April 2012 *Multnomah Lawyer Ethics Focus*

Identity Theft:
Loss of Clients' Confidential Data

By Mark J. Fucile
Fucile & Reising LLP

Technology has transformed the practice of law over the past generation. For many firms, "file rooms" are now a set of servers—sometimes on-site but increasingly in an off-site "cloud." For many lawyers, "brief cases" are now laptops, tablets and smart phones. At the same time, the mobility that technology affords us brings with it new challenges to safeguard client confidentiality within this new electronic environment. A generation ago, leaving a paper file behind at a restaurant after a lunch meeting with a client would bring a sense of embarrassment until it was recovered. Today, the loss of a laptop loaded with multiple client files in those same circumstances would bring much more than just passing embarrassment.

In this column, we'll first look briefly at our duty to protect client confidentiality and safeguard client property. Then we'll turn to what you need to do if computer equipment is lost or stolen (or your computer is "hacked") and, with it, confidential client data is compromised.

Duties of Confidentiality and Safekeeping

RPC 1.6(a) states our bedrock duty to preserve client confidentiality. The duty is both strict (with few exceptions) and broad (extending to "information relating to the representation of a client"). ORS 9.460(3) echoes RPC 1.6(a) and

puts those duties in statutory form. RPC 1.15-1(a), in turn, charges lawyers with the duty to protect client property in their possession.

The Oregon State Bar late last year issued an ethics opinion (2011-188) on third party electronic storage and the Professional Liability Fund this year amended its basic plan to exclude data loss. We'll look at both in detail later this Spring.

Our fundamental duty to protect client confidential information, however, is aptly summarized in the heading to Comment 16 to ABA Model Rule 1.6: "Acting Competently to Preserve Confidentiality." The precise steps we take vary with the circumstances and are gauged by what Comment 17 to Model Rule 1.6 describes as "reasonable precautions." The precautions encompass both physical and electronic security and cover both our firms and outside contractors we may use to assist us in handling client work.

Computer or Data Loss or Theft

If you suffer a computer or data loss or theft that includes sensitive client confidential information, then (in addition to contacting the authorities as appropriate) you need to tell the clients affected. This duty has two sources. First, under RPC 1.4(a), lawyers have a duty to "keep a client reasonably informed about the status of a matter[.]" Of note in this regard, files are generally considered client property in Oregon under OSB Formal Ethics Opinion 2005-125 (at 333 n.2). Second, under the Oregon Consumer Identity Theft Protection Act

(ORS 646A.600-646A.628), firms must notify clients if certain specific classes of information are stolen, such as Social Security numbers, drivers license numbers or financial account numbers. ORS 646A.604 describes the content of the notice and ORS 646A.602(11) outlines the kinds of personal information that trigger the notification requirement. If your firm has offices or clients beyond Oregon that are affected, then you would need to consult the rules and laws in those other jurisdictions as well.

The PLF has developed some excellent practice aides addressing both data security and data loss. They touch on both the ethics rules and the Oregon Consumer Identity Theft Act. The practice aides are available on the PLF's web site at www.osbplf.org. Included among them is a sample notice to clients in the event of a data theft or loss. The sample notice can be tailored to client-specific circumstances or to client-wide data loss. The PLF also has practice management advisors available to help craft security plans tailored to firm size and practice focus.

Summing Up

Simply reading the PLF's sample notice and imagining having to send it to all of your clients should motivate us all to implement rigorous programs to keep client information secure.

ABOUT THE AUTHOR

Mark J. Fucile of Fucile & Reising LLP focuses on legal ethics, product liability defense and condemnation litigation. In his legal ethics practice, Mark handles professional responsibility, regulatory and attorney-client privilege matters and law firm related litigation for lawyers, law firms and legal departments throughout the Northwest. He is a past member of the Oregon State Bar's Legal Ethics Committee, is a past chair of the Washington State Bar Rules of Professional Conduct Committee, is a member of the Idaho State Bar Professionalism & Ethics Section and is a co-editor of the OSB's Ethical Oregon Lawyer and the WSBA's Legal Ethics Deskbook. Mark also writes the monthly Ethics Focus column for the Multnomah (Portland) Bar's Multnomah Lawyer, the quarterly Ethics & the Law column for the WSBA Bar News and is a regular contributor on risk management to the OSB Bar Bulletin, the Idaho State Bar Advocate and the Alaska Bar Rag. Mark's telephone and email are 503.224.4895 and Mark@frllp.com.