Breached Law Firms Bemoan: "The Class Action Attorneys Have Found Us"

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

Remember the Golden Ticket from Willy Wonka?

A lot of lawyers thought they had discovered a golden ticket when they discovered ChatGPT. They were enthused about how fast it was and how they could utilize it for legal research, drafting legal documents, case analysis, legal compliance, composing client communications and the list goes on. It was dizzying in its speed and the conversational language was irresistible – and understandable.

Sadly, many lawyers did not comprehend that they were feeding confidential data to the AI, and that the history of their conversations with ChatGPT could be recalled and even used to train the AI.

If you were keeping an eye on developments, you might know that OpenAI, the creator of ChatGPT, announced on April 25 that it had added the option to turn off chat history for ChatGPT, which meant you could keep your confidential data safe. But if you weren't watching developments – and many lawyers were not – you blithely went along feeding your data to the AI.

There was a reason that Apple and Samsung prohibited the use of generative AI - in Samsung's case, employees unintentionally leaked confidential data. Apple likely feared the same fate. Some law firms have also prohibited the use of ChatGPT. But many more have not, and therein lies the threat.

Timing is Everything – and the Timing is Terrible

Along with the knowledge that many lawyers may have inadvertently given confidential data to ChatGPT, law firms managing partners are facing a tidal wave of law firm data breaches. We have never seen so many law firm data breaches in such a short period of time. It's a one-two punch of considerable proportions.

While some of the reported breaches are only coming to light in 2023, many of the breaches have taken place in 2023, the very time when ChatGPT became much more commonly used.

It really has become "open season" for law firms being the target of so many cyberattacks – thereby endangering the security of their proprietary data. And if you want one more reason to groan, ChatGPT is a great tool for cybercriminals who want to craft better and more effective phishing emails. No more spelling and grammatical errors to shout "phishing email!" at law firm employees.

In late June the UK's National Cyber Security Centre (NCSC) released a threat report indicating that cybercriminals are laser-focused on going after law firms. The NCSC has reported that nearly 75% of the UK's top 100 law firms have been impacted by cyberattacks.

Do you really think it's much different in the U.S.? We certainly don't.

Class Action Lawsuit Attorneys and Data Breaches

Following the reports that Bryan Cave Leighton Paisner had suffered a data breach came word in late June that a class action lawsuit had been filed against the firm. According to a data breach report by

Mondelez, the firm's client, more than 51,000 current and former employees' data was acquired by the attackers who breached the firm.

The complaint said that Bryan Cave was hired in part to provide data and privacy advice and accused the firm of negligence, breach of implied contract, breach of contract, unjust enrichment and invasion of privacy.

We suspect that further class action suits will more rapidly follow the revelation by any law firm that it has been breached. This will no doubt be the despair of the breached law firms who understand full well that class action lawyers receive very handsome rewards for their successes. Class members? Not so much.

The authors have noted that as we have been offered a paltry award of $7.50 for the settlement recently agreed to by Google after it was accused of "storing and intentionally, systematically and repeatedly divulging" users' search queries and histories to third-party websites and companies. Wow! A whole $7.50 to waste energy filing out a form and assembling documentation.

We're not saying that class actions don't have their uses, but a storm of law firms filing class action lawsuits against other law firms is going to complicate an already complicated data breach landscape.

Law Firms Need to Pony Up More Cybersecurity Funding

Considering the double whammy of leaked confidential data and a steep increase in data breaches, it is time for law firms to get serious about battling data breaches. PriceWaterHouseCoopers' Annual Law Firms Survey reported that the top 1000 law firms spent less than 1% (only .46%) of their fee income on cybersecurity.

We've heard all the excuses. "It costs too much." "It takes too much time." "It takes too much training." "We have cyberinsurance." That last one could be the subject of another column. Read your policies carefully. Most of them now have strict requirements for your cybersecurity – if it turns out you didn't abide by the requirements, there may be no payout. A good many policies will not cover the payment of ransoms or will not cover damage resulting from state-sponsored attacks. Frequently, you are paying more and getting less.

Final Words:

One lesson from the recent rash of law firm data breaches is this: "If you can't afford strong cybersecurity, you sure can't afford a data breach."

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*