Case Study

SHORE v. JOHNSON & BELL

THE CATASTROPHIC POTENTIAL OF CYBERSECURITY LAPSES AT PROFESSIONAL SERVICES FIRMS

WindTalker®

INTRODUCTION

Johnson & Bell, a venerable Chicago law firm of 100 plus attorneys had been sued for inadequate cyber security, i.e., for failing to protect the security and confidentiality of its thousands of clients and former clients. Curiously the plaintiffs, two former clients who had paid the firm a mere $30,000 in fees (peanuts for firms of the size and stature of Johnson & Bell), claimed no actual damages — and claimed no negligence in the underlying legal representation they had received.

"THE MOST EXPENSIVE THING IN THE WORLD IS TRUST. IT CAN TAKE YEARS TO EARN AND A MATTER OF SECONDS TO LOSE."

— ANONYMOUS - 2017

But they didn't need to, at least according to the averments made in the originally sealed but later unsealed complaint. The book of remedies permitted much more, and that's what plaintiffs went after: injunctive relief, notification of all the firm's thousands of clients, of the law firm's below-standard data and info-security systems, and disgorgement of all legal fees earned during the two-year period of inadequate cyber-security (measured by the profits pocketed by the firm for insufficient budgeting and spending on cybersecurity). To be clear, the trial court did not rule on the merits of the complaint, and no appellate court did, either. At the behest of plaintiffs' counsel, the case was dismissed without prejudice and the parties agreed to proceed by way of arbitration[1]. But the bell tolls, as the implications are catastrophic: the well-established common law theories alleged in the complaint should have every practicing lawyer, managing partner and law firm in America looking over their shoulder. The dust on the horizon could be the public lawsuit naming you or your firm for cybersecurity legal malpractice.

SUMMARY OF THE CASE & ALLEGATIONS

In the case of *Shore vs. Johnson & Bell*[2], the plaintiffs accused the venerable Chicago law firm of "systemically exposing confidential client information" with the potential of security breach and access over a previous two-year period, from 2014 to 2015. During that time, the two former plaintiff clients, Jason Shor and Coinabul, LLC, a bitcoin website, had retained Johnson & Bell to advise them on their related business matters, emailing the firm confidential documents containing information such as trade secrets and sensitive customer information, while paying over $30,000 in legal fees.

According to the complaint, the firm stored in its computerized systems confidential client data which remained on its servers and billing systems after the representation concluded. Thereafter, it continued, the client plaintiffs discovered the law firm maintained an outdated security system that was vulnerable to attack, including access to its confidential information by third party attackers.

In terms of legal theories, the complaint alleged standard and well-accepted legal malpractice or professional negligence claims: negligence, unjust enrichment, breach of fiduciary duty, and professional negligence.[3] But more specifically, to substantiate these claims factually, they averred that the law firm was running its billing software on an outdated and insecure version of the Java-run application server called JBoss (later renamed WildFly).

[1] Shore v. Johnson & Bell, Case No. 16-ev-4363, U.S. Dt. Ct., Ill, Eastern Dt., Memorandum Opinion and Order, http://law.justia.com/cases/federal/district-courts/illinois/ilndce/1:2016cv04363/325450/56/. [2] Ibid.
[3] Pennington, Dan, The Most Common Types of Legal Malpractice Claims by Type of Error, ABA Journal Online, July-August 2010 Issue, Vol 36, No 4, http://www.americanbar.org/publications/law_practice_home/law_practice_archive/lpm_magazine_webonly_webonly07101.html.

© Copyright 2017 WindTalker® All rights reserved.

Based on this and other claimed cybersecurity failures, the ex-clients accused the firm of the following:

Accusation #1 Using an insecure virtual private network (VPN) accessible from public WiFi, leaving confidential client data vulnerable to so-called "man-in-the-middle" attacks.

Accusation #2 Using a self-hosted email server with obsolete encryption, exposing the firm:

(a) to DROWN attacks, which allow hackers to steal sensitive documents, communications, credit card data, trade secrets and passwords, and

(b) to FREAK attacks, which can help hackers bypass SSL encryption protection on email and other servers.

These claims of course could be further amended (even in arbitration) to include additional allegations if, at any time in the discovery process, further cybersecurity inadequacies should come to light. *In terrorem* at its finest.

THE RELIEF REQUESTED

Though no allegation of data breach was made, the plaintiff former clients sought a preliminary injunction barring the law firm from exposing client data via its VPN, email servers and billing software. In other words, they asked for a court order requiring the firm to overhaul and bring current its inadequate cyber-security system, presumably to be monitored by a court-appointed neutral party.

In a very aggressive move, they also asked the trial court to issue an order:

1. Declaring the firm's conduct to be professionally negligent;
2. Requiring the firm to notify all clients about its data vulnerabilities and state that any information they submitted to the firm wasn't secure;
3. Forcing the firm to undergo a security audit to determine the extent of any data breaches that may have already occurred; and
4. Requiring the firm to forfeit both attorney's fees earned during any data breaches and the profits diverted from spending on reasonable cybersecurity.

LEGAL & PRACTICAL IMPLICATIONS OF SHORE v. JOHNSON & BELL

Shore v. Johnson & Bell does not establish any binding legal precedent, and the firm could win in arbitration, though it is likely that the arbitration will result in some form of mandated action on the part of Johnson & Bell. But the case, no matter what happens, has extraordinary legal and practical implications that should make all attorneys sit up and pay attention. Here's why:

1. The plaintiff and former clients may prevail, obtaining an arbitration award that the law firm committed the legal wrongs alleged, either in part or in combination. This sounds a very loud alarm bell for lawyers and law firms that have not addressed their cybersecurity readiness, as a finding in favour of the plaintiffs will generate copycat legal malpractice lawsuits.

© Copyright 2017 WindTalker® All rights reserved.

2. Even if Johnson & Bell prevails on the facts on all counts, and the arbitrator(s) rule in its favor, the legal theories asserted have solid support in precedent, i.e., the equitable and restitutional relief requested are well-founded in common law[4]. In other words, the claims are certain to be asserted in later litigation in more favorable jurisdictions or under better facts. In all likelihood, one day a federal or leading state appellate court from a leading jurisdiction in California or New York will rule on claims and issues presented by a case like *Shore v. Johnson & Bell*. When that time comes, for many law firms it will be too late, as the claims in *Shore* applied back in time to security already potentially compromised.

3. The *Shore* plaintiffs did not claim any actual damages and actual breach, but merely the potential for irreparable harm and the potential for cybersecurity breach in the future due to the firm's negligence in not addressing its woefully inadequate cybersecurity capabilities. What will happen when an actual law firm security breach occurs and confidential files are in fact accessed, compromised, and/or exploited?

4. Single actions beget class actions. It is only a matter of time before the plaintiffs' class action bar starts taking on the legal profession for inadequate cybersecurity preparedness, asserting the theories of *Shore v. Johnson & Bell* and calling upon the public policy considerations of cases like *FTC v. Wyndham* (covered in an earlier White Paper). And of course, class actions in turn spawn more individual actions, creating a vicious cycle in which the lawyer and law firm are caught in the middle.

5. Significant questions arise as to professional negligence or legal malpractice insurance. Reviewing your malpractice policy with your broker for clarity on the scope and extent of your cybersecurity coverage would be wise. Questions to ask include: a/ are we covered for *Shore v. Johnson & Bell* claims where no actual damages are alleged? b/ does the definition of "professional negligence" under your policy include cyber-security failures? c/ does your policy exclude liability coverage for criminal hacks of others that damage you or your clients? As well as many more. See our White Paper on *Legal Malpractice Insurance in a Cyber-Security Age*.

6. Let's face it, the down and dirty is that all law firms have disgruntled former and current clients. If any of them catches wind of the potential for a *Shore v. Johnson & Bell* claim, they now have leverage to walk away from every dime of legal fees they owe and extort a lump sum payment to boot — if only to avoid the opprobrium of a highly-negative lawsuit about the law firm hitting the local papers, going under a microscope like *Shore v. Johnson & Bell*, or resulting in mass client notification letter.

7. Already law firms are coming under scrutiny for having a reputation of poor cybersecurity systems and practices; so cases like *Shore v. Johnson & Bell* only antagonize the already-anxious ethics overseers. ABA and state ethical rules demand aggressive protection of confidential client data, communications and information[5]. "At all costs" has recently been the call-to-action in California[6]. And with a lawsuit like *Shore v. Johnson & Bell*, together with the cases it spawns, it is likely that enforcement of the cybersecurity ethics rules will receive even greater attention in the future[7].

[4] Dobbs' Law of Remedies: Damages - Equity - Restitution (Hornbook Series) 2nd Edition.
[5] For example, see the official ABA website: http://www.americanbar.org/content/dam/aba/events/labor_law/2015/march/tech/wu_cybersecurity.authcheckdam.pdf
[6] Official California State Bar website: http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3D&tabid=836
[7] Offit-Kurman Legal blog: For Lawyers, Cybersecurity Competence is also an Ethical Obligation, http://www.offitkurman.com/for-lawyers-cybersecurity-competence-is-also-an-ethical-obligation/

© Copyright 2017 WindTalker® All rights reserved.

WHAT LAW FIRMS SHOULD DO BUT DON'T:

The unmistakable trend is toward cyber-security responsibility and accountability for everyone, companies and law firms alike. It is ironic, however, that law firms seem to be the last wave to embrace these responsibilities vigorously. Indeed, since lawyers have heightened, fiduciary responsibilities to their clients, over and above the duties owed of ordinary businesses to their customers, you would think they would be leaders, across the board. And perhaps they should be, but they most emphatically are not. Maybe you are an exception; but then, maybe you are not. Like so many others, maybe you have been focusing on your cases, not your security. But here's what you can do, taking lessons from such cases as *FTC v. Wyndham*, which set forth the primary cybersecurity responsibilities for non-fiduciary corporations (all of which would, logically, then apply to law firms):

- **Change your mind-set toward cybersecurity:** You must overcome the idea that lawyers just practice law and whatever you have in place has always worked well enough.
- **Continuously monitor your capabilities:** You must recognize that the threat of cyber-insecurity is constantly advancing, and the measures you must take must meet your fiduciary duty to your client to protect his or her documents, communications, confidentiality, privacy, and proprietary information.
- **Encrypt ALL sensitive information:** Not just the structured (database records) stuff, but the stuff in motion, the unstructured (documents, emails, and texts) stuff.
- **Invest in vigilance — it costs far less than a negative finding:** While it may appear to be an arms race in enhancements and updates to cybersecurity systems, policies and systems must be vigilantly supported and maintained. The threat persists 24 hours a day, seven days a week, 365 days a year — and what may be reasonable to you, may not be reasonable to your clients, federal and state regulators, business partners, and ethical oversight groups.

The ultimate challenge, therefore, is staying ahead of the game wherever and whenever possible, by routinely auditing and reviewing your information security program, identifying vulnerabilities, establishing a cyber security program budget with contingency funds, and routinely exploring new cyber-security methods and technology.

WHAT DOES THIS MEAN TO YOU:

No matter what types of sensitive information is involved, law firms have ongoing affirmative legal, fiduciary and ethical obligations to develop and implement the latest cyber-security technologies; the latest methods and protocols for protection, education and training; and the most effective means for responding to, correcting, and remedying any prior security breaches. Put another way, it is time for every law firm to review and consider cybersecurity reform, making cybersecurity a way of life for all employees and third-party contractors, and ensuring reasonable data and information security. Anything less exposing the firm to potential catastrophic liability for legal malpractice under the theories pursed in *Shore vs. Johnson & Bell*.

© Copyright 2017 WindTalker® All rights reserved.

ABOUT WINDTALKER:

As cyber-attacks are increasingly sophisticated and a persistent threat to every individual, business, and organization, the typical industry response is to lock information assets down with more restrictive governance policies and security controls. However, when information assets are restricted, the effectiveness and efficiency of a business is significantly impacted. With information being the life blood of an organization, it needs to flow to customers, employees, and business partners. This challenging misalignment of security controls to business process leaves us with either too much or too little security, or the classic business vs. risk decision. The industry lacks a solution that addresses the real problem: protection of the content, "the data" no matter where it travels… Until Now!

WindTalker is a content security platform that allows for the protected movement and sharing of information which integrates with existing popular software. We simply apply encryption to specific portions of sensitive content within unstructured data formats such as documents, emails, text, and images. WindTalker protects these elements of sensitive data, such as personally identifiable information, company secrets, or client-attorney privileged information, while still allowing the movement and sharing of information without major interruption to the way you do business. Using a simple "Click — Protect — Share" philosophy, WindTalker leverages the user's knowledge and skills to enhance the security of the organization. WindTalker provides true control over "Need to Know".

© Copyright 2017 WindTalker® All rights reserved.