McGowanPRO
Professional Liability Insurance

Fraudulent Transfer Scams

Plaguing CPAs

Be very wary of emails requesting fund transfers from hacked accounts.

We've recently seen two phishing scams that have resulted in fraudulent client fund transfers. While the amounts are typically not large (under $100,000), in both cases there were multiple transfers. The losses are different but the claims are essentially identical.

Each of our insureds received an email requesting transfer of funds, and in both cases the email requested that monies be wire transferred from their accounts to a Wells Fargo account. These fraudulent emails included significant identifiable personal details and signatures on faked transfer forms. Signatures were verified against signatures from other valid transfers and determined to be authentic—so they thought.

In one case the bank asked for a phone number to verify the transfer as the transfer form was slightly hard to read (red flag). An email was sent to the hacked account requesting a cell number to verify the transfer. In an email response the sender asked if they could call the bank to verify, and this was allowed as the caller had the correct banking information, social security number and other personal identifying information details to convince the bank to move forward and transfer the funds.

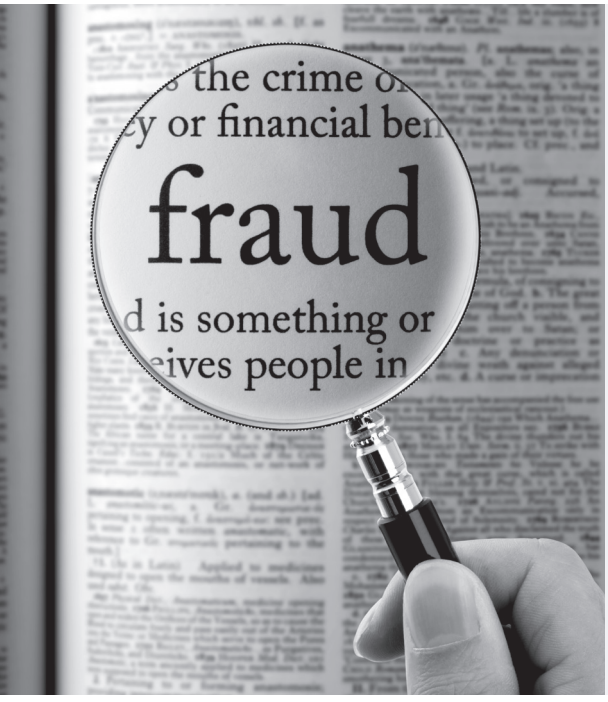
Both of our insureds' clients have been asked to be made whole, and we are in the process of determining the liability associated with each claim.

With one of these claims, the bank clearly has some liability as it did not follow written protocol and allowed a deviation of standards by accepting a "call in" as opposed to the "bank calling out."

Side note: both of these clients are longstanding, very profitable accounts, and our insureds are trying to mitigate damages to maintain the relationship.)

OK, now that you have read the claim summary what's next? Your office needs to take steps to reduce your liability while protecting and safeguarding your clients' assets.

Here are several steps that you should incorporate into your due diligence internal controls:



1 Email requests must be verified by a second means of verification.

In many cases a text message to a cell phone can insure some protection. The theory is that hacked email accounts are usually done from a far (Russia, China, West Africa), and the hackers would not be in possession of the cell phone. Additionally, the text message could include a request for an additional identification password that may not be known by hackers (for example, frequently we see questions like name of their dog or name of their high school). Also often emails have been hacked weeks before the owner becomes aware, and the hacker waits to gather information to be used fraudulently. On the other hand if your cell phone is missing for more than four hours you start to panic and take steps to prevent misuse.

2 Be suspicious and examine emails closely, looking for 'red flags' such as misspelled words, forms that appear to be scanned and are slightly illegible, salutations that are not consistent with other email correspondence.

In some cases a word seems out of place or used incorrectly. In other cases our insureds received numerous follow-up emails asking for details on when exactly when the transfer was completed which showed a level of desperation.

3 *Include internal protocol procedures stipulating that your employees have a second person review and sign off.*

If possible include the key person in the office that has the relationship with the client, as they may have more personal knowledge of the client and sense a fraudulent request.

4 *For larger transfers, elevate the due diligence, requiring absolute second live verification before transfer of funds.*

5 *Consider adding language to the engagement letter that states you will make every effort to verify transfers, and in cases where you are unable to verify the validity of the transfer you will refuse until satisfied that it is an authentic request.*

By incorporating these preventative measures, you could thwart criminal fraud and build your defense should the fraud occur.

See www.mcgowanprofessional.com for more Information Security & Data Privacy Liability resources. And contact McGowanPRO to discuss your information security liability today.

Contact

McGowanPRO
150 Speen Street, Suite 102
Framingham, MA 01701
Phone: 508.656.1300
McGowanProfessional.com

McGowanPRO
Professional Liability Insurance