Victims of Social Engineering Fraud: A Trend You Do *Not* Want to Follow

By Scott R. Schaffer, Antonella G. Dessi and Rebecca F. Rose

The emergence of a worrisome trend involving email hacking is plaguing law firms that find themselves involved with wire transfers of client funds. Primarily, these schemes tend to target real estate attorneys, although we have seen sporadic application of these frauds in other practice areas. Typically, the email hacking is carried out at or about the time of a real estate closing and almost always involves the transmission of fraudulent wire transfer information to the law firm. This causes the firm to unknowingly wire transfer monies into a bank account that can be accessed by the hacker. More often than not, the funds are unrecoverable, as the hacker withdraws the money before the fraud is detected. As the true intended recipient of the funds never receives the money, these "social engineering" schemes, as they are known, open the law firm up to claims from clients, banks and various other parties. The following real-life scenarios convey some important lessons from attorneys who have fallen victim to social engineering fraud.

SCENARIO 1

Law Firm represented Client, a seller, at a real estate closing. In fact, Law Firm had represented Client on numerous occasions in similar engagements. Client was to receive a wire transaction of $100,000, representing the sale proceeds. Unbeknownst to Law Firm, however, its paralegal's email was hacked prior to closing and the hacker sent a series of emails, purporting to be from Client, instructing Law Firm to wire funds to an account at Bank. Law Firm wired the sale proceeds to the account provided in the emails, only to learn later that the instructions were fraudulent. The fraud was discovered after Client called Law Firm to inquire about the funds, which had not been received. Client demanded the amount of the wire transaction, plus additional funds to compensate Client for the costs of taking out a loan to keep his business running. It remains unknown whether Bank will be able to recover any of the funds wired to the fraudulent account.

While Law Firm was a victim of social engineering fraud, the erroneous transfer might have been avoided. The fraudulent emails were sent by a "dummy" account that was created to look almost identical to Client's real email account. The emails purportedly sent from Client, whose email display name would typically appear as "john doe [doej5000@gmail.com]," appeared as "john doe [doej5000@mail.com]." With only the "g" from the "gmail" account omitted from the address, the email name change was easily overlooked by Law Firm. As a takeaway, lawyers should meticulously review emails containing sensitive information such as wire transfer instructions and bank account numbers to ensure that they were sent by the appropriate party. In today's age of electronic communication, a simple telephone call to Client for confirmation purposes would have immediately alerted Law Firm to the fraudulent nature of the emails and the wire transfer of funds to the improper bank account would have been avoided.

Scenario 2

In another matter involving a real estate transaction, Law Firm represented Client, a seller, at a closing. Client was to receive the sale proceeds of $200,000 via wire transfer to her account with Bank. To this end, Client provided Law Firm with a voided check from her bank account containing the appropriate routing and account numbers. Prior to the wire transfer, however, Law Firm received an email, purportedly from Client's real estate agent,

indicating that Client wanted the funds wired to another account due to technical issues. Following the wire transfer, it was discovered that the email was a fraudulent result of a breach of the real estate agent's email systems. Client demanded the sale proceeds from Law Firm.

Here, too, certain preventative measures could have been taken to avoid the fraudulent transfer. The email purporting to be from Client's real estate agent contained the following language: "Due to tech issues with the seller's account seller wants proceeds wired to her personal company's account pleeze send me the info you need to initiate the wire." In this instance, noting the improper grammar and spelling, Law Firm might have paused before proceeding with the wire transfer. In this regard, attorneys should always be suspicious of unsophisticated language in emails, particularly when there are prior communications from the alleged sender that can be used as a reference. As a general rule, a change in wiring instructions to a different account should always raise red flags and, again, a telephone call should be made for verbal confirmation.

SCENARIO 3

Law Firm represented Client in connection with a stock purchase agreement for the sale of Client's business. As part of the sale, $1 million was transferred to an escrow account with Bank and was to be released on a certain date once specific conditions were met. Buyer was to pay an additional $200,000 if various other conditions were met. The required conditions were met, and Buyer became obligated to transfer funds totaling $1.2 million to Client. Seller provided Law Firm with wiring instructions via email and Law Firm was to provide the wiring instructions to Bank and Buyer. Before this could be accomplished, however, Law Firm's email was intercepted by a fraudulent third party. Different wiring instructions were provided to Bank and Buyer via phony email purporting to be from Law Firm. As a result, Bank and Buyer transferred funds to the incorrect bank account.

In this scenario, various other emails exchanged among the parties were also intercepted, such that it is unclear which party's email system was breached. This example demonstrates the incredible sophistication of some of these schemes. Attorneys should be extra cautious when emails containing sensitive information are exchanged among multiple parties, as this creates more opportunities for a security breach. Once again, the simple extra step of reaching out to all involved parties by telephone for verbal confirmation of the wiring instructions would have gone a long way toward preventing fraud.

SCENARIO 4

Law Firm represented Client in connection with the purchase of real estate for $250,000. At closing, Law Firm provided a $250,000 check from its escrow account to Seller's counsel. On the same date, Law Firm received two emails, purportedly from Seller's counsel, requesting that Law Firm instead transfer the proceeds into Seller's counsel's trust account. A few days later, Law Firm received a follow-up email, again purportedly from Seller's counsel, indicating that counsel had destroyed the $250,000 check and wanted the proceeds wired to Bank that day. On the same date, and without confirming that the check had, in fact, been voided, Law Firm's paralegal wired the $250,000 sale proceeds to Bank. Several days later, Bank's fraud risk manager advised Law Firm that the wire transfer was part of an email hacking fraud. Law Firm then discovered that the check provided at closing had not been voided but was actually cashed by Seller's counsel. While this particular social engineering fraud did not result in a loss to a third party, the wire transfer from Law Firm's attorney-client trust account caused a recognizable, albeit unrealized, loss to one or more of Law Firm's other clients that had funds in the trust account at the time.

There are several valuable lessons to be learned here as well. This scenario again demonstrates the importance of being wary of a sudden change in instructions, and the need to follow up with verbal confirmation. Here, there was no confirmation directly with Seller's counsel regarding the change in instructions or verification that the

previously issued check had been voided. Although it would appear to go without saying, attorneys should carefully oversee the actions of their paralegals, assistants and staff particularly where client monies are concerned.

CONCLUSION

These scenarios are actual examples of the recent and growing trend of social engineering fraud that is victimizing law firms. By following the simple recommendations, law firms may be able to avoid exposure and protect client relationships from risk.