Utah State Bar Guidance on Cybersecurity Breaches for Law Firms

Unfortunately, stealthy cyber-criminals are increasingly devising new ways of targeting law practices, seeing an opportunity to seize a firm's most valuable assets: their clients and their reputation. The aims of such criminals are twofold, to seize client files—including proprietary credit card, medical, and financial records—as well as extort firms for large sums to return the stolen data. This threat is exceedingly common—with the ABA's annual cybersecurity *TechReport* noting that in 2020, "reports of malicious activity intensified significantly, affecting all corners of life including the legal profession."

With cyber security threats on the rise, and remote work continuing in the wake of the global Covid-19 pandemic, potentially rendering firm security even more tenuous, it's imperative to ensure your practice is protected from this threat. Additionally, if you have been a victim of such crimes, what are your ethical obligations post-breach?

What can you do to avoid a cyberattack?

- Ensure your firm is up to date on all applicable technological safeguards (password protection, secure and authenticator systems that protect against data breaches, and regularly updating relevant software).
- Draft an iron-clad office policy as it relates to all your employees (lawyer and nonlawyer) to ensure they are abiding by the Rules of Professional Conduct and using secure systems for interacting with client data.
- Ensure your staff and attorneys are trained on email and website security practices.
- Schedule a yearly Penetration Test and a quarterly Vulnerability scan to show you where your weaknesses are.
- Draft an incidence response plan to be prepared in case an attack happens.

If you find yourself the victim of a cyberattack, what are your ethical obligations?

A cyberattack that compromises client information imposes immediate ethical obligations on the compromised firm. The following will outline the various Rules of Professional Conduct implicated by cyberattacks yet refrains from considering any state or federal laws that may impose additional post-breach obligations on the firm.

While firms are victimized by such cyber criminals, it's important to consider the ethical liability that may be imposed on a firm that has failed to take reasonable measures to ensure client data is stored safely. The ABA Standing Committee on Ethics and Professional Responsibility's Formal Opinion 483 "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018), cautions that "the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach."

Applicable Rules of Professional Conduct:

- Rule 1.4 (communication), requires lawyers to keep clients reasonably informed about the status of their case and explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." **This obligation necessitates firms communicating the nature of the breach to affected clients as soon as possible.**

- Rule 1.1 (competence), comment 8 states, "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*…" **This recent amendment to the Rule incorporates language indicating that technological compliance is a necessary component of an attorney's overall competency.**
- Rule 1.6 (confidentiality of information), comment 18, "The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) *if the lawyer has made reasonable efforts to prevent the access or disclosure*." **A law practice which fails to ensure that baseline security measures are instituted for the protection of client data are in violation of this Rule.**
    - Rule 1.6(b)(3) allows for disclosure "to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services." **This language indicates that attorneys may contact the necessary authorities when necessary to prevent substantial financial injury to the client.**
- Rule 5.1 (responsibilities of partners, managers, and supervisory lawyers) requires firms to implement strategies to ensure all firm lawyers are abiding by the Rules of Professional Conduct. Comment [2] states, "such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced legal professionals are properly supervised." While, Rule 5.3 imposes the same standard on nonlawyer assistance. **These Rules impose an obligation to ensure that all employees within a practice (lawyer and nonlawyer) are adequately trained to abide by the Rules of Professional Conduct (including competency and confidentiality concerning client data, noted previously.)**