructions. On December 15 at 10:08 a.m., Law Firm sent an e-mail to Insurance Company with instructions to proceed with the settlement disbursement. At 12:58 p.m., Insurance Company sent an e-mail reply stating the "wire will be processed early next week." Less than ten minutes later, at 1:07 p.m., Law Firm thanked Insurance Company for the update and provided the necessary wire transfer instructions.

On December 15 at 1:29 p.m., Insurance Company received another e-mail from Law Firm's e-mail account, which stated "disregard the wire instruction I sent earlier, I just received confirmation e-mail from Client, they are receiving payment into there[sic] Europe alternative account. I will send you the new wire instructions shortly". Unbeknownst to Insurance Company or Law Firm, this e-mail was sent by the hacker using Law Firm's e-mail account.

Insurance Company responded at 2:41 p.m., stating that it will "AWAIT THE UPDATED BANKING INFO." The new wire instructions were then sent from Law Firm's e-mail account to Insurance Company. After receiving the new wire instructions from Law Firm's e-mail account, Insurance Company responded at 3:13 p.m. stating that the new wire instructions would delay payment and urged Law Firm to remain with the prior wire information used for the first settlement disbursement. At 4:07 p.m., the alternative wire instructions were again sent to Insurance Company from Law Firm's e-mail account.

Believing it was following the instructions of Law Firm, but without confirming by telephone, Insurance Company wired the second partial settlement payment to the alternative bank account that was owned and/or controlled by the hacker.

Three weeks later, Law Firm e-mailed Insurance Company inquiring about the status of the partial settlement payment that was expected to be paid in December. At this time, Insurance Company first learned that Law Firm's e-mail account had been hacked and the partial settlement payment had never

been received by the intended recipient. Immediately upon learning of the fraudulent transfer, Insurance Company sent an e-mail to its bank attempting to freeze the wire transfer sent to the fraudulent account in December. Law Firm was copied on this e-mail from Insurance Company. Apparently, the hacker was still monitoring Law Firm's e-mail account because the hacker sent a responsive e-mail from Law Firm's e-mail account stating: "Good luck with that as I already have your money".

Protecting against such hacking can be done in a myriad of ways, first confirming by telephone when there is a change of instructions. Other time-tested strategies to protect the data of firm, carrier and clients starts with being honest with our IT systems' limitations and vulnerabilities. This can be accomplished by hiring an external vendor to test the firm's system in a simulated attack, as well as a true audit of your systems.

Password protection is also a basic protection of which many people lose sight. Strong passwords that include uppercase, lowercase, numbers, symbols and uncommon words or sequencing are a few recommended practices. Additionally, it is important to use unique passwords for each login you may have and not use common words found in the dictionary or those using personal information.

In one case, a corporate acquisition Law Firm faced a legal malpractice case years after its work was completed because it failed to protect the electronic data of its client with proper passwords and/or encryption. The Law Firm created a web portal to store proprietary information, documents, sensitive financial information, etc. Inadvertently, the portal was accessible to the general public and in fact pops up with a routine search of the company in question. Years after the merger, competitors accessed the site and all of the sensitive information. The Law Firm was accused of legal malpractice for failing to take reasonable steps to properly protect, by password, encryption, or otherwise, the confidential information of its client. See, ABA Rule 1.6.

One last point, especially in all our roles requiring consistent travel, is to ensure we are safe when using public WiFi. Cyber criminals routinely use public WiFi access points in airports, restaurants or coffee shops to steal information. One way to avoid this common pitfall is to install and use encryption software such as a virtual private network software ("VPN") onto your laptop which will encrypt everything sent on a public WiFi system. Beth Waller, *Your Cybersecurity Defense Training for 2019,* Virginia Lawyer, 67, 47.

Lawyers and adjusters can also run into trouble when they interact with the internet in their personal capacity. You should always assume that any post you make can be traced back to you. This is especially true for lawyers, most of whom have a visible preference on the internet. It would not be difficult, for example, for someone to Google "Kate Whitlock", the disgruntled customer who commented on "Yelp" and "Kathryn S. ("Kate") Whitlock", the lawyer at Hawkins Parnell & Young, LLP. It is wise to ensure that your "Yelp" or other internet comments or posts will not embarrass or bring disrepute on your, your firm, or your company. Lest we sound extreme, there is a case where the Plaintiff in a legal malpractice case used the tweets of a major Law Firm partner against him and the firm. Although the tweets were completely unrelated to the Plaintiff or his legal matter, the Plaintiff argued that they showed the lawyer was racist and it was that racism, argued Plaintiff, that caused the partner to commit the act claimed to be malpractice.

"Friending" judges, clients, opposing parties and attorneys can create issues or the appearance of impropriety. Courts have required judges to recuse themselves when they are "friends" with either of the lawyers. *Domville v. State*, 103 So. 3d 184 (Fla. 4th DCA 2012). On the opposite end of the spectrum, lawyers cannot, even in their personal capacities, make derogatory comments about judges online. *In re Disciplinary Proceedings Against Kristine Peshek*, https://www.iardc.org/09CH0089CM.html. Nor can lawyers, even if not acting as counsel for a party, participate in an online campaign to get a judge to change her mind and encouraging other also to do so via ex-parte contact. *In re McCool*, 172 So. 3d 1058 (La. 2015). Online campaign's against opposing counsel are also inappropriate. The Florida Bar v. Ashley Ann Krapacs, Supreme Court of Florida, Case No. SC19-277 (02/27/19) (Debra Cassens Weiss, *Florida Bar asks for emergency suspension of lawyer for social media attack of massive and continuous proportions*, ABA Journal, 02/27/2019). Discussions about cases and clients, on a blog, even if the client's names are not used, also is risky business and should generally be avoided. *In re Disciplinary Proceedings Against Kristine Peshek*, https://www.iardc.org/09CH0089CM.html.

So, too, should informal internal communication be avoided. Companies now have many different internal communication that adjusters and lawyers begin to think of as private. It is not. First, of course, the company has the right to access it. Second, it is permanent--even when deleted it can be, and when suit is filed, must be, recovered. In such "private" communications, we have e-mails in which two insurance company employees discussed how they might trick the insured into voiding coverage. We've seen claims supervisors instructing claims handlers to stop entering events in the claim log because a bad faith claim is anticipated. And we have found discussions between husband and wife lawyers about clients who were not mutual that a state bar later found violated Rule 1.6 regarding disclosure of confidential information. *Disciplinary Counsel v. Homes and Kerr*, Slip Opinion No. 2018-Ohio-4308.

Two easy rules that should make all of these unfortunate situations not one in which you find yourself are to assume that anything you write will be read by a judge and to a jury. Imagine how it will sound then. And protect your clients' and insureds' data like you would want your own data protected. Decide if you would be comfortable with your private information if that was what your computer stored. Thinking and acting carefully about data in and data out results in fewer claims that the professional failed to exercise the care required in representing the client or insured.