Law Firm Data Breaches Surge in 2023

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

Large and Small Firms in the Data Breach Headlines

Headlines about successful outcomes in litigation are welcome. Headlines about law firms which have suffered a data breach are considerably less welcome.

No one really expected that 2023 would be a banner year for law firm data breaches (some of which were reported in 2023 but occurred earlier). Yet the number of breaches that took place in 2023 is astonishing. Even more astonishing is that cybercriminals appear to be successfully hitting small and large firms alike.

And it's not just a U.S. problem. In the UK and France, national cybersecurity agencies issued a warning that law firms should upgrade their security, specifying security designed to defend against ransomware attacks.

Three Top 50 Law Firms Breached

In July, we learned that three top 50 law firms had been breached: Kirkland & Ellis, K&L Gates and Proskauer Rose. All were breached by the ransomware group Clop. If these very large firms could be breached, who is safe?

Also breached were Loeb & Loeb (the incident occurred in 2022) and Orrick, Herrington & Sutcliffe (breached in the first quarter of 2023).

Class Action Suits Have Followed

2023 appears to be the year in which class action firms have discovered fertile ground in law firm data breaches. As of July 2023, five class action suits have been filed against Bryan Cave; Cadwalader, Wickersham & Taft; Smith, Grambrell & Russell, as well as two smaller firms – Cohen Cleary and Spear Wilderman. The lawsuits against Cadwalader and Smith Gambrell have since been dropped.

The basis of the suits was fundamentally the same – that the law firms did not have adequate security to protect their data from cyberattacks.

It amazed us how many smaller firms reported data breaches in 2023. They certainly need to up their cybersecurity game, especially in light of the class action suits that are proliferating. There has been a 154% increase in the last year in federal data breach class actions. Truly a surge! The pre-trend lawsuit average was 13 each month – it has escalated to 33 per month now.

Want another headache? Some federal courts are finding that post breach security assessments may not be privileged.

Government Regulators Are Taking Action

In January of 2023, the Securities and Exchange Commission subpoenaed Covington & Burling over a 2020 attack which may have resulted in client data being taken. While the law firm fought back and enlisted support from many other law firms, the SEC seems to have scored a partial victory. The SEC wanted the names of 298 publicly traded clients whose data may have been exfiltrated.

It didn't get anything that broad. U.S. District Judge Amit Mehta ordered on July 24 that Covington and Burling give the SEC a list of seven clients whose material nonpublic information may have been accessed by Chinese hackers.

Judge Mehta wrote, "The court finds some merit to both parties' positions, but ultimately holds that the SEC's demand for the names of affected clients does not exceed its statutory authority or cross any constitutional lines."

It was immediately clear that neither the SEC nor the law firm liked that ruling so the odds are high that the ruling will be appealed.

Covington argued that it has a duty to keep client names confidential. It also said that the SEC's demand for client names could damage relationships between law firms and clients and could cause victims of cyberattacks to decide not to consult with law firms.

Covington also warned, backed by many law firms, that victims could be disincentivized from reporting breaches to the federal government. That's critical because the U.S. government relies on voluntary cooperation from victims to comprehend the scope of hacks and respond.

Judge Mehta, in his opinion, did not disagree, writing "The SEC's approach here could cause companies who experience cyberattacks to think twice before seeking legal advice from outside counsel. Law firms, too, very well might hesitate to report cyberattacks to avoid scrutiny of their clients."

Mehta noted that "[t]he court's role, however, is limited. Its task is only to assess whether the subpoena exceeds the SEC's statutory authority or fails to meet minimum constitutional requirements. It is not to pass on the wisdom of the SEC's investigative approach."

Mehta's ruling requires Covington only to "disclose the names of the seven clients as to whom it has not been able to rule out that the threat actor accessed material nonpublic information."

He also wrote, "In the court's estimation, the SEC has not made the case that it needs the names of the 291 clients whose material nonpublic information Covington has determined was not accessed. Those clients, by the SEC's own admission, are not relevant to its investigation. Therefore, the court is not prepared to grant the SEC access to a client list of nearly 300 names when only seven are actually needed to satisfy the agency's stated law enforcement interests."

The judge considered the SEC's argument that it could not "independently verify" Covington's conclusion that other clients had not had their data accessed but determined that didn't mean that the SEC should get the full list of names.

Ugly Statistics on Law Firm Breaches

Checkpoint Research reported in April that cyberattacks rose by 7% in the first quarter of 2023 when compared with the first quarter of 2022. All sorts of organizations, in the first quarter, experienced 1,248 attacks. What caught our attention was that one out of every 40 attacks targeted a law firm or an insurance provider.

As we have often pointed out, law firms are prime targets because of the extensive data they hold of government entities as well as corporations. Experts have consistently noted that many law firms fall short of best cybersecurity practices.

Many of our clients are law firms, so we have some expertise here. Why do law firms sometimes fail to take adequate security measures? Here are the usual reasons we hear:

- It's too expensive. Note this: IBM's *Cost of a Data Breach Report*, released in late July, found that half of breached organizations are not willing to increase their cybersecurity budget. It also found that only 1/3 of data breaches are discovered by an organization's own security team. 27% are disclosed by the attacker.
- It will interfere too much with our operations.
- We're not really a target for cybercriminals.
- Our employees already have security fatigue - this will make it worse.
- Legal ethics rules don't require this.

Short-sighted? Yes, it sure is. Several clients have paid dearly for refusing to use multi-factor authentication. And as you might guess, after they got hit, they couldn't adopt MFA soon enough. As to ethics rules, they require reasonable cybersecurity – and what's reasonable has changed significantly over time.

In fairness, cybersecurity can indeed be expensive – and one of our prime directives to our IT/cybersecurity team is to find affordable solutions for our solo/small/midsize clients.

Happily, such solutions do indeed exist!

Final Words

"Time is the new currency in cybersecurity, both for the defenders and the attackers. . . early detection and fast response can significantly reduce the impact of a breach" – Chris McCurdy, GM Worldwide IBM Security Services.

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*