36

1:16-cv-04363
Judge Milton I. Shadur
Magistrate Judge Susan E. Cox

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION**

JASON SHORE and COINABUL, LLC, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

JOHNSON & BELL, LTD, an Illinois corporation,

Defendant.

Case No.:

**DOCUMENT FILED PROVISIONALLY UNDER SEAL**

DV

FILED

APR 15 2016

THOMAS G. BRUTON
CLERK, U.S. DISTRICT COURT

**VERIFIED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiffs Jason Shore and Coinabul, LLC bring this Verified Class Action Complaint and Demand for Jury Trial ("Complaint") against Defendant Johnson & Bell, LTD ("Johnson & Bell") to put an end to Defendant's practice of systematically exposing confidential client information and storing client data without adequate security. Plaintiffs allege as follows upon personal knowledge as to themselves and their own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by their attorneys.

## NATURE OF THE ACTION

1. Johnson & Bell is a Chicago-based law firm with more than 100 attorneys and practice groups ranging from administrative law to professional liability.[1] To manage those attorneys and groups, Johnson & Bell operates several computer systems that allow clients and employees to connect remotely to internal servers, access and transmit emails, and manage and record detailed time records of work carried out for clients. These computers systems, in turn,

[1] *Practices - Johnson and Bell*, http://johnsonandbell.com/practices-home/ (last visited Apr. 15, 2016).

connect with other Johnson & Bell computer systems—including systems which contain highly sensitive client data.

2. Unfortunately, Defendant fails to keep its clients' information secure. Defendant's computer systems suffer from critical vulnerabilities in its internet-accessible web services. As a result, confidential information entrusted to Johnson & Bell by its clients has been exposed and is at great risk of further unauthorized disclosure (if it hasn't already been disclosed).

3. Johnson & Bell has injured its clients by charging and collecting market-rate attorneys' fees without providing industry standard protections for client confidentiality. The longer Johnson & Bell is allowed to maintain its vulnerable systems, the more likely its clients will become victims of a data breach. Alternatively, if a breach has already occurred, each day that passes without knowledge and notice of a breach puts client information in greater danger of widespread distribution. As it stands, Johnson & Bell has failed in its obligations to keep its clients' confidential information secure.

4. Accordingly, this putative class action lawsuit seeks: (i) to compel Johnson & Bell to stop exposing its clients' confidential information to unauthorized parties (which it can do by implementing industry standard protocols); (ii) to compel Johnson & Bell to allow an independent, third-party firm to conduct a security audit; (iii) to inform Johnson & Bell's clients that their confidential information has been exposed; (iv) damages; and (v) attorneys' fees and costs.

## PARTIES

5. Plaintiff Jason Shore is a natural person and citizen of the State of California.

6. Plaintiff Coinabul, LLC is a Wyoming limited liability company.

7. Defendant Johnson & Bell, LTD is an Illinois corporation with its headquarters

located at 33 West Monroe Street, Suite 2700, Chicago, Illinois 60603. Johnson & Bell conducts business throughout this District, the State of Illinois, and the United States.

## JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this case under 28 U.S.C. § 1332(d)(2) because (a) at least one member of the putative class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and (c) none of the exceptions under that subsection apply to this action.

9. This Court has personal jurisdiction over this case because Defendant is headquartered and conducts its principal operations in this state.

10. Venue is proper in this District under 28 U.S.C. § 1391(b) as (i) Defendant's principal place of business is in this District, and (ii) most of the operative facts giving rise to Plaintiffs' complaint occurred in this District.

## FACTUAL ALLEGATIONS

### I. Johnson & Bell Promises to Keep Information Secure and Markets Itself as a Cybersecurity Expert.

11. Johnson & Bell is a Chicago-based law firm with more than 100 attorneys practicing in a wide range of areas.[2] Some of Johnson & Bell's largest clients include those in the insurance and health care industries, and companies seeking to merge with and/or acquire other entities. Johnson & Bell also handles confidential corporate compliance and investigatory work.

12. Like any large firm, Johnson & Bell receives a vast amount of confidential client information, including financial records, trade secrets, sensitive communications, and personal information (*e.g.*, addresses, contact information, and social security numbers) ("Confidential

[2] *Practices - Johnson and Bell*, http://johnsonandbell.com/practices-home/ (last visited Apr. 15, 2016).

Client Information"). Johnson & Bell also generates additional Confidential Client Information from that client data as a part of litigation, due diligence, investigation, time and billing records, and its day-to-day business.

13. Moreover, Johnson & Bell relies on a suite of computer systems to provide its legal services. Those include, amongst others, a time entry system, a virtual network system, and an email system, all of which are designed to interface with the internet (*i.e.*, to be publicly accessible). The computer systems exposed to the internet are also connected to many of Johnson & Bell's internal systems. A vulnerability in one of these systems can expose Johnson & Bell's entire computer system and all the Confidential Client Information it contains.

14. Johnson & Bell knows that modern clients demand assurances that their confidential data is secure while kept on its computer systems. That is why Johnson & Bell markets itself to existing and potential clients as an expert in data security. In 2014, Joseph R. Marconi, a shareholder at Johnson & Bell, with assistance from an associate, wrote an article showcasing Johnson & Bell's purported expertise, noting that "[d]ata management safeguards can prevent possible legal malpractice from cyber-security breaches.[3] Marconi wrote:

> Given the confidential and valuable information passed between clients and their lawyers due to the attorney-client privilege, lawyers' and law firms' computer and e-mail accounts have become favorite targets [of hackers]. … In addition, mobile devices and both cloud-based and in-firm corporate networks and email systems are susceptible to electronic hacking where a hacker will illegally gain access to electronic information using a variety of more sophisticated methods. Law firms and lawyers present a particularly appealing target for hackers because the mandatory confidentiality of the attorney-client relationship creates a virtual treasure trove of sensitive client information—such as social security numbers, medical information, trade secrets, wire transfer instructions, privileged litigation

---

[3] Joseph R. Marconi and Brian C. Langs, *Don't Let Cybersecurity Breaches Lead to Legal Malpractice: The Fax Is Back*, ISBA Mutual Practice Updates, https://www.isbamutual.com/liability-minute/donrsquot-let-cybersecurity-breaches-lead-to-legal (last visited Apr. 15, 2016). A true and accurate copy of the article is attached as Exhibit 1).

communications and strategy, and internal corporate strategies—much of which can be very valuable to an array of criminal enterprises.

15. Marconi acknowledged that lawyers are under a duty to protect client data, stating:

> Illinois Rule of Professional Conduct 1.6(a) requires a lawyer practicing in Illinois to make reasonable efforts to ensure the confidentiality of client information, including electronically stored client information. … While technology utilization is necessary, the prudent lawyer will also realize that the use of technology to electronically store and transfer sensitive client information necessitates proactive implementation of safeguards that will help in the prevention and defense of this information's electronic theft.

16. Marconi then recommended specific precautions to protect client data:

> Every law firm should maintain computer-use policies requiring employees to use and routinely update passwords for e-mail, document management systems, mobile devices, and laptops. Intranets, extranets [e.g., web portals], and Citrix-like virtual desktops also invariably require password protection. … Other safeguards may include limiting who may access particular materials electronically and when they may share, print, or alter data. Finally, every firm's computer-use policy should communicate to its employees, (1) the seriousness of the firm's confidentiality obligation to its clients, (2) the very real possibility of a cyber-attack, and (3) the procedure for reporting a potential data breach or suspected disclosure.

17. As Johnson & Bell's marketing demonstrates, it promises to its clients that it takes confidentiality and cybersecurity seriously. Unfortunately, Johnson & Bell utterly fails to deliver on that promise. By visiting Johnson & Bell's public websites, it is revealed that Defendant has failed to keep its Confidential Client Information secure.

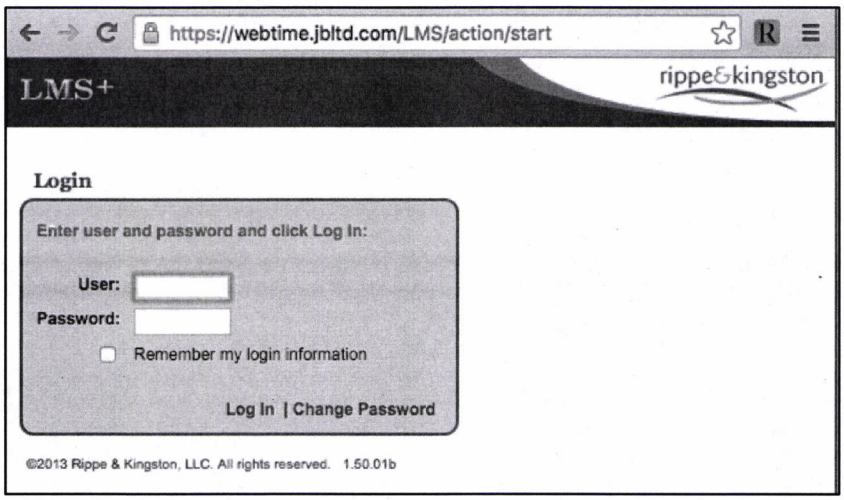
## II. Johnson & Bell Has Failed To Secure Confidential Client Information, Exposing the Data to Hackers and Thieves.

As introduced above, Johnson & Bell maintains several internet-accessible computer networks. A review of public information, though, shows that Johnson & Bell has failed to maintain up-to-date security. As a result, Johnson & Bell has exposed Confidential Client Information. It is only a matter of time until hackers learn of these vulnerabilities (if they have

not already). As a result, Johnson & Bell's clients not only face the current harm of having their Information exposed but the risk that hackers will gain access to confidential billing records, be able to intercept and decrypt attorney-client communications, and obtain additional documents stored by Johnson & Bell.

### *A. Defendant's Webtime Server Leaves Sensitive Billing Records Exposed.*

18. To let its staff and attorneys track the time they spend working on each matter, Defendant maintains a time-tracking system that is accessible from the internet. On its website (jbltd.com), Johnson & Bell operates a "Webtime" service developed by Rippe & Kingston, an information technology company. *See* Figure 1. There, attorneys and others are prompted to submit their usernames and passwords. Once submitted, the users are taken to a system where they are able to enter and track the time spent on client matters. The time tracking system maintains each record submitted by each attorney.




**(Figure 1.)**

19. Defendant's system, though, does not limit access to individuals with valid usernames and passwords. Instead, hackers can breach its system with impunity because Defendant has improperly configured the service and left it running out-of-date software. A review of the publically available specifications of Defendant's Webtime service shows that it is

more than a decade old and has not been updated with critical security patches.

20. Defendant's Webtime time tracking system is built on a "JBoss Application Server" which implements Java (a virtual computing language) for applications. By using Java, service providers are able to let users run applications on myriad devices without having to rewrite the application for each type device (*e.g.*, a Java application can run on a Mac and a PC without modification).

21. Johnson & Bell's JBoss system is woefully out-of-date and suffers from a critical vulnerability. Defendant's JBoss system is listed as running version 4.0.2. A review of industry literature reveals that that version of JBoss was introduced in 2005 and is "End of Life," or, no longer supported or recommended for use. For comparison, the latest version of JBoss (now called WildFly) is version 10.

22. JBoss 4.0.2 has been termed End of Life for an important reason: it is insecure. In September 2013, the National Institute of Standards and Technology, sponsored by the Department of Homeland Security, updated its National Vulnerability Database to include a vulnerability specific to this version of JBoss. NIST reported that the vulnerability was "network exploitable," had a "low" level of access complexity, and that it "[a]llows unauthorized disclosure of information; [a]llows unauthorized modification; [and a]llows disruption of service."[4] That is, JBoss version 4.0.2 allows hackers to access previously protected information with little to no effort.

23. The risk of this vulnerability is not just theoretical. Computer security experts have recently observed an ongoing and "widespread campaign" attacking JBoss computer

---

4 *NVD – Detail*, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4810 (last visited Apr. 15, 2016).

systems of the exact type used by Defendant.[5] In these attacks, "[a]dversaries are exploiting known vulnerabilities in unpatched JBoss servers [just like Defendant's out-of-date servers] before installing [malicious software], identifying further network connected systems, and installing SamSam ransomware to encrypt files on these devices." That is, hackers are targeting entities that have not updated their JBoss servers and then holding sensitive data hostage until a ransom is paid.

24. On April 4, 2016, a user commented about this attack with the following:

> We were hit by this ransomware and I wasn't sure if it was jboss related or a compromised user account. Good to at least know it was jboss related. We had port 443 open to the world on an aging server :([6]

25. That user, just like Johnson & Bell, ran an outdated server that was exposed to the internet ("port 443 open to the world") and was attacked. It is just a matter of time until a hacker discovers Johnson & Bell's vulnerable server and further exposes Confidential Client Information.

***B. Defendant's VPN Server Fails to Protect Client Data.***

26. To allow its attorneys and staff access to documents and files while they are offsite, Johnson & Bell operates a virtual private network. But just like its Webtime system, Johnson & Bell's remote computer system is vulnerable to attacks.

27. Employees physically present in a corporation's office are able to access internal computer networks, or *intranets*. Intranets often include private webpages for employees, shared storage systems, printer controls, and more. Normally, intranets are isolated from external network traffic (the internet). As such, employees located offsite are unable to access the internal

---

[5] Cisco Talos Blog: SamSam: The Doctor Will See You, After He Pays The Ransom, http://blog.talosintel.com/2016/03/samsam-ransomware.html?m=1 (last visited Apr. 15, 2016).

[6] *Id.*

resources unless provided a means to virtually connect to the intranet. Defendant remedied this by implementing a "virtual private network" or "VPN." By using the VPN, offsite employees use encrypted communication protocols to connect to Johnson & Bell's internal networks. While use of a VPN is industry standard, Defendant's implementation is not.

28. Specifically, Defendant's VPN supports insecure renegotiation, leaving it vulnerable to man-in-the-middle attacks.

29. This is a serious security deficiency, especially considering the purpose of a VPN: to securely connect to a company's servers housing its most sensitive information. Most troubling is that Johnson & Bell's VPN system supports insecure renegotiation, opening the door to a "Man In The Middle Attack." A Man In The Middle Attack is a well-known type of attack used by, amongst others, computer hackers,[7] spy agencies,[8] and foreign governments[9] to eavesdrop on private communications and steal Confidential Client Information.

30. And, because Johnson & Bell's VPN users are mobile and working from remote locations, a Man In The Middle Attack is a serious concern. Defendant's attorneys accessing Johnson & Bell's internal document repositories through the VPN likely do so from hotels, conference centers, opposing counsel's offices, cafes, and/or public networks. Each location presents a new place attackers could gain access to Johnson & Bell's systems and Confidential Client Information. Simply by using its VPN solution, then, Defendant and its attorneys can expose Johnson & Bell's Confidential Client Information.

---

[7] *DoubleDirect: Hackers Redirect High-Traffic Sites Via New MITM Attack*, http://www.tripwire.com/state-of-security/latest-security-news/doubledirect-hackers-redirect-high-traffic-sites-using-new-man-in-the-middle-attack/ (last visited Apr. 15, 2016).

[8] *NSA disguised itself as Google to spy, say reports – CNET*, http://www.cnet.com/news/nsa-disguised-itself-as-google-to-spy-say-reports/ (last visited Apr. 15, 2016).

[9] *Chinese government launches man-in-middle attack against iCloud [Updated] | Ars Technica*, http://arstechnica.com/security/2014/10/chinese-government-launches-man-in-middle-attack-against-icloud/ (last visited Apr. 15, 2016).

### *C. Johnson & Bell's Email System Vulnerability*

31. Rather than use a third-party email provider, such as Google's Gmail, Johnson & Bell hosts its own email server. Johnson & Bell's attorneys and staff use this email server to send, receive, and store communications between them and opposing counsel, courts, and, importantly, its clients. Johnson & Bell also uses this email system to transmit sensitive and confidential documents as email attachments. While Johnson & Bell attempts to protect the content of the communications from prying eyes by using encryption, its attempts fail. Johnson & Bell's email system has broken security that leaves clients' confidential communications and documents exposed to unauthorized disclosure.

32. Specifically, Johnson & Bell's email server:

- Supports SSL 2, which is obsolete, insecure, and is exploited by the "DROWN" attack, and
- Supports 512 bit export suites and is vulnerable to the "FREAK" attack.

33. These vulnerabilities demonstrate that Johnson & Bell has deficient security and fails to protect Confidential Client Information. However, the fact Johnson & Bell's email server is exploitable by the DROWN attack is concerning. The DROWN attack (short for **D**ecrypting **R**SA with **O**bsolete and **W**eakened E**N**cryption) "allows attackers to break the encryption and read or steal sensitive communications, including passwords, credit card numbers, trade secrets, or financial data."[10] By using a DROWN attack, hackers can gain access to a server's secrets "in under 8 hours at a cost of $440."[11] And once the server is breached, hackers can access the contents of Johnson & Bell's previously encrypted emails and attachments.

34. For instance, a law firm based in Panama notoriously suffered what is likely the

---

10 *DROWN Attack*, https://drownattack.com (last visited Apr. 15, 2016).

11 *Id.*

largest data breach of all time, likely stemming from the DROWN attack.[12] Over 2 *terabytes* of client information was stolen and leaked to investigative journalists. While the result of that breach has been the unearthing of widespread corruption, there are undoubtedly thousands of innocent clients whose private information has been disclosed.[13] While the exact means of the breach are not known, what is known is that the firm had poor network security. Notably, the firm "failed to update its Outlook Web Access login since 2009 and not updated its client login portal since 2013," leaving it "vulnerable to the DROWN attack, a security exploit that targets servers supporting the obsolete, insecure SSL v2 protocol."[14]

## III. Johnson & Bell's Exposure of Client Data Makes a Data Breach Inevitable.

35. Johnson & Bell markets itself as a sophisticated firm capable of representing individuals and companies with complicated legal issues. Hospitals, insurance companies, and more, trust Johnson & Bell with their sensitive information and trade secrets. And because hackers and corporate spies covet such data, Johnson & Bell is a target for an attack.[15] As such,

---

[12] *Panama Papers law firm says it is a hacking 'victim'*, http://www.usatoday.com/story/news/2016/04/06/panama-papers-law-firm-says-hacking-victim/82695208/ (last visited Apr. 15, 2016).

[13] *Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption · ICIJ*, https://panamapapers.icij.org/20160403-panama-papers-global-overview.html (last visited Apr. 15, 2016) ("As with many of Mossack Fonseca's clients, there is no evidence that Chan used his companies for improper purposes. Having an offshore company isn't illegal. For some international business transactions, it's a logical choice.")

[14] *Panama Papers: The security flaws at the heart of Mossack Fonseca (Wired UK)*, http://www.wired.co.uk/news/archive/2016-04/06/panama-papers-mossack-fonseca-website-security-problems (last visited Apr. 15, 2016).

[15] In fact, insurance companies and those in the healthcare industry (regulated companies that are under separate duties to protect highly sensitive information), arguably have their own duty to properly vet the security of any law firm they work with to ensure it will properly secure client data.

Such companies, which are some of Johnson & Bell's largest clients, are also at great risk of having their data stolen by hackers. Indeed, hackers prize patients' medical data because of its value on the black market. Entire online "underground exchanges" have been created "where hackers sell [stolen] information," such as "names, birth dates, policy numbers, diagnosis codes

Johnson & Bell's clients expect—based on the long-standing attorney obligation to maintain client confidentiality and Johnson & Bell's own marketing—that Johnson & Bell will protect Confidential Client Information with equally sophisticated methods or at least industry standards. As it stands, Johnson & Bell falls far short of those standards.

36. Simply put, with the Confidential Client Information it maintains and the low security it has employed, Johnson & Bell is a data breach waiting to happen. Presently, Johnson & Bell's time record system can be accessed without any username or password (or any other credential), meaning Johnson & Bell exposes, amongst other things:

(i) The identity of all of its current clients;

(ii) The identity of clients that have ended their relationship with Johnson & Bell;

(iii) The identity of clients involved in non-public investigations (both internal and external), confidential transactions, and litigation under seal;

(iv) The details and scope of each client's representation;

(v) Trade secrets; and,

(vi) Discussions shared under the supposed protections of attorney-client privilege.

37. Johnson & Bell's exposure of client billing records could be devastating. A company anticipating toxic tort lawsuits might retain Johnson & Bell to investigate its potential liability—unauthorized disclosure of that fact alone might prove fatal. Or, the time records might reveal investigations into managers accessing websites especially prone to distributing malware

---

and billing information." *See Your medical record is worth more to hackers than your credit card | Reuters*, www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 (last visited Apr. 15, 2016). On these exchanges, "medical information is worth 10 times more than [] credit card number[s]." *Id.*

Johnson & Bell's clients in the medical and insurance industry have undoubtedly sent Johnson & Bell such sensitive information. Just by retaining those documents, then, Johnson & Bell is at an increased risk of being targeted by hackers seeking to obtain those valuable records.

and viruses (*e.g.*, pornographic websites) while at work and then disseminating inappropriate materials to subordinates. Undoubtedly, Johnson & Bell's time records contain incredibly sensitive information that, if exposed, will reveal criminal investigations, sexual harassment suits, pre-litigation investigations, and more. Given that, Johnson & Bell is providing insufficient security to protect the sensitive information at issue.

38. Moreover, once attackers have accessed the time records, they will use the data to social engineer (or "phish" for) further hacks. Recently, Proskauer Rose LLP revealed that it suffered from a data breach stemming from a phishing attack.[16] It was reported that Proskauer Rose "complied with an email from an 'unauthorized third party' claiming to be a senior executive making a purportedly 'legitimate request' for employees' 2015 W-2 tax forms."[17] That is, the hackers used information sourced from previous attacks to convince Proskauer Rose that they were a legitimate party that had need for sensitive information.

39. Worse, with the Confidential Client Information in Johnson & Bell's time records, a hacker will invariably phish each of Johnson & Bell's clients. By knowing the name of the attorney working a matter, the nature of the representation, and up-to-date details (*e.g.*, that a meeting occurred on a specific date at a specific time with specific people), the hacker can impersonate Johnson & Bell attorneys or staff (or their clients or vendors) to obtain from its clients or its own employees (1) additional details of trade secrets or confidential information, (2) financial data, or (3) methods to infiltrate additional computers and networks.

40. The risk of such targeted phishing attacks are real and are called "spear phishing attacks." Regarding spear phishing, the FBI states:

---

16 *Proskauer Rose Revealed Worker Tax Info In Phishing Scam - Law360*, http://www.law360.com/privacy/articles/781372 (last visited Apr. 15, 2016).

17 *Id.*

> [C]riminals need *some* inside information on their targets to convince them the e-mails are legitimate. They often obtain it by hacking into an organization's computer network (which is what happened in the above case) or sometimes by combing through other websites, blogs, and social networking sites. Then, they send e-mails that look like the real thing to targeted victims, offering all sorts of urgent and legitimate-sounding explanations as to why they need your personal data.
>
> Finally, the victims are asked to click on a link inside the e-mail that takes them to a phony but realistic-looking website, where they are asked to provide passwords, account numbers, user IDs, access codes, PINs, etc.
>
> **Criminal gain, your loss.** Once criminals have your personal data, they can access your bank account, use your credit cards, and create a whole new identity using your information.[18]

41. Overshadowing these concerns, though, is that once hackers have breached the Webtime system, there's no indication that they will be stopped. Indeed, if the described vulnerabilities are any indication, Johnson & Bell's computer systems likely have many more security deficiencies not identified herein. Johnson & Bell's clients, though, are left in the dark about Defendant's lax security practices.

## IV. Johnson & Bell Fails in its Obligation to Keep Confidential Client Information Secure, Lagging Behind Industry Peers.

42. Hackers know that law firms like Johnson & Bell routinely handle and exchange highly confidential trade secrets, business plans, financial data, and myriad personal information. That is why the risk of a breach is particularly acute for Johnson & Bell. Yet, individuals and businesses trust that when they hand over such information to Johnson & Bell, it is obligated to use industry standard protections to guard that information. But while other firms are taking the threat of breaches seriously, Johnson & Bell does not, falling short of its peers.

### *A. Law Firms are on Notice that Hackers are Targeting Them.*

---

[18] FBI — Spear Phishing, https://www.fbi.gov/news/stories/2009/april/spearphishing_040109, (last visited Apr. 15, 2016).

43. The ABA notes that law firms are required by "[t]he ethics rules," "common law," "contractual and regulatory obligations to protect information relating to clients and other personally identifiable information."[19] Illinois Supreme Court Rule 1.6(e) recognizes the long-standing duty attorneys have to maintain client confidentiality, stating, "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[20]

44. The comments to the rule go on to explain that the "reasonable efforts" attorneys must use to protect client data varies based on "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."[21] And, when attorneys "transmit[] a communication that includes information relating to the representation of a client, [*e.g.*, through email or VPN] the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[22]

45. The Illinois State Bar Association additionally warns attorneys about the risks of failing to maintain proper data security:

> There is good reason to fear that hackers might be coming after your law firm, Brooks says. "The legal industry, in particular, is the target of a lot of hacker attacks right now,' he says. "We're targets because we handle sensitive financial information and we're behind the curve in terms of security."

---

19 ABA, *Security*, http://www.americanbar.org/publications/techreport/2015/Security.html (last visited Apr. 15, 2016).

20 Article VIII. Illinois Rules of Professional Conduct of 2010, http://www.illinoiscourts.gov/supremecourt/rules/art_viii/artviii_new.htm (last visited Apr. 15, 2016).

21 *Id.*

22 *Id.*

...

> It's larger firms that face the most risk, Flaming says. That's "because ... they're much bigger targets, and [] the data they hold is much more valuable to someone trying to hack in," he says.[23]

46. Likewise, the ABA sends out periodic "Member Cyber Alerts" "in response to a request from the FBI that the ABA share Private Industry Notification cybersecurity alerts ('cyber alerts') with the legal community." In these alerts, the ABA notes "the increase in efforts to hack into the computer systems of legal professionals to reach the significant amounts of non-public information they hold. The FBI alerts are reminders to us all that we need to be alert to increasingly sophisticated cyber schemes."

***B. Johnson & Bell has Ignored Calls to Bolster Security.***

47. But while Johnson & Bell has shirked its responsibility to be "alert," other firms have started heeding the warnings from the FBI, the ABA, and state bar associations. For instance, in August 2015, "law firms including Sullivan & Cromwell; Debevoise & Plimpton; Paul, Weiss, Rifkind, Wharton & Garrison; Allen & Overy; and Linklaters" worked with cybersecurity experts to create the "Legal Services Information Sharing and Analysis Organization (LS-ISAO)." Through the LS-ISAO, these firms will "anonymously share threat data" so as to better protect the entire group.

48. Similarly, other firms are spending resources to bolster security and to obtain international certification for information security management. Shook, Hardy & Bacon spent more than two years trying to earn the ISO 27001 certification to "make sure [it] had the

---

[23] *Feeling Secure in the Cloud | Illinois State Bar Association*, http://www.isba.org/ibj/2015/01/feelingsecurecloud (last visited Apr. 15, 2016).

processes in place so [its clients] had confidence that [it] w[as] doing the best [it] could."[24]

49. Leading firms have also been "increasingly hiring dedicated security managers," conducting "third-party penetration tests, … as part of regular risk assessment activities," and requiring security training for employees.[25] Law firms have been taking these steps because they "are already under an obligation to adhere to professional ethics rules that govern client confidentiality and privilege issues. Another motivation for law firms should be the horror stories that sweep the media with increasing regularity about corporate data breaches."[26]

50. As the vulnerabilities discussed herein show, Johnson & Bell has not kept up with the rest of the legal industry in securing Confidential Client Information. While other firms are dedicating substantial resources to protect data, Johnson & Bell runs decade-old software presumably to save money. As a result, Johnson & Bell has exposed Confidential Client Information and made it accessible to hackers and thieves.

**FACTS SPECIFIC TO PLAINTIFFS**

51. On August 23, 2014, Plaintiffs retained Johnson & Bell for legal representation. On February 24, 2015, Johnson & Bell terminated its representation of Plaintiffs. In total, Plaintiffs paid Johnson & Bell $30,000 for legal services.

52. During the time Defendant represented Plaintiffs, Plaintiffs transmitted to Defendant Confidential Client Data. Specifically, and following Defendant's instructions, Plaintiffs transmitted via email to Defendant confidential information about their clients, orders,

---

[24] *Law firm makes a case for security certification | CIO*, http://www.cio.com/article/2969323/security/law-firm-makes-a-case-for-security-certification.html (last visited Apr. 15, 2016).

[25] *A Soft Target For Hacks, Law Firms Must Step Up Data Security - Law360*, http://www.law360.com/articles/706312/a-soft-target-for-hacks-law-firms-must-step-up-data-security (last visited Apr. 15, 2016).

[26] *Id.*

processes, trade secrets, and other Confidential Client Data. Presently, Defendant maintains Plaintiffs' Confidential Client Data on its computer servers.

53. In addition, Defendant maintains detailed records of the time attorneys and staff spent working on Plaintiffs' matter and stores those records electronically. In those time records, Defendant wrote detailed descriptions of confidential matters.

54. Plaintiffs understood and expected that Johnson & Bell would use industry standard measures to protect their Confidential Client Data. Plaintiffs value their privacy and the privacy of their clients and customers. Plaintiffs would not have retained Defendant or provided their Confidential Client Data had they known that Defendant had lax security protocols and insecure systems.

55. In fact, because Coinabul operated as federally regulated financial institution, Plaintiff Shore spoke with Defendant's agents and representatives about his expectation of privacy and security prior to retaining Defendant. Specifically, he discussed with Johnson & Bell that it needed to provide strong security to protect Plaintiffs' Confidential Client Data. Defendant assured Mr. Shore that it had sufficient security in place that would protect Plaintiffs' Confidential Client Data.

56. Defendant has exposed, and continues to expose, Plaintiffs' Confidential Client Data.

## CLASS ALLEGATIONS

57. **Class Definition**: Plaintiffs Shore and Coinabul bring this action pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), and (b)(3) on behalf of themselves and a class of similarly situated individuals, defined as follows:

> All Johnson & Bell LTD clients that have had their client records maintained by Johnson & Bell LTD within the statute of limitations period, excluding insurance

companies and clients operating in the health care industry.

Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

58. **Numerosity**: The exact size of the Class is unknown and not available to Plaintiffs at this time, but it is clear that individual joinder is impracticable. On information and belief, there are thousands of individuals or entities in the Class, making joinder of each individual member impracticable. Ultimately, members of the Class will be easily identified through Defendant's records.

59. **Commonality and Predominance**: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual members:

(a) Whether Defendant committed legal malpractice by breaching its contracts with Plaintiffs and the Class;

(b) Whether Defendant's conduct constitutes negligent legal malpractice;

(c) Whether Defendant has a duty to maintain the confidentiality of Plaintiffs' and the Class's Confidential Client Information;

(d) Whether Defendant breached its duty to maintain the confidentiality of Plaintiffs' and the Class's Confidential Client Information;

(e) Whether Defendant failed to implement industry standard data security

measures;

(f) Whether Defendant has been unjustly enriched;

(g) Whether Defendant breached its fiduciary duty to Plaintiffs and members of the Class; and

(h) Whether Plaintiffs and the members of the Class are entitled to equitable relief as well as actual damages as a result of Defendant's conduct.

60. **Typicality**: Plaintiffs' claims are typical of the claims of the other members of the Class. Plaintiffs and members of the Class sustained damages as a result of Defendant's uniform wrongful conduct during transactions with Plaintiffs and the Class.

61. **Adequate Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex class actions. Plaintiffs have no interest antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiffs.

62. **Policies Generally Applicable to the Class**: This class action is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward members of the Class, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's practices challenged herein apply to and affect members of the Class uniformly, and Plaintiffs' challenge of those practices hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

63. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of

this controversy given that joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered and uniformity of decisions ensured.

**FIRST CAUSE OF ACTION**
**Breach of Contract (Legal Malpractice)**
**(On behalf of Plaintiffs and the Class)**

64. Plaintiffs incorporate by reference the foregoing allegations as if fully set forth herein.

65. Plaintiffs and Class members entered into contracts with Defendant for attorney services.[27] Within each contract, Defendant states:

> Document Retention. During the course of the representation, J&B shall maintain a file on your behalf. The file may include material such as pleadings, transcripts, exhibits, reports, contracts, certificates, and other documents as are determined to be reasonably necessary to the representation ("Your File"). Your File shall be and remain your property. J&B may also include in the file its attorney work product, mental impressions, and notes (collectively "Work Product"). The Work Product shall be and remain the property of J&B.

66. Implicit in Defendant's Document Retention clause is that Johnson & Bell will

---

[27] A true and accurate copy of Plaintiffs' engagement letter contract with Johnson and Bell is attached as Exhibit 2.

keep all documents and files confidential using reasonable methods.

67. As detailed in this Verified Complaint, Defendant has breached the above contracts by exposing Plaintiffs' and the Class's Confidential Client Information. In addition, Johnson & Bell continuously breaches the above contracts by failing to safeguard Plaintiffs' and the Class's Confidential Client Information.

68. At all times relevant to this action, Defendant acted willfully and with intent to breach contracts entered into with Plaintiffs and the Class. Specifically, Defendant (and its website developers and network security employees) programmed and implemented its Webtime, email, and VPN systems with inadequate safeguards.

69. Plaintiffs and the Class have fully performed their contractual obligations.

70. As a direct and proximate result of Defendant's breach and continuing breach of contract, Plaintiffs and the Class have been injured. Specifically, Plaintiffs and the Class have been injured because Johnson & Bell exposed their Confidential Client Information; they have suffered a diminished value of the services they received from Johnson & Bell; and they are threatened with irreparable loss of the integrity of their Confidential Client Information and further injury and damages from the theft of that information.

71. Defendant's breach will continue unless enjoined by this Court. Plaintiffs and members of the Class are likely to succeed on the merits, are without adequate remedies at law for Defendant's continuing breach, are threatened with irreparable loss, injury, and damages unless the Court grants the equitable relief requested, and the equitable relief requested is also in the public interest.

72. Plaintiffs and members of the Class will suffer substantially more from the denial of an order enjoining Defendant from further breaches than the Defendant would suffer from its

issuance.

73. As such, Plaintiffs and the Class request that the Court enjoin Defendant from operating its Webtime, email, and VPN services until it implements industry standard security protocols to protect their Confidential Client Information and disconnecting its servers from external networks (*e.g.*, the internet). In addition, Plaintiffs and the Class seek an order compelling Defendant to inform clients that their Confidential Client Information is exposed on Defendant's computer systems and that they face a threat of unauthorized disclosure due to Johnson & Bell's substandard security measures.

74. In addition, Plaintiffs and members of the Class have been harmed by Defendant's prior breach. Specifically, a portion of the attorneys' fees that Plaintiffs and the Class paid to Johnson & Bell were to be used by Johnson & Bell, in part, to pay for the administrative costs of data management and security (*i.e.*, to keep their Confidential Client Information secure).

75. Defendant did not use those funds for the administrative costs of data management and security. Thus, Plaintiffs and the Class did not receive the contracted benefits.

76. As such, Plaintiffs and the Class also seek to recover the damages suffered as a result of Defendant's breach of contract.

**SECOND CAUSE OF ACTION**
**Negligence (Legal Malpractice)**
**(On behalf of Plaintiffs and the Class)**
**(In the alternative to the First Cause of Action)**

77. Plaintiffs incorporate by reference the foregoing allegations as if fully set forth herein, excluding paragraphs 64-76.

78. At all relevant times, an attorney-client relationship existed between Plaintiffs and members of the Class and Defendant.

79. Defendant breached its duty to Plaintiffs and members of the Class by failing to use a reasonable degree of professional care and skill required in its representation of Plaintiffs and members of the Class. Specifically, Defendant failed to implement industry standard data security measures, resulting in the Vulnerabilities and the exposure of their confidential data. And, Defendant failed to disclose that it does not use industry data security measures.

80. As a direct and proximate cause of Defendant's negligent conduct, Plaintiffs and members of the Class have incurred damages in the form of legal fees paid to Johnson & Bell. Specifically, Plaintiffs and members of the Class would not have paid legal fees to Johnson & Bell or they would have paid significantly less had Defendant disclosed that it does not use industry standard data security measures.

81. Moreover, Plaintiffs and members of the Class are continuously injured because Defendant's lax security measures have placed their confidential information at extreme risk of theft and unauthorized disclosure and are threatened with irreparable loss of trade secrets, financial loss, and other losses.

82. Defendant's breach will continue unless enjoined by this Court. Plaintiffs and members of the Class are likely to succeed on the merits, are without adequate remedies at law, are threatened with irreparable loss, injury, and damages unless the Court grants the equitable relief requested, and the equitable relief requested is also in the public interest.

83. Plaintiffs and members of the Class will suffer substantially more from the denial of an order enjoining Defendant from further unfair or deceptive conduct than the Defendant would suffer from its issuance.

84. As such, Plaintiffs and the Class request that the Court enjoin Defendant from operating all internet-accessible portals (including its time entry portal) until it implements

industry standard security protocols to protect their confidential information. In addition, Plaintiffs and the Class seek an order awarding damages and attorneys' fees and compelling Defendant to inform its clients that its computer systems are not secure and that they face a threat of unauthorized disclosure of confidential data due to Defendant's substandard security measures.

**THIRD CAUSE OF ACTION**
**Unjust Enrichment**
**(On behalf of Plaintiffs and the Class)**
**(In the alternative to the First And Second Causes of Action)**

85. Plaintiffs incorporate by reference the foregoing allegations as if fully set forth herein, excluding paragraphs 64-84.

86. Plaintiffs hereby plead the Second Cause of Action in the alternative to the First Cause of Action.

87. Plaintiffs and members of the Class conferred a measurable monetary benefit on Defendant. Defendant received and retained money belonging to Plaintiffs and the Class in the form of a portion of the attorneys fees paid to Johnson & Bell. Defendant appreciates or has knowledge of such benefit.

88. A portion of the attorneys fees that Plaintiffs and the Class paid to Johnson & Bell were to be used by Johnson & Bell, in part, to pay for the administrative costs of data management and security (*i.e.*, to keep their Confidential Client Information secure).

89. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and members of the Class. Defendant has failed to keep Plaintiffs' and Class members' Confidential Client Information from being exposed and to implement industry standard data management and security measures to secure that data, and under such circumstances, Defendant's retention of the benefit without payment

would be unjust.

90. Accordingly, Johnson & Bell has received money from Plaintiffs and the Class through the unlawful practices alleged herein, which in equity and good conscience should be returned.

**FOURTH CAUSE OF ACTION**
**Breach of Fiduciary Duty**
**(On behalf of Plaintiffs and the Class)**
**(In the alternative to the First, Second, and Third Causes of Action)**

91. Plaintiffs incorporate by reference the foregoing allegations as if fully set forth herein, excluding paragraphs 64-90.

92. Plaintiffs hereby plead the Third Cause of Action in the alternative to the First and Second Causes of Action.

93. At all relevant times, Defendant owed Plaintiffs and the Class a fiduciary duty to maintain confidentiality of all matters discussed and investigated.

94. Defendant breached its fiduciary duty to Plaintiffs and members of the Class by failing to use a reasonable measures to protect their Confidential Client Information. Specifically, Defendant failed to implement industry standard data security measures, resulting in the Vulnerabilities and the exposure of Confidential Client Information. And, Defendant failed to disclose that it does not use industry data security measures.

95. At all times relevant to this action, Defendant acted willfully and with intent to breach its fiduciary duty to Plaintiffs and the Class. Specifically, Defendant (and its website developers and network security employees) programmed and implemented its Webtime, email, and VPN systems with inadequate safeguards.

96. As a direct and proximate result of Defendant's breach, Plaintiffs and members of the Class have incurred damages in the form of legal fees paid to Johnson & Bell. Specifically,

Plaintiffs and members of the Class would not have paid legal fees to Johnson & Bell or they would have paid significantly less had Defendant disclosed that it does not use industry standard data security measures.

97. Moreover, Plaintiffs and members of the Class are continuously injured because Defendant's lax security measures have exposed their Confidential Client Information, leaving that information at extreme risk of theft and further unauthorized disclosure and are threatened with irreparable loss of trade secrets, financial data, and other losses.

98. Defendant's breach will continue unless enjoined by this Court. Plaintiffs and members of the Class are likely to succeed on the merits, are without adequate remedies at law, are threatened with irreparable loss, injury, and damages unless the Court grants the equitable relief requested, and the equitable relief requested is also in the public interest.

99. Plaintiffs and members of the Class will suffer substantially more from the denial of an order enjoining Defendant from further breaching its fiduciary duty than the Defendant would suffer from its issuance.

100. As such, Plaintiffs and the Class request that the Court enjoin Defendant from operating its Webtime, email, and VPN services until it implements industry standard security protocols to protect their Confidential Client Information and disconnecting its servers from external networks (*e.g.*, the internet). In addition, Plaintiffs and the Class seek an order compelling Defendant to inform clients that their Confidential Client Information is exposed on Defendant's computer systems and that they face a threat of further unauthorized disclosure due to Johnson & Bell's substandard security measures.

101. In addition, Plaintiffs and members of the Class have been harmed by Defendant's prior breaches of its fiduciary duty. Specifically, a portion of the attorneys fees that

Plaintiffs and the Class paid to Johnson & Bell were to be used by Johnson & Bell, in part, to pay for the administrative costs of data management and security (*i.e.*, to keep their Confidential Client Information secure).

102. Defendant did not use those funds for the administrative costs of data management and security. As such, Plaintiffs and the Class are entitled to a full or partial forfeiture of the fees paid to Defendant during the time of the breach.

103. In addition, Defendant unfairly profited from its breach of its fiduciary duty at the expense of Plaintiffs and the Class. Defendant did not use the paid-for funds to cover the costs of the data management and security owed to Plaintiffs and the Class, but rather used it to increase its profits.

104. As such, Plaintiffs and the Class also seek to recover the damages suffered as a result of Defendant's breach of fiduciary duty and any profits Defendant unfairly generated.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiffs Jason Shore and Coinabul, LLC, on behalf of themselves and the Class, respectfully request the following relief:

A. A preliminary injunction enjoining Defendant from:

i. Exposing its Confidential Client Information through its internet-accessible portals;

ii. Compromising the integrity of client communications, and, in turn, Confidential Client Information, transmitted through its virtual private networks; and

iii. Exposing its Confidential Client Information through its email systems;

B. An order certifying this case as a class action on behalf of the Class defined above, appointing Jason Shore and Coinabul, LLC as representatives of the Class, and appointing their counsel as class counsel; and,

C. An order:

i. Declaring that Defendant's conduct, as set out above, constitutes legal malpractice, breach of contract, negligence, unjust enrichment, and/or breach of fiduciary duty;

ii. Requiring Defendant to inform its clients that its computer systems are not secure and that they face a threat of further unauthorized disclosure of Confidential Client Information due to its substandard security measures;

iii. Compelling Defendant to allow an independent third-party firm to conduct a security audit of its systems to ensure the integrity of Confidential Client Information and determine the extent of any data breach that may have already occurred;

iv. Requiring Defendant to forfeit attorneys fees earned during its breach with Plaintiffs and the Class and any profits diverted from spending on cybersecurity;

v. Awarding reasonable attorneys' fees and expenses;

vi. Awarding pre- and post-judgment interest, to the extent allowable; and,

vii. Awarding such other and further relief as equity and justice may require.

**JURY DEMAND**

Plaintiffs request a trial by jury of all claims that can be so tried.

Respectfully Submitted,

**JASON SHORE and COINABUL, LLC**, individually and on behalf of all others similarly situated,

Dated: April 15, 2016

By: _____
One of Plaintiffs' Attorneys

Jay Edelson
jedelson@edelson.com
Benjamin Richman
brichman@edelson.com
Benjamin Thomassen
bthomassen@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378
Firm ID: 44146

Todd Logan*
EDELSON PC
329 Bryant Street
San Francisco, California 94107
Tel: 415.234.5260
Fax: 415.373.9495