Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Lawyers' Data Targeted In String Of Bar Association Hacks

By **Xiumei Dong**

Law360 (December 11, 2020, 8:01 PM EST) -- The Washington State Bar Association restored a website portal it uses to license new members on Thursday, nearly a month after the bar group had taken it down following the discovery of a cyber intrusion.

On Nov. 13, the bar association informed its members and the public that it had been hit with a cyberattack, potentially exposing payment card information and other personal information registered on its website, myWSBA.org.

The association disclosed more details of the attack on Nov. 16, saying it discovered that a "malicious code that targets credit card numbers" was introduced to its website. However, the association said it didn't know whether the hackers accessed any credit card information.

"As soon as we detected the issue, we disabled the website and launched an investigation," the group said in a statement to Law360. It said it enlisted a digital forensics firm to work on the investigation and is in the process of notifying "those whose payment cards may have been affected during the incident."

A spokesperson for the group said it is also in the process of notifying regulatory authorities, including the state attorney general's office, about the event.

The Washington State Bar Association is just one of a handful of legal professional associations to have reported a cyberattack targeting lawyers' information this year, according to public records and cybersecurity experts.

The Los Angeles County Bar Association and Pennsylvania Bar Association also discovered malicious code invading their websites earlier in the year, according to reports they filed with state attorneys general. Meanwhile, the New York City Bar Association and the Chicago Bar Association reported having found malicious code affecting a third-party vendor they used for their websites.

To date, none of the bar associations have reported knowing the source of the attacks or whether the attacks are correlated. According to cybersecurity consultant John Reed Stark, "malicious code" can describe a number of different attacks, such as computer viruses, worms, Trojan horses or malicious scripts.

"Bar associations are large, sophisticated organizations with very high-net-worth members, so from that perspective, they are certainly a target-rich environment, in terms of identity theft and other types of crimes related to data theft," said Stark, president of data breach response and

digital compliance firm John Reed Stark Consulting LLC.

Thousands of Bar Members' Info Compromised

Aside from the Washington State Bar Association hack, most of these attacks were discovered either in late spring or early summer, according to reports filed with state authorities. In one incident, cyberattackers were reported to have gained access to a bar association's data as early as April.

In a report filed with the Maryland attorney general's office in late May, the Pennsylvania Bar Association said it had been notified around April 7 that certain members had discovered suspicious activity in their financial accounts, which quickly led to the discovery of "malicious code embedded in its website."

The Pennsylvania bar group said it had removed the code on April 8, but later added that it was informed of a similar incident on April 21. According to the report, an unauthorized individual had access to some names and credit card information entered into the association's website, although it was still investigating the incident.

"There was a possibility as many as 2,752 customers were impacted," Francis J. O'Rourke, deputy executive director of the Pennsylvania Bar Association, said in a statement to Law360. "All of those potentially impacted were notified and reports of the data issue were made to all government agencies as required."

Similarly, in a letter sent to its general members on July 14, the Los Angeles County Bar Association said it had notified a group of approximately 2,632 members about a data breach, which it said appeared to be "a scheme by cybercriminals that targeted a number of other large bar associations and other professional organizations."

The LA bar group became aware of the attack on June 11, but its investigation later revealed that hackers had placed code on its website as early as May 10, it said.

"The malicious code functioned by copying information as it was typed on the website and transferring it to a server operated by the cybercriminals," the group said in the letter.

For most of the members who were notified, the breached information included their name, password, attorney bar number and any other data they had shared with the website, while a group of less than 370 members also had their payment card data breached, the letter said.

The Chicago Bar Association did not respond to Law360's requests for comment on the scope of its breach. The New York City Bar Association and its City Bar Fund said that "a small fraction" of the bar's membership was affected but declined to provide the exact number.

Malicious Code That Captures Payment Data

Both the New York City and Chicago bar groups' breaches involved credit card information that was potentially gathered through unauthorized code inserted into a third-party commerce and management software called iMIS, which they used on their websites, according to notice letters filed with the Maryland attorney general's office this summer and recently obtained by Law360. Breaches are typically reported to each state where residents have been impacted.

The New York City bar group said the code was present on its website between April 23 and May 1. The Chicago bar group reported that its investigation showed the code had acted as "a credit

card skimmer" between May 22 and May 28.

"As a result, the malicious code may have allowed an unauthorized individual to collect credit card data from transactions that occurred within this time period," Chicago Bar Association counsel Ernest Koschineg of Cipriani & Werner wrote in a letter dated July 13. "Importantly, the vulnerability, as well as the malicious code, has been removed."

In a statement to Law360, New York City Bar Association communications director Eric Friedman said the group had removed the unauthorized code from its web server, notified law enforcement and launched an investigation into the matter.

To help prevent a similar breach from happening, Friedman said the group has "implemented advanced malware protection software with enhanced monitoring and alerting capabilities."

The Pennsylvania Bar Association's O'Rourke told Law360 that his group has also "implemented several new security enhancements to prevent future incidents and alert its IT staff to potential malicious activity."

According to Claudia Rast, Butzel Long PC's cybersecurity group leader and co-chair of the American Bar Association's cybersecurity legal task force, bar associations and other legal entities have long been targets for cyberattackers for hosting substantial amounts of attorneys' confidential information.

"If you go behind what we call the paywall in the state bar, you have the name, address, phone number, you have a tremendous amount of information about those individual attorneys who have access to client information," she said.

While it is important for bar associations to enhance their security systems, it is even more important for attorneys to incorporate safe practices themselves, Rast said.

Because attorneys are often considered a "trusted source," if a bad actor uses a breached attorney account to send malicious emails, it is more likely that people will respond, she added.

"As individuals we not only represent risks to ourselves, but we represent risks to those we work with, and the companies we work for, so we have to be incredibly vigilant individually," Rast said.

Since early this year, cybercrimes have been on the rise as a result of the COVID-19 pandemic that forced much of the world into working remotely. Law firms, which handle large amounts of sensitive client information, data and money, are also **increasingly becoming** attractive targets for cyberattackers.

In October, Seyfarth Shaw LLP and Fragomen, Del Rey, Bernsen & Loewy LLP both disclosed **security incidents**, including a **malware attack**, that put clients' sensitive information at risk.

--Editing by Aaron Pelc and Nicole Bleier.