

36

FILED

5/27/2016

PK

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

**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. 16 CV 4363
Honorable John W. Darrah

**DEFENDANT JOHNSON & BELL, LTD'S MEMORANDUM IN SUPPORT OF ITS
MOTION TO DISMISS PLAINTIFFS' VERIFIED CLASS ACTION COMPLAINT
PURSUANT TO FEDERAL RULES OF CIVIL PROCEDURE 12(b)(1) AND 12(b)(6)**

Defendant JOHNSON & BELL, LTD., by and through its attorneys, WILLIAMS MONTGOMERY & JOHN, LTD., and for its Memorandum of Law in Support of its Motion to Dismiss "Plaintiffs' Verified Class Action Complaint" Pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), states as follows:

INTRODUCTION

This is a putative class action brought against a law firm by former clients of the firm. Plaintiffs claim that "implicit" in the attorney fees they paid the firm was a promise by the firm to keep the clients' confidential information confidential. Plaintiffs' claims are fatally defective because absent from the complaint is any claim that the firm did not keep the clients' confidential information confidential. Instead, plaintiffs claim that the information was "exposed" or

“vulnerable” to possibly being compromised at some unknown point in the future, but not that it ever was compromised.¹

Indeed, if plaintiffs’ claims are actionable, then every lawyer who carries a briefcase, takes notes in court or in a deposition, or speaks with his or her client in public could be subject to being named in a class action lawsuit because in each instance a client’s confidential information was “exposed” or “vulnerable,” never mind the fact that the client’s confidences remained confidential.

Because a mere potentiality of harm is insufficient to maintain a suit plaintiffs’ claims must be dismissed for the following separate, but equally compelling reasons:

First, plaintiffs lack standing to bring this action under Article III because they have not suffered a concrete and particularized injury. There is no allegation of a breach or that client confidences were ever disclosed. Any claimed deficiencies no longer exist. Plaintiffs claim they paid Johnson & Bell to keep their confidential information confidential, and it remained confidential. Thus, plaintiffs received their claimed “benefit of the bargain” and their claims fail.

Second, plaintiffs’ third cause of action for unjust enrichment should be dismissed because the parties’ relationship is governed by a written contract.

Third, plaintiffs’ fourth cause of action for breach of fiduciary duty should be dismissed as duplicative of the first and second causes of action for legal malpractice.

¹ See “exposed” and “vulnerable.” Merriam-Webster Online Dictionary. 2016. <http://www.merriam-webster.com>. (May 26, 2016) (defining “expose” as “to leave (something) without covering or protection” and “vulnerable as “capable of being physically or emotionally wounded.”).

BACKGROUND

This is a putative class action brought by former clients of the defendant law firm, Johnson & Bell, Ltd. (“Johnson & Bell”) (Complaint attached as Exhibit A). Johnson & Bell previously represented and defended plaintiffs Jason Shore and Coinabul in a class action initiated by the same attorneys that initiated this action, the Edelson firm and Jay Edelson (“Edelson”). That prior matter is captioned *Hussein v. Coinabul, LLC, et al.*, No. 1:14-cv-05735 (N.D. Ill.) (“*Hussein*”) and, after Johnson & Bell’s motion to withdraw was granted, resulted in a default judgment being entered in favor of Edelson’s client and against Jason Shore and Coinabul on July 6, 2015 (*Hussein* Docket attached as Exhibit B). Now, only months after being adverse to Jason Shore and Coinabul in the *Hussein* matter, Edelson is here representing Jason Shore and Coinabul in this related matter claiming plaintiffs Confidential Client Information was “vulnerable” and could have been “exposed.”

Plaintiffs claim they disclosed to Johnson & Bell during its representation certain Confidential Client Information. (Ex. A, ¶ 52). Plaintiffs do not allege that through Johnson & Bell the Confidential Client Information was ever compromised or disclosed to others. Instead, plaintiffs claim is founded on a claim that the information could have possibly been compromised at some point in the future. (Ex. A, ¶ 25).

More specifically, plaintiffs claim Johnson & Bell uses a suite of computer systems in its operation, some of which are designed to interface with the internet (to be publicly accessible). (Ex. A, ¶13). Plaintiffs allege these systems allow internet access in three of their functions: (1) Webtime time and billing; (2) virtual private network (“VPN”) and (3) e-mail. (Ex. A, ¶ 13). The internet access allows firm personnel to enter time, access documents and files or send and receive e-mail while out of the office. (Ex. A, ¶ 25).

Plaintiffs do not allege an intrusion or unauthorized “hack” into any of the three functions. Nevertheless, plaintiffs claim certain “vulnerabilities” that could possibly allow an intrusion. And, further postulating, once in the system through one of the three functions, the undefined hacker could go to undefined places within defendant’s computer systems and then possibly access Confidential Client Information. (Ex. A, ¶¶ 1, 13). Again, plaintiffs do not allege this ever happened.

The primary so-called claimed vulnerability is that the Webtime time-tracking system uses a “JBoss Application Server” that is now allegedly out-of-date by “industry standards.” Johnson & Bell has advised plaintiffs pursuant to FRCP Rule 11 that this allegation is false, that at the time of filing Johnson & Bell did not use a “JBoss Application Server,” and that the claims should be withdrawn.

Plaintiffs also claim a so-called “vulnerability” in the VPN server in that it “supports insecure renegotiation, leaving it vulnerable to man-in-the-middle attacks,” which allegedly could possibly allow others to “eavesdrop on private communications and steal Confidential Client Information.” (Ex. A, ¶¶ 28, 29). With respect to the email server, plaintiffs allege it supports “SSL 2” and “512 bit export suite,” which are possibly “vulnerable” to outside attacks from hackers. (Ex. A, ¶¶ 32, 33).

Plaintiffs now contend all three alleged “vulnerabilities” no longer exist. (*See* Motion to Unseal, Ex. B, ¶¶ 3–5).

Plaintiffs claim they retained Johnson & Bell in respect to the *Hussein* matter and the terms of that retention are reflected in a written engagement letter (Ex. A, ¶ 51, Ex. 2). Plaintiffs further claim they expected their Confidential Client Information shared with Johnson & Bell would remain confidential (Ex. A, ¶ 54). Plaintiffs do not allege the confidential information did not

remain confidential or that it was ever compromised by Johnson & Bell. Rather they allege only that the information was “exposed” to possible compromise.

Nevertheless, plaintiffs claim “implicit” in Johnson & Bell’s written agreement to retain documents on the *Hussein* case is an agreement that Johnson & Bell “will keep all documents and files confidential using reasonable methods.” (Ex. A, ¶ 66, Ex. 2). Plaintiffs further claim that Johnson & Bell “breached the above contracts by exposing plaintiffs’ and the Class’s Confidential Client Information.” (Ex. A, ¶ 67).

Plaintiffs claim they were 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.” (Ex. A, ¶ 70). As alleged harm, plaintiffs claim a portion of the attorneys’ fees paid to Johnson & Bell was “to keep their Confidential Client Information secure” and that plaintiffs “did not receive their contracted benefits.” (Ex. A, ¶¶ 74, 75). However, again, nowhere do plaintiffs claim their Confidential Client Information did not remain confidential.

Nonetheless, based on these allegations, plaintiffs claim the following causes of action:

1. Breach of Contract (Legal Malpractice) (On behalf of plaintiffs and the Class).
2. Negligence (Legal Malpractice) (On behalf of plaintiffs and the Class) (In the alternative to the First Cause of Action).
3. Unjust Enrichment (On behalf of plaintiffs and the Class) (In the alternative to the First and Second Causes of Action).
4. Breach of Fiduciary Duty (On behalf of plaintiffs and the Class) (In the alternative to the First, Second and Third Causes of Action).

Plaintiffs seek injunctive relief; a declaratory judgment finding that Johnson & Bell’s conduct has constituted malpractice, breach of contract, negligence, unjust enrichment and/or breach of

fiduciary duty; and an order requiring Johnson & Bell to 1) inform its clients that its computer systems are not secure; 2) allow an independent third-party firm to conduct an audit of its security systems; 3) forfeit attorneys' fees paid during the time of alleged breach and any profits diverted from cybersecurity; 4) pay attorneys' fees; and 5) pay pre- and post-judgment interest. (Ex. A, Prayer for Relief).

For the separate but equally compelling reasons set out below, plaintiffs' complaint should be dismissed.

ARGUMENT

I. Plaintiffs' Complaint Should Be Dismissed Pursuant to Rule 12(b)(1) Because Plaintiffs Lack Article III Standing.

Because plaintiffs do not have standing, the Court must dismiss the complaint for lack of subject-matter jurisdiction under Rule 12(b)(1). Standing is "an essential and unchanging part of the case-or-controversy requirement of Article III" of the United States Constitution. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). To satisfy Article III standing, a plaintiff must show: (1) injury in fact; (2) that defendant's complained-of conduct caused that injury; and (3) a likelihood that the requested relief will redress that injury. *Id.* at 560. A plaintiff "is required to show it meets all elements necessary for standing." *Id.* at 561. "The question of standing is whether the litigant is entitled to have the court decide the merits of the dispute or particular issues." *Apex Digital, Inc. v. Sears, Roebuck & Co.*, 572 F.3d 440, 444 (7th Cir. 2009). "Because standing is not a mere pleading requirement but rather an indispensable part of the plaintiff's case, it must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of litigation." *Lujan*, 504 U.S. at 561. In ruling on a Rule 12(b)(1) motion, the Court may consider

extrinsic evidence. *See Conrad v. Nutramax Labs, Inc.*, 2013 WL 5288152, at *1 (N.D. Ill. Sept. 18, 2013).

To establish Article III standing, a plaintiff must demonstrate that it has “suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision. *P.F. Chang’s China Bistro, Inc. v. Lewert*, 2016 WL 1459226, No. 14-3700 (7th Cir. April 14, 2016). Here, plaintiffs cannot allege a “concrete and particularized” injury because none exists. Further, none of plaintiffs’ damages theories are sufficient to establish an injury for purposes of Article III standing. Accordingly, plaintiffs’ complaint should be dismissed.

A. Plaintiffs Have Not And Cannot Allege A Concrete and Particularized Injury.

Plaintiffs have not and cannot allege that they have suffered a “concrete and particularized injury” necessary for plaintiffs to have standing to bring this action. A concrete and particularized injury is one that is “actual or imminent, not conjectural or hypothetical.” *Lujan*, 504 U.S. at 560.

Plaintiffs’ complaint is littered with “ifs” and “could-bes” and references nothing more than a possibility of harm at some possible time in the unknown future. For example, plaintiffs allege: it is only “a *matter of time*” until hackers learn of the system vulnerabilities; “Johnson & Bell is a data breach *waiting to happen*;” and that the exposure of client information “*could be devastating*.” (Ex. A, ¶¶ 25, 36, 37). Tellingly, plaintiffs do not make any allegations of an *actual* injury. Plaintiffs do not allege that Johnson & Bell’s systems were ever breached or that any of its clients’ confidential information, including plaintiffs’ information, was ever compromised. Thus, plaintiffs have not suffered a “concrete and particularized injury” and do not have Article III standing to bring their claims.

B. Plaintiffs' Allegations Do Not Give Them Article III Standing.

The allegations that plaintiffs *do* make—that plaintiffs *could* be harmed in the future or that they were harmed by not receiving the “benefit of their bargain”—are not sufficient to give them standing to bring this action.

First, plaintiffs' allegations that they are threatened with future harm are insufficient to confer standing because (1) the alleged “vulnerabilities” identified in plaintiffs' complaint are no longer present; and (2) plaintiffs do not plead how, without these vulnerabilities, they are likely to suffer any future harm. “When an injury is threatened in the future, the risk of harm must be substantial and more than speculative.” *Otompke v. Hill*, 592 F. App'x 495, 498 (7th Cir. 2014), *reh'g denied* (Dec. 4, 2014), *cert. denied*, 136 S. Ct. 49 (2015). “Although imminence is [] a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending.” *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (emphasis original) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 564 (1992)).

Second, plaintiffs' benefit of the bargain theory is insufficient to establish an injury for purposes of Article III standing because plaintiffs' confidential information was never compromised, and thus, plaintiffs received the full benefit of their alleged bargain.

Plaintiffs' benefit of the bargain theory is based on allegations that a portion of the attorneys' fees paid to Johnson & Bell was “to keep their Confidential Client Information secure” and that plaintiffs “did not receive their contracted benefits.” (Ex. A, ¶¶ 74, 75).² However,

² Under plaintiffs' alternatively pled negligence claim, plaintiffs allege that Johnson & Bell failed to implement industry standard data security measures, which left their confidential information exposed. (Ex. A, ¶ 79.) Plaintiffs further allege that they suffered damages in that they would not have paid legal fees to Johnson & Bell or would have paid substantially less. (Ex. A, ¶ 80). Although plaintiffs' allegations are phrased somewhat differently under their negligence claim than under their other alleged causes of action, plaintiff's theory of damages is the same—they didn't receive the full benefit of the bargain.

plaintiffs do not claim that Johnson & Bell's computer systems were ever breached or that plaintiffs' Confidential Client Information was ever compromised. Accordingly, plaintiffs' benefit of the bargain claim is fatally defective.

Further, because plaintiffs' do not allege that confidential information was ever compromised, plaintiffs have not and cannot allege "something more" than vague, conclusory allegations of overpayment or diminished value of services. Like the present case, where the alleged wrong stems from allegations of insufficient performance, plaintiffs must allege something more than overpayment or diminished value of services to survive a motion to dismiss for lack of standing. *See In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588, at *5 (N.D. Ill. Sept. 3, 2013) (finding that plaintiffs' claim of injury in the form of diminished value of products and services was insufficient to establish standing); *Rivera v. Wyeth-Ayerst Labs.*, 283 F.3d 315, 320 (5th Cir. 2002) (rejecting the "benefit of the bargain" argument and dismissing the case for lack of standing where plaintiffs sought unjust enrichment for failure to receive the benefit but they had no damages); *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013) (granting a motion a dismiss for lack of standing under a "benefit of the bargain" theory and holding that because plaintiffs took issue with the way in which LinkedIn performed the security services, they had to allege "something more" than pure economic harm such as a harm that occurred as a result of the deficient security services and security breach—for example, theft of their personally identifiable information).³

In sum, plaintiffs have not satisfied their burden of demonstrating that they have Article III standing to bring this case before the Court. To the contrary, plaintiffs' complaint, combined with

³ Although the *LinkedIn* court ultimately denied a motion to dismiss plaintiff's later pled second amended complaint, the court made clear in its ruling that plaintiff had abandoned its "benefit of the bargain" theory. *In re LinkedIn Use Privacy Litigation*, 2014 WL 1323713, No. 5:12-CV-03088-ED, at *4 (N.D. Cal. March 28, 2014).

their subsequent admissions before this Court, demonstrates that they do not have standing because they have not alleged the necessary concrete, particularized injury required. As such, the Court must dismiss plaintiffs' complaint in its entirety.

II. Plaintiffs' Equitable Claims Should Be Dismissed Pursuant to Rule 12(b)(1) Because They Are Moot.

Under Article III, federal courts may adjudicate only actual, ongoing cases or controversies. *Hein v. Freedom From Religion Found., Inc.*, 551 U.S. 587, 597 (2007). Accordingly, a motion to dismiss under Rule 12(b)(1) should be granted when intervening events after the filing of a lawsuit prevent a court from ordering any relief, thus rendering the case moot. *Chafin v. Chafin*, 133 S. Ct. 1017, 1023, 185 L. Ed. 2d 1 (2013). Here, plaintiffs' equitable claims for injunctive and declaratory relief should be dismissed because a system compromise is not claimed and none of the three alleged so-called "vulnerabilities" identified in the complaint remain today. "The law does not require the performance of useless acts." *Nat'l Labor Rel. Bd. v. Die & Tool Makers Lodge No. 113*, 231 F.2d 298, 301 (7th Cir. 1956).

III. Counts III and IV of Plaintiffs' Complaint Should Be Dismissed Pursuant To Rule 12(b)(6) Because Plaintiffs Failed To State A Claim

A. Claim for Unjust Enrichment in Count III Cannot Be Stated Because a Contract Governs the Parties' Relationship.

Plaintiffs' alternative claim for unjust enrichment should be dismissed because the relationship between the parties is governed by a written contract, which plaintiffs have attached as an exhibit to their verified complaint.

"[T]he existence of an express contract forecloses recovery under a theory, such as unjust enrichment, implied in law." *Golden v. State Farm Mut. Auto. Ins. Co.*, 745 F.3d 252, 256 (7th Cir. 2014); *Chicago Title Ins. Co. v. Teachers' Ret. Sys.*, 2014 IL App (1st) 131452, ¶ 18, 7 N.E.3d 19, 24, *reh'g denied* (Mar. 20, 2014), *appeal denied sub nom. Chicago Title Ins. Co. v. Teachers'*

Ret. Sys, 20 N.E.3d 1252 (Ill. 2014) (finding that unjust enrichment is not an independent cause of action and is inapplicable when an express contract governs the parties' relationship). Further, "[a]lthough Fed.R.Civ.P. 8(e)(2) allows [parties] to plead alternative and inconsistent claims, when a party has incorporated allegations of a specific contract into an unjust enrichment claim, courts in this district have granted motions to dismiss those unjust enrichment claims." *Citadel Grp. Ltd. v. Sky Lakes Med. Ctr., Inc.*, No. 06-C-6162, 2008 WL 1924958, at *7 (N.D. Ill. Apr. 30, 2008); *Purizer Corp. v. Battelle Mem'l Inst.*, No. 01 C 6360, 2002 WL 22014 (N.D. Ill. Jan. 7, 2002) (dismissing unjust enrichment claim plead in the alternative because it incorporated by reference allegations of existing contracts).

Because plaintiffs attached the contract that explicitly governs the parties' relationship to their verified complaint in this matter, plaintiffs cannot maintain a claim for unjust enrichment. Consequently, plaintiffs' unjust enrichment claim should be dismissed.

B. Breach of Fiduciary Duty Claim is Duplicative.

Plaintiffs' first and second causes of action are for legal malpractice and its fourth cause of action is based on the same facts and claims a breach of fiduciary duty. The claim for breach of fiduciary duty should be dismissed as duplicative. *See Hassebrock v. Bernhoft*, 815 F.3d 334, 343 (7th Cir. 2016) (recognizing Illinois case law holding that breach-of- fiduciary-duty claims plead alongside malpractice claims are properly dismissed as duplicative); *Hoagland ex rel. Midwest Transit, Inc. v. Sandberg, Phoenix & von Gontard, P.C.*, 385 F.3d 737, 744 (7th Cir. 2004) ("Illinois courts hold that 'when a breach of fiduciary duty claim is based on the same operative facts as a legal malpractice claim, and results in the same injury, the later claim should be dismissed as duplicative.'").

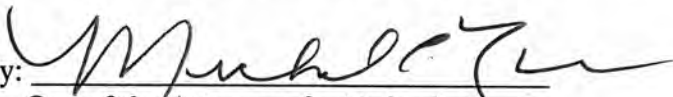
Under Illinois law, a fiduciary duty claim is considered duplicative of an attorney malpractice claim and should be dismissed. *Calhoun v. Rane*, 234 Ill. App. 3d 90, 599 N.E.2d 1318 (1st Dist. 1992) (dismissal of fiduciary duty count as duplicative of legal malpractice count affirmed); *Majumdar v. Lurie*, 274 Ill.App.3d 267, 273–74, 653 N.E.2d 915, 921 (1995) (“when, as in this case, the same operative facts support actions for legal malpractice and breach of fiduciary resulting in the same injury to the client, the actions are identical and the later should be dismissed as duplicative.”).

CONCLUSION

WHEREFORE Defendant Johnson & Bell, Ltd. respectfully requests that this Court dismiss “Plaintiffs’ Verified Class Action Complaint” with prejudice, and grant such other and further relief as this Court deems just and proper.

Respectfully submitted,

WILLIAMS MONTGOMERY & JOHN LTD.

By: 
One of the Attorneys for Defendant

Michael C. Bruck
Megan A. Zmick
Max H. Gaston
Williams Montgomery & John Ltd.
233 S. Wacker Drive, Suite 6100
Chicago, Illinois 60606
312-443-3200
Firm ID 04933

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

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

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

Plaintiffs,

v.

JOHNSON & BELL, LTD, an Illinois
corporation,

Defendant.

DOCUMENT FILED PROVISIONALLY
UNDER SEAL

RECEIVED

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.

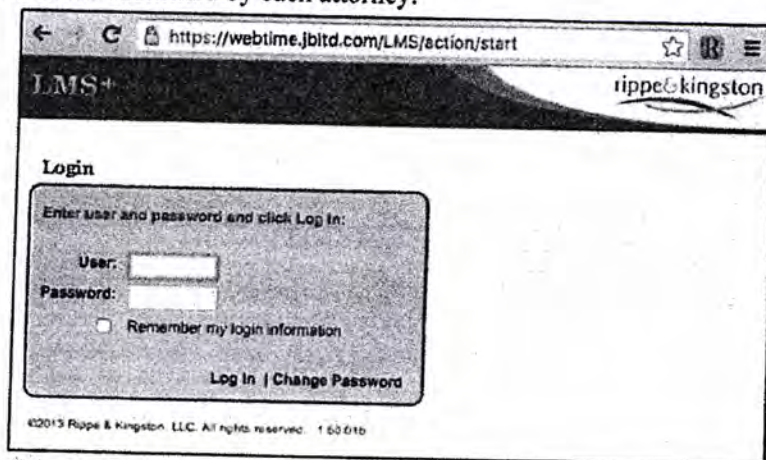
II. Johnson & Bell Has Failed To Secure Confidential Client Information, Exposing the Data to Hackers and Thieves.

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 governments⁹ 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 Decrypting RSA with Obsolete and Weakened ENcryption) "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.

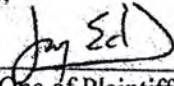
JURY DEMAND

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

Exhibit 1

4/7/2016

Don't Let Cybersecurity Breaches Lead to Legal Malpractice: The Fax Is Back

Don't Let Cybersecurity Breaches Lead to Legal Malpractice: The Fax Is Back

E-mail and wire fraud risks increase in a cloud-based world. Data management safeguards can prevent possible legal malpractice from cyber-security breaches.

By Joseph R. Marconi & Brian C. Langs¹

Johnson & Bell, Ltd.

Chicago

Back in July of 2011, we warned of a then popular e-mail/fraudulent check scheme whereby lawyers would receive e-mails from alleged potential foreign clients looking to collect debts from customers. Those scammers convinced the unsuspecting lawyers to deposit fraudulent "settlement checks" into client accounts and wire the "clients' share" to foreign accounts after the bogus checks cleared. When the frauds were eventually uncovered by the banks, the lawyers were left with liability to the banks for the fraudulent check and wire transfers.² Since then, newer, more complex electronic scams have surfaced whereby hackers intercept e-mails between lawyers and clients that contain wire transfer instructions. After intercepting such an e-mail, the hacker changes the instructions in the e-mail to wire money to his own untraceable account. The hacker forwards his bogus wiring instructions to the unsuspecting recipient, all while "masking" his identity as the sender and making it appear to the recipient as if the instruction came from the correct sender, whether lawyer or client.

It's cloud's illusions that I recall
I really don't know clouds at all...

— *Judy Collins*

Attorneys Present a Target for Sophisticated Hackers & Wire Fraud

Depending on your firm's sophistication and budget, the type of transaction involved, and the needs of your client, there are some preventative measures that can be considered with regard to protecting your firm and your clients from this and other wire transfer and electronic fraud schemes. Prevention techniques can include hiring a third-party e-mail encryption service provider or sending sensitive wire transfer instructions via facsimile rather than e-mail.³

4/7/2016

Don't Let Cybersecurity Breaches Lead to Legal Malpractice: The Fax Is Back

This and other even more sophisticated electronic scams are becoming more prevalent. 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. Whether an attorney transfers or stores confidential client information using password-protected corporate e-mail systems, "cloud computing,"⁴ third-party off-site network administrator vendors, third-party hosted e-discovery management platforms, or a variety of other electronic data transfer or data storage solutions available through the Internet, the attorney inevitably faces an inherent risk that confidential client information will be susceptible to theft by a hacker or by an unscrupulous third-party employee. In the absence of reasonable, preventative, and precautionary measures, the lawyer also risks losses for the firm and its clients associated with such a theft.

Understanding how and why lawyers and law firms may be exposed to cybercrime is the first step in prevention. Because of the ever increasing capabilities of cloud computing and, with it, the proliferation of everyday use of mobile devices—such as smartphones, tablets, and laptops—lawyers and law firms put sensitive client material at risk simply by falling asleep on the train home or finishing a brief on the redeye. A misplaced smartphone or briefcase can result in serious consequences if a device ends up in the wrong hands. 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 communications and strategy, and internal corporate strategies—much of which can be very valuable to an array of criminal enterprises.

Professional Obligations of Attorneys in the Cloud

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.⁵ However, to be competitive in today's legal services market, lawyers and law firms must utilize the cost-saving and organizational advantages technology allows them to offer recurring and prospective clients. 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. The extent and levels of necessary safeguards will likely be determined by the size of the law firm and its areas of practice, among other considerations. Depending on the specific needs of a firm or solo practitioner, there is a vast selection of cyber security precautions available but every law firm utilizing the technology discussed in this article should at least consider undertaking the following.⁶

Implement Data Management Safeguards

4/7/2016

Don't Let Cybersecurity Breaches Lead to Legal Malpractice: The Fax Is Back

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, and Citrix-like virtual desktops also invariably require password protection. In today's corporate environments, while all networks and company laptops probably employ anti-virus protection, employees using personal laptops to perform work outside of the office must be required to install similar anti-virus protection. Firm policies should include periodic inspections of mobile devices and personal laptops to ensure that employees do not turn off password and/or anti-virus protection functions out of convenience or technical incompetence. 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.

Address Firm Data Retention Policies

A law firm likely houses an incredible amount of data through its electronic document management system and its corporate network and e-mail system. It should maintain clear policies regarding the length of time certain types of data will be stored, the strength of security to be maintained for certain stored data, and the procedures for eliminating unnecessary or outdated data. Just as a law firm is routinely required to destroy or shred sensitive hard copy materials, it must have procedures in place to completely remove and destroy sensitive electronic data from firm databases and to destroy unwanted or out of date firm equipment that may have housed sensitive information.

In conclusion, attorneys can and should take the necessary precautions to minimize the likelihood of cyber-security breaches, not only to give their clients peace of mind, but also to better shield themselves from third-party and first-party liabilities if a theft of information or other security breach actually occurs.

[1] Joe is a shareholder of Johnson & Bell, Ltd., and the chairman of the business litigation/transaction group and co-chair of the employment group. He appreciates Johnson & Bell associate, Brian C. Langs, for his assistance in the drafting of this article.

[2] For the full article, see Joseph R. Marconi and Victor J. Pioli, *Lawyers are Increasingly the Targets of Email/Fraudulent Check Schemes*, ISBA Mutual Insurance Company Liability Minute, (July 13, 2011 12:46 PM), <http://www.isbamutual.com/liability-minute/lawyers-are-increasingly-the-targets-of-emailfraud>.

[3] For more detailed information and recommendations regarding protecting your firm and your clients from e-mail interception and other types of check and wire transfer fraud, see Ronald Trubiana, *Title Agents and Lawyers: Be Wary and Protect Yourself*, THE TRUSTED ADVISOR, October 2010, <http://www.atgf.com/tools->

4/7/2016

Don't Let Cybersecurity Breaches Lead to Legal Malpractice: The Fax Is Back

[publications/trusted-adviser/check-and-wire-transfer-fraud-growth-industry](#) (last visited July 25, 2014); ALTA Best Practices Frequently Asked Questions: Best Practices #3: Email Encryption, ATTORNEYS' TITLE GUARANTY FUND, <http://www.atgf.com/tools-publications/alta-best-practices-frequently-asked-questions> (last visited July 25, 2014); Ronald Trubiana, *Update from ATG Administration: Five Ways to Reduce Exposure to Wire Fraud*, THE TRUSTED ADVISOR, April 2010, <http://www.atgf.com/tools-publications/trusted-adviser/five-ways-reduce-exposure-wire-fraud> (last visited July 25, 2014).

[4]"Cloud computing" can include receiving and sending e-mails on a smartphone or tablet; using a web-based email platform like Gmail, Yahoo! or Microsoft Outlook Web Access; or using products like Google Docs, Microsoft Office 365, Dropbox, SharePoint intranets/extranets, and Citrix Desktop as a Service ("DaaS"). As Formal Opinion 2011-200 of the Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility aptly remarks, "cloud computing is merely a fancy way of saying stuff's not on your computer."

[5]See Ill. State Bar Ass'n Adv. Op. Prof'l. Conduct Nos. 96-10, 10-01; see also State Bar Ariz. Ethics Op. 09-04; N.Y. State Bar Ass'n Ethics Adv. Op. 842; Mass. Bar Ass'n Ethics Op. 12-03; Pa. Bar Ass'n Form. Op. 2011-200 (all discussing substantially similar versions of subsection (a) of IRCP 1.6, entitled "Confidentiality of Information," and its applicability to a lawyer's ethical duty to protect electronically stored or transferred confidential client information).

[6]Much of the content below making particular suggestions for precautionary actions by law firms was taken from two excellent articles: Seth L. Laver, *Understanding and Protecting Against Cyber Risk*, FOR THE DEFENSE (DRI's Monthly Magazine), July 2012 at 46-49 and Rene L. Siemens and David L. Beck, *Cyber Insurance—Mitigating Loss from Cyber Attacks*, PERSPECTIVES ON INSURANCE RECOVERY NEWSLETTER, Summer 2012, <http://www.pillsburylaw.com/publications/cyber-insurancemitigating-loss-from-cyber-attacks> (last visited July 8, 2014). Both articles are recommended readings that provide detailed discussion of many of the issues raised in this article.

Exhibit 2

JOHNSON & BELL
TRIAL LAWYERS

Joseph R. Marconi

WRITER'S DIRECT DIAL: (312) 984-0211

E-MAIL: marconij@jbltd.com

August 22, 2014

VIA ELECTRONIC SUBMISSION

Jason Shore
jay@coinabul.com

RE: *Yazan Hussein, et al. v. Coinabul, LLC, et al.*
Court No: 14-cv-05735

Dear Mr. Shore:

This engagement letter confirms the engagement of Johnson & Bell, Ltd, an Illinois corporation ("J&B"), to represent you, individually, and Coinabul, LLC, ("you"), and the basis on which J&B will represent you. We appreciate your confidence and thank you for selecting J&B as your counsel for this matter.

1. Scope of Representation. J&B will be representing you in defense of the above referenced lawsuit.

Except as we may agree otherwise in writing, J&B will be representing only you and Coinabul, LLC will not be representing any of its parents, subsidiaries, affiliated entities, shareholders, partners, directors, officers, agents, or employees. J&B will advise you in connection with, and the scope of J&B's engagement and duties to you shall relate solely to, the defense of the *Hussein v. Coinabul, et al.* Litigation and the prosecution of possible cross-claims and counterclaims (or third-party claims) against any potentially liable persons or entities.

Because the representation is limited to a specific undertaking, J&B's acceptance of this engagement does not involve an undertaking to represent you or your interests in any other matter unless specifically requested by you and agreed to in writing by J&B.

Fees and Expenses. Our fees are based substantially upon hours charged, recorded in tenth of an hour increments, at J&B's scheduled rates which are in effect at the time the services are performed. Those scheduled rates are periodically adjusted, generally at the beginning of a calendar year. Reasonable adjustments to the scheduled rates may also be made in particular matters to account for the complexity of issues, uniqueness of the services provided, or previous experience of the attorneys involved. My present hourly rate is \$400, Frank P. Nowicki \$325,

CHICAGO OFFICE PH (312) 372-0770 / FAX (312) 372-9818
SUITE 2700 / 33 WEST MONROE ST / CHICAGO, IL 60603-5404

INDIANA OFFICE PH (219) 791-1900 / FAX (219) 791-1901
SUITE B / 11051 BROADWAY ST / CROWN POINT, IN 46307

WWW.JOHNSONANDBELL.COM

JOHNSON & BELL
TRIAL LAWYERS

Jason Shore
Coinabul, LLC
August 22, 2014
Page 2 of 4

Victor Pioli \$300, Ann Zipfel \$225 and Brian C. Langs is \$200.00 and \$125 for paralegals and project assistants.

Our invoices will include, in addition to charges for professional services, costs incurred on your behalf, including, but not necessarily limited to: filing fees, telephone toll charges, photocopy charges, messenger and overnight courier, postage costs for large volume mailings or special postage services, fax costs, word processing charges, secretarial and word processing operator overtime, librarian and computer research costs, and attorney and staff travel and meal costs which have not been billed directly to you. These items will be invoiced in accordance with our regularly established procedures and charges.

It is our policy not to advance the costs of services provided by outside vendors in amounts exceeding \$500. We will forward invoices from such vendors to you for payment directly to the vendors. You agree to pay all such invoices promptly.

You have agreed to wire \$30,000 to our law firm's account before close of business on Monday, August 25, 2014, as a condition precedent to our filing an appearance in the above referenced lawsuit. Said funds will be held in our segregated client's fund account as security for the payment of fees in this case. In addition to providing said security you have agreed to pay each invoice for services within fourteen (14) days of receipt of said invoice. It is the intent of both our firm and you that the security deposit will not be diminished and will remain intact as you will pay invoices as received in addition to maintaining the above deposit.

Termination of Representation. Either of us may terminate the engagement at any time for any reason by providing written notice, subject on the part of J&B to the requirements of applicable rules of professional conduct. Unless we agree to render additional legal services for you, J&B's representation of you and the attorney/client relationship will terminate upon the date J&B sends its disengagement letter to you.

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.

At the termination of the representation and for a period of two (2) years thereafter, and provided there are no outstanding unpaid statements for fees and charges owed by you to J&B, you shall have the right on request to take possession of Your File, not including the Work Product. In such event, J&B at its expense may make and retain copies of all or portions of Your File. If you do not request possession of Your File within such two (2) year period, J&B will

JOHNSON & BELL
TRIAL LAWYERS

Jason Shore
Coinabul, LLC
August 22, 2014
Page 3 of 4

have no further responsibility for the retention and maintenance of Your File and may at its option dispose of all or parts of Your File without further notice to you.

Litigation Hold Directive. This litigation places an obligation upon you to preserve documents that might be relevant to the litigation. The preservation obligation includes both paper documents (writings on paper that can be read without the aid of computer devices such as correspondence, memoranda, handwritten notes and similar documents) as well as electronic documents (writings that can only be read through the use of computers). The "litigation hold" requires you to suspend your routine document retention/destruction policy immediately as it relates to documents that are required to be preserved. A directive should be sent to all employees to produce electronic copies of their relevant active files and make sure that all backup media which you are required to retain (i.e., actively used for information retrieval), are identified and stored in a safe place. Please institute this "litigation hold" in writing on a company wide basis, retain the writing in the event it is needed in the future, and forward a copy of the writing to us for our files. Please call us if you have any questions regarding your litigation hold responsibilities or need assistance in implementing the litigation hold.

Please signify your agreement to the arrangement for legal services described in this letter by returning to us a signed copy of the engagement letter. By signing this engagement letter on your behalf, the signatory warrants that he or she has the authority to engage us to represent you as set forth in this engagement letter. In most instances, we will not commence work on your behalf unless and until we have received the signed copy of this engagement letter. However, on occasion, we may be required to commence work on your behalf before receipt of the signed engagement letter. Under those circumstances, we retain the right to stop work and if needed, close the file, should you fail to sign and return the engagement letter.

We recommend that you seek the advice of independent counsel before signing this engagement letter. If we receive the signed engagement letter, we will presume that you have either consulted with independent counsel and chosen to go forward with our representation of you in the *Hussein v. Coinabul, LLC, et al.* Litigation or have considered the terms of the engagement letter and chosen to retain us without the need for the advice of independent counsel.

Arbitration of Disputes. Although we do not expect that any dispute between us will arise, in the unlikely event of any dispute under this agreement, including a dispute regarding the amount of fees or the quality of our services, such dispute shall be determined through binding arbitration with the mediation/arbitration services of JAMS Endispute of Chicago, Illinois. Any such arbitration shall be held in Chicago, Illinois unless the parties agree in writing to some other location. Each party to share the costs of the arbitration proceeding equally. Each party will be responsible for their own attorney's fees incurred as a result of the arbitration proceeding.

If any provision of this agreement is held to be void, voidable or unenforceable, the remaining provisions shall remain in full force and effect.

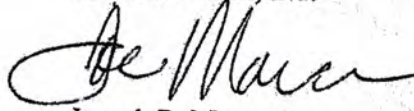
JOHNSON & BELL
TRIAL LAWYERS

Jason Shore
Coinabul, LLC
August 22, 2014
Page 4 of 4

We look forward to working with you in the *Hussein v. Coinabul, LLC, et al.* Litigation.

Very truly yours,

Johnson & Bell, Ltd.



Joseph R. Marconi

COINABUL, LLC, a Wyoming limited liability company

By: _____

Title: _____

Date: _____

#3831091

TERMED, VALDEZ

**United States District Court
Northern District of Illinois - CM/ECF LIVE, Ver 6.1.1 (Chicago)
CIVIL DOCKET FOR CASE #: 1:14-cv-05735**

Hussein v. Coinabul, LLC et al
Assigned to: Honorable James B. Zagel
Demand: \$9,999,000
Cause: 28:1332 Diversity-Other Contract

Date Filed: 07/25/2014
Date Terminated: 06/18/2015
Jury Demand: Both
Nature of Suit: 190 Contract: Other
Jurisdiction: Diversity

Plaintiff

Yazan Hussein

*individually and on behalf of all others
similarly situated,*

represented by **Rafey S. Balabanian**

Edelson PC
329 Bryant Street
Suite 2C
San Francisco, CA 94107
(415)212-9300
Fax: 415.373.9435
Email: rbalabanian@edelson.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Alicia Elaine Hwang

Edelson P.C.
350 North La Salle
Suite 1300
Chicago, IL 60654
(312) 572-7214
Email: ahwang@edelson.com
ATTORNEY TO BE NOTICED

Benjamin Scott Thomassen

Edelson P.C.
350 North LaSalle Street
Suite 1300
Chicago, IL 60654
(312) 589-6370
Fax: (312) 589-6378
Email: bthomassen@edelson.com
ATTORNEY TO BE NOTICED

David Ira Mindell

Edelson P.C.
350 North LaSalle
Suite 1300
Chicago, IL 60654
(312) 572-7213
Fax: (312) 589-6378
Email: dmindell@edelson.com



ATTORNEY TO BE NOTICED

V.

Defendant

Coinabul, LLC
a Wyoming limited liability company

represented by **Coinabul, LLC**
PRO SE

Ann Elizabeth Zipfel
Johnson And Bell, Ltd.
33 West Monroe Street
Suite 2700
Chicago, IL 60603
(312) 984-0282
Email: zipfela@jbltd.com
TERMINATED: 03/03/2015

Brian C. Langs
Johnson & Bell Ltd.
33 W. Monroe St.
Chicago, IL 60603
(312) 372-0770
Email: langsb@jbltd.com
TERMINATED: 03/03/2015

Frank P. Nowicki
Johnson & Bell, Ltd.
33 West Monroe Street
Suite 2700
Chicago, IL 60603
(312) 372-0770
Email: nowickif@jbltd.com
TERMINATED: 03/03/2015

Joseph R. Marconi
Johnson & Bell, Ltd.
33 West Monroe Street
Suite 2700
Chicago, IL 60603
(312) 984-0211
Fax: 312-372-9818
Email: marconij@jbltd.com
TERMINATED: 03/03/2015

Defendant

Jason Shore
an individual,

represented by **Jason Shore**
PRO SE

Ann Elizabeth Zipfel
(See above for address)
TERMINATED: 03/03/2015

Brian C. Langs
 (See above for address)
 TERMINATED: 03/03/2015

Frank P. Nowicki
 (See above for address)
 TERMINATED: 03/03/2015

Joseph R. Marconi
 (See above for address)
 TERMINATED: 03/03/2015

Date Filed	#	Docket Text
07/25/2014	<u>1</u>	COMPLAINT filed by Yazan Hussein; Jury Demand. Filing fee \$ 400, receipt number 0752-9707533. (Attachments: # <u>1</u> Civil Cover Sheet)(Thomassen, Benjamin) (Entered: 07/25/2014)
07/25/2014	<u>2</u>	MOTION by Plaintiff Yazan Hussein to certify class (Thomassen, Benjamin) (Entered: 07/25/2014)
07/25/2014		CASE ASSIGNED to the Honorable James B. Zagel. Designated as Magistrate Judge the Honorable Maria Valdez. (rc,) (Entered: 07/25/2014)
07/28/2014		SUMMONS Issued as to Defendants Coinabul, LLC, Jason Shore (pg,) (Entered: 07/28/2014)
08/04/2014	<u>3</u>	SUMMONS Returned executed by Plaintiff Yazan Hussein regarding Summons in a Civil Case, Class Action Complaint and Demand for Jury Trial, Plaintiff's Motion for and Memorandum in Support of Class Certification, Letter Dated July 28, 2014 served on Coinabul, LLC on July 29, 2014; Answer due August 19, 2014. (Thomassen, Benjamin) (Docket text modified by Clerk's Office.) (tln). (Entered: 08/04/2014)
08/06/2014	<u>4</u>	ATTORNEY Appearance for Plaintiff Yazan Hussein by David Ira Mindell (Mindell, David) (Entered: 08/06/2014)
08/06/2014	<u>5</u>	ATTORNEY Appearance for Plaintiff Yazan Hussein by Benjamin Scott Thomassen (Thomassen, Benjamin) (Entered: 08/06/2014)
08/06/2014	<u>6</u>	ATTORNEY Appearance for Plaintiff Yazan Hussein by Rafey S. Balabanian (Balabanian, Rafey) (Entered: 08/06/2014)
08/06/2014	<u>7</u>	ATTORNEY Appearance for Plaintiff Yazan Hussein by Alicia Elaine Hwang (Hwang, Alicia) (Entered: 08/06/2014)
08/29/2014	<u>8</u>	ATTORNEY Appearance for Defendants Coinabul, LLC, Jason Shore by Joseph R. Marconi (Marconi, Joseph) (Entered: 08/29/2014)
08/29/2014	<u>9</u>	ATTORNEY Appearance for Defendants Coinabul, LLC, Jason Shore by Ann Elizabeth Zipfel (Zipfel, Ann) (Entered: 08/29/2014)
08/29/2014	<u>10</u>	ATTORNEY Appearance for Defendants Coinabul, LLC, Jason Shore by Frank P. Nowicki (Nowicki, Frank) (Entered: 08/29/2014)
08/29/2014	<u>11</u>	MOTION by Defendants Coinabul, LLC, Jason Shore for extension of time to file answer regarding complaint <u>1</u> DEFENDANTS' MOTION FOR EXTENSION OF TIME TO ANSWER OR OTHERWISE PLEAD TO PLAINTIFF'S COMPLAINT (Zipfel, Ann) (Entered: 08/29/2014)
08/29/2014	<u>12</u>	NOTICE of Motion by Ann Elizabeth Zipfel for presentment of motion for extension of time to file answer, motion for relief <u>11</u> before Honorable James B. Zagel on 9/4/2014 at 09:30 AM. (Zipfel, Ann) (Entered: 08/29/2014)

09/03/2014	<u>13</u>	ENTERED in ERROR (Langs, Brian). Modified on 9/3/2014 (gcy,). (Entered: 09/03/2014)
09/03/2014	<u>14</u>	NOTICE of Correction regarding attorney appearance <u>13</u> . (gcy,) (Entered: 09/03/2014)
09/03/2014	<u>15</u>	ATTORNEY Appearance for Defendants Coinabul, LLC, Jason Shore by Brian C. Langs (Langs, Brian) (Entered: 09/03/2014)
09/03/2014	<u>16</u>	MINUTE entry before the Honorable James B. Zagel: Defendants' Motion for an Extension of Time <u>11</u> is granted. Defendants shall answer or otherwise plead on or before 10/3/14. Hearing set for 9/4/14 is stricken and no appearance is necessary. Status hearing set for 10/21/14 at 9:15 a.m. Mailed notice (ep,) (Entered: 09/03/2014)
09/08/2014	<u>17</u>	SUMMONS Returned Executed by Yazan Hussein as to Jason Shore on 8/9/2014, answer due 9/1/2014. (Hwang, Alicia) (Entered: 09/08/2014)
10/03/2014	<u>18</u>	MOTION by Defendants Jason Shore, Coinabul, LLC to dismiss <i>pursuant to Fed. R. Civ. P. 12(b)(3)</i> , MOTION by Defendants Jason Shore, Coinabul, LLC to strike complaint <u>1</u> <i>class allegations</i> (Attachments: # <u>1</u> Exhibit A)(Zipfel, Ann) (Entered: 10/03/2014)
10/03/2014	<u>19</u>	NOTICE of Motion by Ann Elizabeth Zipfel for presentment of motion to dismiss, motion to strike, motion for relief,,, <u>18</u> before Honorable James B. Zagel on 10/21/2014 at 09:30 AM. (Zipfel, Ann) (Entered: 10/03/2014)
10/21/2014	<u>20</u>	MINUTE entry before the Honorable James B. Zagel: Motion hearing held. Defendants' Jason Shore, Coinabul, LLC Motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(3) <u>18</u> is entered and continued. Plaintiff's Response due 11/4/2014. Defendants' Reply due 11/18/2014. Status/Ruling hearing set for 12/16/2014 at 9:15 a.m. Mailed notice. (nf,) (Entered: 10/22/2014)
11/04/2014	<u>21</u>	MOTION by Plaintiff Yazan Hussein for extension of time to file response/reply as to motion to dismiss, motion to strike, motion for relief,,, <u>18</u> [<i>Unopposed Motion to Extend Briefing Schedule on Defendants' Motion to Dismiss</i>] (Thomassen, Benjamin) (Entered: 11/04/2014)
11/04/2014	<u>22</u>	MINUTE entry before the Honorable James B. Zagel: Plaintiff's Unopposed Motion to Extend Briefing Schedule on Defendants' Motion to Dismiss <u>21</u> is granted. Plaintiff's Response due by 11/11/2014, Defendants' Replies due by 11/25/2014. Mailed notice. (nf,) (Entered: 11/04/2014)
11/11/2014	<u>23</u>	RESPONSE by Yazan Husseinin Opposition to MOTION by Defendants Jason Shore, Coinabul, LLC to dismiss <i>pursuant to Fed. R. Civ. P. 12(b)(3)</i> MOTION by Defendants Jason Shore, Coinabul, LLC to strike complaint <u>1</u> <i>class allegations</i> <u>18</u> (Attachments: # <u>1</u> Exhibit 1 - Balabanian Decl., # <u>2</u> Exhibit 2 - Hussein Decl.)(Balabanian, Rafey) (Entered: 11/11/2014)
11/25/2014	<u>24</u>	REPLY by Defendants Coinabul, LLC, Jason Shore to motion to dismiss,, motion to strike,, motion for relief, <u>18</u> (<i>attachment filed separately</i>) (Zipfel, Ann) (Entered: 11/25/2014)
11/25/2014	<u>25</u>	DECLARATION of Jason Shore regarding reply <u>24</u> (Zipfel, Ann) (Entered: 11/26/2014)
11/26/2014	<u>26</u>	Attachment to Declaration (Dkt # <u>25</u>) by Coinabul, LLC, Jason Shore (Zipfel, Ann) Docket Text Modified by Clerk's Office on 11/26/2014 (ph,). (RESTRICTED) (Entered: 11/26/2014)
12/02/2014	<u>27</u>	MOTION by Defendants Coinabul, LLC, Jason Shore to seal document other <u>26</u> (Zipfel, Ann) (Entered: 12/02/2014)
12/02/2014	<u>28</u>	NOTICE of Motion by Ann Elizabeth Zipfel for presentment of motion to seal document, motion for relief <u>27</u> before Honorable James B. Zagel on 12/9/2014 at 09:30 AM. (Zipfel, Ann) (Entered: 12/02/2014)
12/08/2014	<u>29</u>	MINUTE entry before the Honorable James B. Zagel: The defendants' agreed motion to motion to place document Motion to seal document <u>27</u> is granted. The Clerk's Office shall place document <u>26</u> under seal. No appearance is required on 12/9/2014. Mailed notice (cdh,) (Entered: 12/08/2014)

12/12/2014	<u>30</u>	MINUTE entry before the Honorable James B. Zagel: The hearing set for 12/16/2014 is canceled and reset to 1/28/2015 at 9:30 a.m. No appearance is required on 12/16/2014. Mailed notice (cdh,) (Entered: 12/12/2014)
12/19/2014	<u>31</u>	MEMORANDUM OPINION AND ORDER Signed by the Honorable James B. Zagel on 12/19/2014. Defendants' motion to dismiss and motion to strike the class action allegations are both denied. Mailed notice(cdh,) (Entered: 12/19/2014)
01/13/2015	<u>32</u>	ANSWER to Complaint with Jury Demand by Coinabul, LLC, Jason Shore(Zipfel, Ann) (Entered: 01/13/2015)
01/28/2015	<u>33</u>	MINUTE entry before the Honorable James B. Zagel:Status hearing held on 1/28/2015 and continued to 4/28/2015 at 09:15 AM.Mailed notice (kef,) (Entered: 01/28/2015)
02/02/2015	<u>34</u>	MOTION by counsel for Defendants Coinabul, LLC, Jason Shore to withdraw as attorney <i>for the Defendants without Substitution</i> (Zipfel, Ann) (Entered: 02/02/2015)
02/02/2015	<u>35</u>	NOTICE of Motion by Ann Elizabeth Zipfel for presentment of motion to withdraw as attorney <u>34</u> before Honorable James B. Zagel on 2/24/2015 at 09:30 AM. (Zipfel, Ann) (Entered: 02/02/2015)
02/03/2015	<u>36</u>	<i>Amended</i> NOTICE of Motion by Ann Elizabeth Zipfel for presentment of motion to withdraw as attorney <u>34</u> before Honorable James B. Zagel on 2/24/2015 at 09:30 AM. (Zipfel, Ann) (Entered: 02/03/2015)
02/24/2015	<u>37</u>	MINUTE entry before the Honorable James B. Zagel: Defendants' Motion to Withdraw Counsel of Record without Substitution <u>34</u> is granted. Defendants' counsel are granted leave to withdraw no earlier than 3/3/15. Status hearing set for 4/28/15 is stricken and reset to 4/7/15 at 9:15 a.m. Mailed notice (ep,) (Entered: 02/24/2015)
04/07/2015	<u>38</u>	MINUTE entry before the Honorable James B. Zagel: Status hearing held and continued to 5/6/15 at 9:15 a.m. Failure of Defendant to appear at the next status hearing may result in default judgment. Mailed notice (ep,) (Entered: 04/07/2015)
05/06/2015	<u>39</u>	MINUTE entry before the Honorable James B. Zagel: Status hearing held. Defendant failed to appear. In accordance with the Court's Order issued on 4/7/15 <u>38</u> , default is entered. Prove-up hearing set for 6/4/15 at 9:30 a.m. Mailed notice (ep,) (Entered: 05/07/2015)
06/01/2015	<u>40</u>	MINUTE entry before the Honorable James B. Zagel: Prove-up hearing set for 6/4/15 is stricken and reset to 6/18/15 at 9:30 a.m. Mailed notice (ep,) (Entered: 06/01/2015)
06/17/2015	<u>41</u>	DECLARATION of Yazan Hussein <i>in Support of Damages Prove-Up</i> (Attachments: # <u>1</u> Exhibit A, # <u>2</u> Exhibit B, # <u>3</u> Exhibit C, # <u>4</u> Exhibit D, # <u>5</u> Exhibit E, # <u>6</u> Exhibit F)(Scharg, Ari) (Entered: 06/17/2015)
06/18/2015	<u>42</u>	MINUTE entry before the Honorable James B. Zagel: Prove-up hearing held. Pursuant to Plaintiff's Declaration in Support of Damages <u>41</u> , default judgment is entered in favor of Plaintiff and against Defendants in the amount of \$1,557,247.82 in damages and \$816.00 in costs. Counsel may submit a judgment order to the Court's proposed orders inbox. All pending motions are moot. Civil case terminated. Mailed notice (ep,) (Entered: 06/19/2015)
07/06/2015	<u>43</u>	ORDER of Default Judgment. Signed by the Honorable James B. Zagel on 7/6/2015.(lcw,) (Entered: 07/06/2015)

PACER Service Center
Transaction Receipt
05/03/2016 16:47:57