Law Firm Employees Allegedly Misbehaving Make Headlines

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke

You don't have to go back far in history to read about the many misbehaviors of law firm employees. Whether the media stories concern the alleged actions of partners, associates or support personnel, there is plenty of fodder to make law firms rethink its hiring practices and firm culture to keep the firm name out of the headlines. Unfortunately, they aren't always successful in achieving that goal. While we don't have first-hand knowledge of the details, there are several examples of alleged misbehavior that we can learn from.

Data theft

One major risk for law firms is the theft of data by current and/or ex-employees. Typically, that means client confidential data associated with a legal matter and/or client contact information. In other words, data that can be used to take the business to another law firm or assist in the starting of a new firm.

Jonathan O'Brien, the former chief operating officer for Proskauer Rose, is accused of stealing sensitive internal information. According to the lawsuit, O'Brien is alleged to have tricked firm employees into allowing him to copy 34 gigabytes of client and compensation data prior to his giving notice of leaving the firm. O'Brien has denied the firm's claims that he intended to take the data to another employer. He said that the data was needed to allow him to work during his two-week vacation to Mauritius.

In another case, Littler Mendelson sued ex-associate, Uliana Kozeychuk, for uploading more than 7,900 documents to an external Dropbox account, which included proprietary firm and client confidential data. Bloomberg Law reported that Kozeychuk said in an interview, "They know that I didn't take any documents and they did it as a smear campaign to silence me and make sure that nobody believes me when I finally get around to speaking about them."

Abuse of client assets

Inappropriate activity isn't restricted only to firm data. Lawyers are also entrusted with client assets. A former Miami Beach law firm employee, Susan Rolle, is accused of stealing from an elderly woman under the guardianship of the Kahn & Kahn law firm. The former employee allegedly used a client's credit card to rack up close to $600 of charges at Publix, Victoria's Secret, McDonald's Family Dollar and Walmart. In addition, she is accused of writing herself a $5,290 check from the client's trust account.

Another example involves a former paralegal, Betty Louise Sutton, at Saul Ewing Arnstein & Lehr in Chicago. Sutton is alleged to have transferred bankruptcy funds in excess of $600,000 for creditors to a different account that she controlled. Prosecutors allege that a credit card account, mortgage account, student loan account, personal bank account and a PayPal account she created were used to receive the transferred funds.

Document falsification

You would think that a lawyer's involvement in the falsification of documents would be related to the representation of their clients and not the activity of the lawyer themselves. Our next example of misbehavior comes from the state of Illinois. As reported by the ABA Journal, attorney James Thomas Rollins agreed to make a $100,000 capital contribution in exchange for ownership in an asbestos-defense firm along with three other lawyers. The contribution would be adjusted for any expenses he paid for startup expenses.

Apparently, he submitted false invoices for $81,000 to represent startup expenses when the actual expenses were only $18,000. In other words, he tried to cheat the firm out of $63,000. When challenged, he submitted phony bank statements and fake checks. Not a good idea to take a bad action and dig a deeper hole. An Illinois review board recommended a five-month suspension.

BEC victim

According to the FBI's 2023 Internet Crime Report, Business Email Compromise (BEC) was responsible for $2.7 billion in financial loss for 2022. Lawyers, especially those handling wire transfers of funds, are at significant risk of being targeted in a BEC attack. A lawsuit filed in Connecticut Superior Court on April 24, 2023 by Lesley Moody said the title to her recently purchased home is encumbered by the seller's mortgage as a result of a Connecticut lawyer sending part of the proceeds to the wrong bank account.

Allegedly, the seller's lawyer, William Cote, wired over $159,000 to a fraudster's bank account after receiving phony payoff instructions. In a classic BEC scheme, apparently, his paralegal received an email from someone claiming to be the seller with a change in wiring instructions. The funds were transferred to the wrong account instead of being paid to Freedom Mortgage Corp. as should have occurred.

Solutions

While the above examples are unfortunate experiences for law firms, there are some things you can do to stop or limit misbehaviors. One of the first things that comes to mind is the concept of "least privilege." Users should only have access to information needed to do their jobs. You can also implement technology that monitors data access and logs activities. As a minimum, your firm should have written policies for acceptable practices. This would include policies for internet usage, remote access, social media policy, privacy policy, acceptable computer usage, BYOD, etc. As a bonus, policies don't cost you anything except the time to develop them.

Watching the money should also be at the top of your concerns. Your office procedures should have a process of checks and balances to reconcile the firm financials. It's not just about balancing a checkbook every month, but client funds in a trust account should be reconciled at least monthly with that reconciliation being verified by second person.

You should also have a procedure for verifying that a money transfer request is valid. Don't count on instructions in an email. Make sure you call the person authorizing the wire transfer at a phone number known to you to be good. You may also consider having a code word for verification of wire transfers that periodically changes. In addition, you should be performing security awareness training, at least annually, to educate employees in secure practices and recognition of the latest phishing, smishing and similar attacks. If you haven't seen it already, your cyberinsurance carrier will likely require periodic security awareness training and a written procedure for validating wire transfers.

You are particularly at risk when an employee leaves the firm, whether on good terms or not. According to the 2023 Insider Risk Investigations Report from DTEX Systems, there was a 35% increase in data theft incidents caused by employees leaving a company. On top of that, 12% of employees took sensitive IP (sales contracts, customer data, health records, employee data, etc.) when they left.

What can you do about the potential theft of firm data? You can start by banning the usage of non-firm approved devices. In addition, you should have an employee termination checklist. Don't forget to disable the departing employee's user access to the firm network and any third-party services the firm uses. Make the employee sign a statement that they have surrendered all firm assets and no longer possess any firm data.

Think your employees aren't misbehaving? You might be right – or you might be wrong. Better to be prepared!

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com*