CONTINUING
LEGAL EDUCATION

Quite a Catch! Phishing for Social Engineering Fraud and Understanding the Importance of Legal Project Management

Presentation for the Rhode Island Bar Association

Thomas Wilson Jr., Esquire
Scott Schaffer, Esquire
Jonathan Meer, Esquire
Wilson Elser, Moskowitz, Edelman & Dicker, LLP, NY, NY

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

Quite a Catch! Phishing for Social Engineering Fraud and Understanding the Importance of Legal Project Management

Rhode Island Bar Association

Table of Contents

Tab

Tab A

WILSON ELSER

Professional Liability
Advocate

Rise in Cyberattacks on Professional Services Firms

By Gregory Bautista on January 20, 2016

POSTED IN ACCOUNTANTS, CYBERSECURITY & DATA PRIVACY

Wilson Elser's Cyber Incident Response Team has seen an alarming uptick in cyber-criminal activity targeted at professional services firms, particularly accounting firms. As described in more detail below, the criminal activity follows a very specific pattern. We take this opportunity to remind all professionals of the need to be wary and skeptical of what communications they receive electronically. Consider starting the New Year with training and education for yourself as well as your partners, staff and employees on cyber risk and how to best avoid an attack and mitigate any damages if an attack occurs. In the past three months, we have noticed a pattern of activity targeted at small to midsize professional services firms. Attackers attempt to

gain access to computer systems containing sensitive financial information, which may result in a legal duty on the part of the professional to notify their clients that their confidential information was or may have been exposed.

So what does an attack look like?

In one scenario, a professional services firm's partner or employee receives an email offering a free download of a program such as Microsoft Office 365, Windows 10 or some other desirable program. The email appears to be legitimate, and when the user clicks on it, a pop-up message provides a number for the user to call. The number connects the user with what seems to be a legitimate company. The cyber-criminal responding to the call then asks for access to the user's computer, citing a need to check for viruses or to see if the computer is compatible with the download, or some other legitimate-sounding reason. Once the user provides access, the cyber-criminal tells the user that the computer is infected, and tries to sell an anti-virus or anti-malware software for about $350.

Even if the sale is rejected by the user, once access is granted, the cyber-criminal has *full* access to the files on the computer. Even if the hacker does not access or download sensitive information, the mere fact that the server was hacked could trigger client notification obligations under state laws, since it is not always possible to conclusively prove whether the cyber-criminal did indeed access or download the information.

While this activity seems to be targeting accounting firms, it is likely that any organization that handles sensitive client information will be targeted.

So how do you protect yourself?

Education, training and diligence. Partners and employees alike need to be educated about cybersecurity risks and trained to identify them. Everyone with a password into the system needs to think twice about the communications they receive, the sites they visit and the access they are willing to give third parties (*i.e.*, strangers) to their computers. If you receive an email that offers a branded product for free,

contact the named company before downloading or clicking on any links or attachments in the email. Use a telephone number from the official website (rather than from the email) to see if this is a legitimate offer. If it sounds too good to be true, it most likely is.

Wilson Elser's Data Privacy & Security practice is available to provide education and training to your organization and assistance in the event you are the victim of an attack.

Related Posts

What Attorneys Can Learn from History's Largest Data Breach

Negative Online Reviews: The Best Defense

The Proof Is in the Password!

Welcome to the Digital Age, Officer

Surf's Up: The Wave of High-profile Privacy Class Actions

Professional Liability Advocate

Tab B

WILSON ELSER

Professional Liability Advocate

The Proof Is in the Password!

By Geoffrey Belzer on May 4, 2016

POSTED IN CYBERSECURITY & DATA PRIVACY, PROFESSIONAL LIABILITY

Consider this scenario: A young couple entrusts you, an experienced real estate attorney, to assist them in the purchase of their first home. Days before closing, your unsecured email account gets hacked and your client receives an email, which to all appearances is from you, telling them to wire funds to a third-party account instead of bringing the cash to closing. You only find out about "your" email to your client after the transfer has been made and your clients' savings, accumulated over many years, is gone. What exactly do you think you can say to your clients to make it better?

This is not a fantasy – it happens far too often, as noted in a recent ***ABA Journal***

article. We, in fact, were involved on behalf of the depository bank in this exact situation in Illinois, where clients followed what they thought were the instructions of their attorney.

As a professional, you are required to keep abreast of changes in technology and to safeguard your client's confidential information under ***ABA Model Rules*** 1.1 and 1.6. This standard of care must be taken seriously and the idea that "it won't happen to me" is an insufficient defense. There are two immediate steps you can and should take to help prevent a foreseeable loss.

First, pick a "secure" password. You are putting yourself and your clients at risk if any of your passwords are like those on a ***GeekWire*** list. Second, if you have not enabled the security features on your mobile phone – even after all the media coverage of the federal government's attempt to compel Apple to tell it how to unlock data on an iPhone – do so immediately.

The need to understand technology and enable a strong password to protect accounts is not limited to professionals. Consider the recent case of ***Laremy Tunsil*** , an NFL prospect who arguably lost more than $13 million because someone hacked his Twitter and Instagram accounts at the worst possible time, resulting in his precipitous drop in the NFL draft.

In our case, the attorney was able to avoid liability by spending a considerable amount of time chasing down his clients' funds, which were traced to the hacker's account and recovered. However, this only occurred after the attorney put his insurer on notice of a potential claim and six months of litigation.

Takeaway

Have you spent the time to think about whether you and your clients are up to date on the latest technology and know how to keep that technology secure? Have you spent the time and effort to fully safeguard your client's confidential information on your computers? If you engage in social media, have you considered the implications of the strength or weakness of your password? The importance of thinking this issue

through now – before a problem occurs – cannot be over-emphasized. Your electronic communications must be kept secure. If necessary, hire a consultant or adviser. The cost of preventing a data breach is money well spent.

We ask our readers to join in if they have questions or have dealt with this issue in the past.

Related Posts

What Attorneys Can Learn from History's Largest Data Breach

Negative Online Reviews: The Best Defense

Rise in Cyberattacks on Professional Services Firms

Welcome to the Digital Age, Officer

Surf's Up: The Wave of High-profile Privacy Class Actions

Professional Liability Advocate

Tab C

WILSON ELSER

Professional Liability Advocate

What Attorneys Can Learn from History's Largest Data Breach

By William F. McDevitt on June 21, 2016

POSTED IN ATTORNEYS, CYBERSECURITY & DATA PRIVACY, PROFESSIONAL LIABILITY

On April 3, 2016, the public learned that millions of client documents from the Panamanian law firm and corporate services provider Mossack Fonseca & Co. (MF) had made their way to an international organization, the International Consortium of Investigative Journalists (ICIJ), and that the information would be used to publish potentially damaging stories. In addition, authorities across the globe, from Japan to Switzerland to the United States, are reviewing the documents and investigating potential tax implications, regulatory violations and criminal activity.

Background

It is estimated that since its inception in 1977, MF has incorporated 250,000 businesses, largely in offshore jurisdictions. MF serves a wide range of clients, including politicians, celebrities and corporations. Incorporating "anonymous" businesses is entirely legal. There is, however, a stigma attached to "shell companies," and several of the public figures associated with these businesses have already been embarrassed by exposé-style articles. The ICIJ has promised that additional, highly compromising articles will be published.

Following the disclosure of the breach, MF stated that it experienced an "e-mail server breach" at one if its data centers. It also has been reported that the documents were removed over the course of a year, beginning in early 2015. This followed a 2014 "whistleblower" data breach involving MF's activities in Germany.

The details of how MF's client data was removed, who removed it and why are not known and may never be made public. Regardless, the breach raises important questions that are relevant to any lawyer who uses a computer to create, store and access attorney-client materials:

- After a whistleblower distributed client materials to the German government in 2014, what additional safeguards were implemented to protect client files? Does your firm regularly review security procedures? What process does your firm implement when computers, phones or remote storage devices are lost, stolen or decommissioned? What process does your firm follow if a data breach or virus is discovered in your system?
- How long should client files remain on accessible servers? More than 11.5 million MF documents dating from 1977 forward were exposed by an "e-mail server breach." Many of these documents surely predated MF's current computer system. For whatever reason, "historical" documents were stored on the same servers that handled routine e-mail functions. What is your firm's protocol for retaining "historical" documents on "active" servers?

- Were notifications issued when non-active files were accessed? MF apparently had a policy of assuring that all documents for the 250,000 companies that it formed were readily available. But did the "primary" attorney on those files receive any type of notification when materials from their assigned clients were accessed? Did the system administrator receive notification when older files that had not been accessed for a significant period were suddenly downloaded? Does your firm have electronic notifications in place when files are accessed? Are sensitive files restricted to certain users? Are your files password protected?
- News articles indicate that the breach was publicly disclosed only because a journalist contacted a representative of the Russian government who raised the possibility of a data breach with MF on March 28, 2016. MF notified their clients on April 1, 2016. ICIJ then issued a press release about the breach on April 3, 2016. The data breach(es) likely occurred over the course of several months, starting in 2015. When should the breach(es) have been discovered and disclosed to MF's clients? Does your firm regularly monitor its access logs? Does your firm have a data breach response plan? Has your firm prepared a letter to advise a client of a discovered breach? Has your firm prepared a press release if a wider disclosure is necessary?

Lessons Learned

The MF data breach represents a sea change in the management of client data by law firms. The bar for safeguarding client data has risen. All attorneys must now consider the potential pitfalls of maintaining "historical" data on their servers, the implementation of notifications when files are accessed and protocols for issuing client disclosures when files are accessed. It is likely that MF will face considerable litigation over the undocumented data breach. Attorneys seeking to avoid litigation need to learn from MF's failure and ensure that their data is protected.

Related Posts

Negative Online Reviews: The Best Defense

The Proof Is in the Password!

Rise in Cyberattacks on Professional Services Firms

Welcome to the Digital Age, Officer

Surf's Up: The Wave of High-profile Privacy Class Actions

Professional Liability Advocate

Tab D

Victims of Social Engineering Fraud: A Trend You Do *Not* Want to Follow

By, Scott R. Schaffer, Esq. and Antonella G. Dessi, Esq. – October 2016

The emergence of a worrisome trend involving email hacking is plaguing law firms that find themselves involved with wire transfers of client funds. Primarily, these schemes tend to target real estate attorneys, although we have seen sporadic application of these frauds in other practice areas. Typically, the email hacking is carried out at or about the time of a real estate closing and almost always involves the transmission of fraudulent wire transfer information to the law firm. This causes the firm to unknowingly wire transfer monies into a bank account that can be accessed by the hacker. More often than not, the funds are unrecoverable, as the hacker withdraws the money before the fraud is detected. As the true intended recipient of the funds never receives the money, these "social engineering" schemes, as they are known, open the law firm up to claims from clients, banks and various other parties. The following real-life scenarios convey some important lessons from attorneys who have fallen victim to social engineering fraud.

Scenario 1

Law Firm represented Client, a seller, at a real estate closing. In fact, Law Firm had represented Client on numerous occasions in similar engagements. Client was to receive a wire transaction of $100,000, representing the sale proceeds. Unbeknownst to Law Firm, however, its paralegal's email was hacked prior to closing and the hacker sent a series of emails, purporting to be from Client, instructing Law Firm to wire funds to an account at Bank. Law Firm wired the sale proceeds to the account provided in the emails, only to learn later that the instructions were fraudulent. The fraud was discovered after Client called Law Firm to inquire about the funds, which had not been received. Client demanded the amount of the wire transaction, plus additional funds to compensate Client for the costs of taking out a loan to keep his business running. It remains unknown whether Bank will be able to recover any of the funds wired to the fraudulent account.

While Law Firm was a victim of social engineering fraud, the erroneous transfer might have been avoided. The fraudulent emails were sent by a "dummy" account that was created to look almost identical to Client's real email account. The emails purportedly sent from Client, whose email display name would typically appear as "john doe [doej5000@gmail.com]," appeared as "john doe [doej5000@mail.com]." With only the "g" from the "gmail" account omitted from the address, the email name change was easily

overlooked by Law Firm. As a takeaway, lawyers should meticulously review emails containing sensitive information such as wire transfer instructions and bank account numbers to ensure that they were sent by the appropriate party. In today's age of electronic communication, a simple telephone call to Client for confirmation purposes would have immediately alerted Law Firm to the fraudulent nature of the emails and the wire transfer of funds to the improper bank account would have been avoided.

Scenario 2

In another matter involving a real estate transaction, Law Firm represented Client, a seller, at a closing. Client was to receive the sale proceeds of $200,000 via wire transfer to her account with Bank. To this end, Client provided Law Firm with a voided check from her bank account containing the appropriate routing and account numbers. Prior to the wire transfer, however, Law Firm received an email, purportedly from Client's real estate agent, indicating that Client wanted the funds wired to another account due to technical issues. Following the wire transfer, it was discovered that the email was a fraudulent result of a breach of the real estate agent's email systems. Client demanded the sale proceeds from Law Firm.

Here, too, certain preventative measures could have been taken to avoid the fraudulent transfer. The email purporting to be from Client's real estate agent contained the following language: "Due to tech issues with the seller's account seller wants proceeds wired to her personal company's account pleeze send me the info you need to initiate the wire." In this instance, noting the improper grammar and spelling, Law Firm might have paused before proceeding with the wire transfer. In this regard, attorneys should always be suspicious of unsophisticated language in emails, particularly when there are prior communications from the alleged sender that can be used as a reference. As a general rule, a change in wiring instructions to a different account should always raise red flags and, again, a telephone call should be made for verbal confirmation.

Scenario 3

Law Firm represented Client in connection with a stock purchase agreement for the sale of Client's business. As part of the sale, $1 million was transferred to an escrow account with Bank and was to be released on a certain date once specific conditions were met. Buyer was to pay an additional $200,000 if various other conditions were met. The required conditions were met, and Buyer became obligated to transfer funds totaling $1.2 million to Client. Seller provided Law Firm with wiring instructions via email

and Law Firm was to provide the wiring instructions to Bank and Buyer. Before this could be accomplished, however, Law Firm's email was intercepted by a fraudulent third party. Different wiring instructions were provided to Bank and Buyer via phony email purporting to be from Law Firm. As a result, Bank and Buyer transferred funds to the incorrect bank account.

In this scenario, various other emails exchanged among the parties were also intercepted, such that it is unclear which party's email system was breached. This example demonstrates the incredible sophistication of some of these schemes. Attorneys should be extra cautious when emails containing sensitive information are exchanged among multiple parties, as this creates more opportunities for a security breach. Once again, the simple extra step of reaching out to all involved parties by telephone for verbal confirmation of the wiring instructions would have gone a long way toward preventing fraud.

Scenario 4

Law Firm represented Client in connection with the purchase of real estate for $250,000. At closing, Law Firm provided a $250,000 check from its escrow account to Seller's counsel. On the same date, Law Firm received two emails, purportedly from Seller's counsel, requesting that Law Firm instead transfer the proceeds into Seller's counsel's trust account. A few days later, Law Firm received a follow-up email, again purportedly from Seller's counsel, indicating that counsel had destroyed the $250,000 check and wanted the proceeds wired to Bank that day. On the same date, and without confirming that the check had, in fact, been voided, Law Firm's paralegal wired the $250,000 sale proceeds to Bank. Several days later, Bank's fraud risk manager advised Law Firm that the wire transfer was part of an email hacking fraud. Law Firm then discovered that the check provided at closing had not been voided but was actually cashed by Seller's counsel. While this particular social engineering fraud did not result in a loss to a third party, the wire transfer from Law Firm's attorney-client trust account caused a recognizable, albeit unrealized, loss to one or more of Law Firm's other clients that had funds in the trust account at the time.

There are several valuable lessons to be learned here as well. This scenario again demonstrates the importance of being wary of a sudden change in instructions, and the need to follow up with verbal confirmation. Here, there was no confirmation directly with Seller's counsel regarding the change in instructions or verification that the previously issued check had been voided. Although it would appear to go without saying, attorneys should carefully oversee the actions of their paralegals, assistants and staff particularly where client monies are concerned.

Conclusion

These scenarios are actual examples of the recent and growing trend of social engineering fraud that is victimizing law firms. By following the simple recommendations, law firms may be able to avoid exposure and protect client relationships from risk.

Tab E

Social Engineering Fraud: An Update

By, Scott R. Schaffer, Esq. and Antonella G. Dessi, Esq. – November 2016

There continues to be a troubling trend involving email hacking surrounding law firms that handle wire transfers of client funds. While these social engineering schemes typically target firms involved in real estate transactions, where wire transfers often occur on a daily basis, any firms that utilize wire transfers in their practice are vulnerable. This article will provide an update as to the different types of schemes that we have encountered so that lawyers can be on the lookout for any suspicious behavior and take the necessary precautions to guard against such fraud.

Scenario 1

Law Firm represented Client, a seller, at a real estate closing. Client was to receive a wire transaction of over $900,000, representing the sale proceeds. Unbeknownst to Law Firm, however, an email account was hacked prior to closing and the hacker sent a series of emails, purportedly from Client, instructing Law Firm that a fax would be sent with wiring instructions to wire funds to three separate accounts at three different banks. It is unknown whether the hacker targeted Law Firm's email systems or one of the other parties involved in the transaction. In any event, Law Firm wired the sale proceeds to the accounts provided in the fax, only to later learn that the instructions were fraudulent. The fraud was discovered after Client inquired about the funds, which had not been received. Fortunately, one of the three recipient banks was able to fully recover the wired funds before the fraudulent party was able to withdraw them. Client demanded the balance of the missing funds and, while the other two recipient banks were able to recover some of the wired funds, it remains unknown whether full recovery will ultimately be made.

In this instance, the fraud would likely have been avoided had the Insured taken just a few simple extra steps. As we have seen on numerous occasions, the fraudulent emails were sent by an email account that was designed to look almost identical to Client's actual email account. As such, the email account name change was easily overlooked by Law Firm, as the emails purportedly sent from Client simply inserted an additional letter into the account name. As a takeaway, lawyers should always carefully review emails containing wire transfer instructions to ensure that they were sent by the appropriate party. The Insured should also have taken notice that the grammar and language used in the hacker's email were not as sophisticated as that used in Client's prior emails to Law Firm. Furthermore, in today's age of electronic communication, a simple telephone call to Client for confirmation purposes would have immediately

alerted Law Firm to the fraudulent nature of the emails and the wire transfer of funds to the improper recipient bank accounts would have been avoided.

Scenario 2

In another matter involving a real estate transaction, Law Firm represented Clients, the buyers. Clients decided to back out of their purchase of real property. Law Firm sent a letter to the seller's attorney requesting the return of Clients' $9,000 deposit. When Law Firm did not receive the funds, it called the seller's attorney, who advised that the funds had been wired to Law Firm's bank account. However, Law Firm had not requested that the funds be wired to this particular account. Law Firm later learned that seller's attorney received a second mailed letter purportedly from Law Firm requesting that the funds be wired to a fraudulent account. Seller's attorney completed the transfer and the funds were withdrawn. Although the letter used Law Firm's name and address, it was easily distinguishable from Law Firm's normal letterhead, which had previously been provided to the seller's attorney. Additionally, an IT company retained to review Law Firm's email system found no evidence that the Insured's email system had been hacked. The seller's attorney ultimately reimbursed the full $9,000 and is pursuing the involved banks for reimbursement.

Here, while the Insured Law Firm was not ultimately liable for the loss, there are some important lessons to be learned from the seller's attorney. First, it is worth noting that despite the recent rise in electronic fraud, some criminals still use other methods of perpetuating fraud on unsuspecting attorneys, in this case the U.S. mail. As such, lawyers should be just as wary of hard copy communications as they are of emails. Second, as with Scenario 1, there were certain discrepancies with the letterhead that the seller's attorney could have recognized. And, once again, a telephone call to Law Firm to confirm the instructions would have immediately alerted the parties to the fraud.

Scenario 3

Law Firm represented Clients in connection with a stock purchase agreement for the sale of Clients' business. As part of the sale, $1.3 million was transferred to an escrow account with Bank and was to be subsequently transferred to Clients. Clients emailed wiring instructions to Law Firm, which were to be forwarded to the Bank and the Buyer. At some point, however, an imposter created fraudulent e-mail addresses that varied by one number or letter from the legitimate e-mail addresses of Clients and the contact person for the Buyer. At the imposter's instruction, both the Bank and the Buyer wired Clients'

money to an entity not mentioned in the escrow instructions and to a bank not previously used by Clients. Clients alleged that the imposter hacked into the e-mails of Law Firm and was able to ascertain sensitive banking information due to Law Firm's use of an unencrypted internet portal. While approximately $500,000 was recovered by the FBI, Clients alleged damages of nearly $700,000, constituting the sum of the transferred funds which were not recovered, plus interest, costs, and attorney fees.

As the case proceeded through litigation, a California court granted Law Firm's motion for summary judgment. In a favorable turn of events, Law Firm was successfully able to argue that it did not have a legal duty to provide the type of internet security Clients alleged the Insured breached by failing to provide. Specifically, it was successfully argued that there can be no liability for failure to act if there is no duty to act. The motion was premised upon four arguments: (1) Law Firm, as an internet user, had no duty to provide security to prevent someone from misusing its email; (2) even if Law Firm, as counsel for Clients, had a duty to provide a reasonably secure internet portal for transmission of e-mails, Law Firm complied with any such duty in accordance with the skill, prudence and diligence commonly possessed by members of the legal profession and thus there was no actionable legal malpractice; (3) assuming, *arguendo*, Law Firm's e-mail system permitted a hacker to obtain Clients' sensitive information, such act on the part of Law Firm does not constitute a breach of fiduciary duty; and (4) Clients did not possess, and could not obtain, any evidence that it was any actual e-mail or system failure of Law Firm that permitted the imposter to gain Clients' sensitive information, and without causation, there is no liability on any cause of action alleged.

Despite the favorable court ruling, this example demonstrates how lawyers should be extra cautious when exchanging emails among multiple parties, as this creates even more opportunities for a security breach. Furthermore, it is recommended that attorneys always ensure that their email and internet systems are secure so as to protect against security breaches. Finally, as is almost always the case in these examples, the simple step of verbally confirming the wiring instructions would have gone a long way toward preventing fraud.

Conclusion

These scenarios are real examples of the recent and growing trend of social engineering fraud that is plaguing law firms. By following the simple recommendations above, attorneys may be able to avoid exposure to fraud and protect client relationships from risk of any breach.

Tab F

Continuing Legal Education

Introduction to Legal Project Management & Process Improvement

Speaker: C. Peter Hitson (WP)

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

LEAN Process Improvement

LEAN is grounded in understanding client needs.

Process Improvement focuses on a number of areas of opportunity, such as:

- Fully utilize people talent. Match the needs of each assignment with the right staffing. Train attorneys and paralegals to be able to use the full extent of their skill and knowledge.

- Reduce Errors, Mistakes & Rework. It is more efficient to do something right the first time. Improve delegation and guidance for others on a team.

- Perform work at the right time. Reduce work that is performed before it is needed.

- Reduce waiting time and bottlenecks.

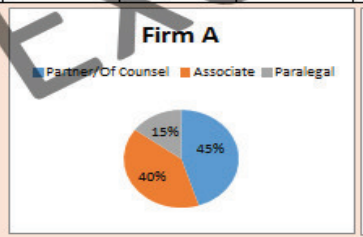
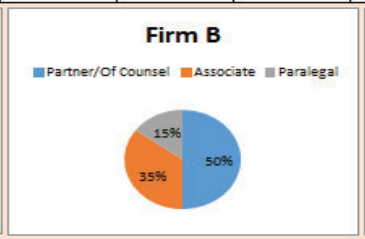
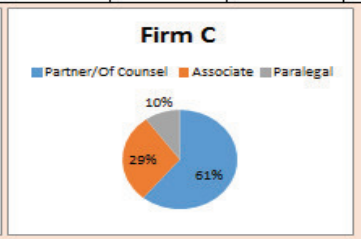
- Avoid overproduction: Creating more than is necessary or before it is needed; sending information automatically if not required; printing before necessary, etc..

- Reduce inventory of materials and information that are not needed.

- Reduce excess movement of files, documents or people. Reduce time looking for information or documents.

WILSON ELSER

Law Firm Evaluation – Scorecard Sample

SAMPLE FINANCIAL SCORECARD		Current Year to Date				Prior Year to Date				Prior Year			
		Law Firm A	Law Firm B	Law Firm C	Total	Law Firm A	Law Firm B	Law Firm C	Total	Law Firm A	Law Firm B	Law Firm C	Total
Inventory & Assignments	Total Cases	50	30	16	96	50	28	17	95	50	35	18	10
	New Assignments	2	12	6	20	5	8	5	18	20	22	12	5
	Closed Cases	2	10	7	19	5	15	6	26	25	23	11	5
	Open/Closed Ratio	1.0	1.2	0.9	1.1	1.0	0.5	0.8	0.7	0.8	1.0	1.1	0.
	$0 - $50,000 Reserve	8	12	2	22	7	8	1	16	15	15	1	3
	$50,000- $100,000 Reserve	27	8	3	38	24	3	2	29	30	12	4	4
	$100,000 - $250,000 Reserve	11	3	10	24	15	12	10	37	2	2	6	1
	$250,000+ Reserve	4	7	1	12	4	5	4	13	3	6	7	1
	$0 - $50,000 Reserve	16.0%	40.0%	12.5%	22.9%	14.0%	28.6%	5.9%	16.8%	30.0%	42.9%	5.6%	30.1
	$50,000- $100,000 Reserve	54.0%	26.7%	18.8%	39.6%	48.0%	10.7%	11.8%	30.5%	60.0%	34.3%	22.2%	44.7
	$100,000 - $250,000 Reserve	22.0%	10.0%	62.5%	25.0%	30.0%	42.9%	58.8%	38.9%	4.0%	5.7%	33.3%	9.7
	$250,000+ Reserve	8.0%	23.3%	6.3%	12.5%	8.0%	17.9%	23.5%	13.7%	6.0%	17.1%	38.9%	15.5
Aging	Open Cases - Average Age (Days)	260	310	318	314	270	301	325	320	305	310	318	31
	Closed Cases - Average Days to close	235	323	345	330	245	330	317	315	350	323	345	33
Fees & Expenses	Fees Billed - All Cases	$100,123	$128,591	$75,238	$303,952	$99,642	$134,896	$80,321	$314,859	$185,459	$165,830	$104,591	$455,88
	Expenses Billed - All Cases	$9,856	$8,506	$8,750	$27,112	$8,500	$9,201	$5,900	$23,601	$12,896	$16,345	$9,745	$38,98
	Total Billed - All Cases	$109,979	$137,097	$83,988	$331,064	$108,142	$144,097	$86,221	$338,460	$198,355	$182,175	$114,336	$494,86
	Fee/Expense Ratio	91.0%	93.8%	89.6%	91.8%	92.1%	93.6%	93.2%	93.0%	93.5%	91.0%	91.5%	92.1
	Fees/Closed Case	$7,500	$12,857	$18,435	$13,281	$8,203	$13,567	$27,982	$15,678	$12,897	$13,459	$24,596	$15,39
	Expenses/Closed Case	$1,250	$977	$1,854	$1,045	$1,450	$1,055	$2,500	$1,560	$1,357	$1,045	$2,138	$1,53
	Total Legal Expense/Closed Case	$8,750	$13,834	$20,289	$14,326	$9,653	$14,622	$30,482	$17,238	$14,254	$14,504	$26,734	$16,92
Billing Accuracy	Invoice Audit Rate	3.5%	4.5%	4.3%	4.1%	5.2%	5.1%	7.5%	5.5%	5.5%	6.7%	6.2%	6.0
	Invoice Audit Total	$3,849	$6,169	$3,611	$13,574	$5,623	$7,349	$6,467	$18,615	$10,910	$12,206	$7,089	$29,69
Hours	Total Hours (Billed)	646	691	355	1652	656	725	402	1740	1212	892	510	253
	Average Hours/Open Case	35	50	53	52	37	53	60	48	35	51	53	4
	Average Hours/Closed Case	48	69	87	72	54	73	140	87	84	72	120	8
Distribution of Work	Partner/Of Counsel	45.0%	50.0%	61.0%	49.0%	46.0%	55.0%	70.0%	55.0%	47.0%	54.0%	55.0%	51.0
	Associate	40.0%	35.0%	29.0%	36.0%	39.0%	35.0%	27.0%	35.0%	39.0%	35.0%	27.0%	35.0
	Paralegal	15.0%	15.0%	10.0%	15.0%	15.0%	10.0%	3.0%	10.0%	15.0%	10.0%	3.0%	10.0
Quick Comparison of Distribution of Current Work:													
Task Code Distribution	Case Assessment & Development	28.2%	36.7%	40.1%	35.2%	29.3%	34.2%	38.9%	35.0%	29.3%	34.2%	38.9%	33.3
	Pleadings & Motions	29.0%	13.1%	21.0%	22.5%	29.0%	15.0%	12.6%	22.5%	29.0%	15.8%	12.0%	18.4
	Discovery	34.0%	35.0%	29.5%	32.0%	32.0%	32.0%	32.0%	26.0%	32.0%	32.0%	32.6%	32.0
	Trial & Hearings (Prep/Attend)	8.5%	12.0%	9.4%	9.5%	9.0%	10.0%	9.0%	9.5%	9.0%	10.0%	10.0%	9.3
	Appeals	0.3%	1.2%	0.0%	0.8%	0.7%	8.8%	7.5%	7.0%	0.7%	8.0%	6.5%	7.0
	Total	100.0%	98.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0
Rates	Average Timekeeper Rate	$155	$186	$212	$184	$152	$186	$200	$181	$153	$186	$205	$18
	Increase vs. Prior Year	1.3%	0.0%	3.4%	2.2%								

Legal Project Management - Stakeholder Analysis

Stakeholders include all people who are either affected by or who can affect the outcome and handling of the legal matter (positively or negatively). This analysis should be ongoing, as people and roles can change.

Stakeholder analysis facilitates setting expectations, success factors, timeline, budgets, risks and a communication plan.

Consider, by example, people who may:

- ✓ Provide initial and ongoing information and documents you need;
- ✓ Receive reports, copies of letters, and other communication;
- ✓ Determine settlement authority;
- ✓ Authorize strategic decisions like trial, experts or key motions;
- ✓ Approve budgets;
- ✓ Pay legal bills or other costs; or
- ✓ Define "success" for the outcome and handling.

Save this template in the electronic file to provide information to the handling team and to track changes and additional stakeholders.

Case Name:
Wilson Elser File Number:
Client Claim Number:
Date Created/Updated:
Person Completing/Updating this Analysis:

Stakeholder Identification

Role	Name	Comments
Individual Client(s)		
Business Client contacts		
Client employees		
Client personal attorney or in-house counsel		
Others related to client		
Referral Source		

Role	Name	Comments
Claim Handler		
Claim Manager(s)/Management		
Claim Executives		
Carrier in-house counsel		
Bill audit team or third party audit service		
Agent/Broker		
Plaintiff attorney/opposing counsel		
Other lawyers		
Judge		
Other		

Questions for Stakeholders:

- ✓ What is your goal or objective?
- ✓ What are you trying to avoid?
- ✓ What would be a good result? (Do others in your organization agree?)
- ✓ How can we understand your business better?
- ✓ Are there parts of the investigation or handling that you want to take on or help?
- ✓ If we've worked together before, what do you hope we do better or differently?
- ✓ Who will be involved in making decisions about this case?
- ✓ Do you have an expectation of the defense cost?
- ✓ How long do you think this case will take to resolve?
- ✓ What is the best way to communicate with you?

Legal Project Management Planning & Scoping Considerations

Setting Expectations & Lines of Communication

- ☐ What is the client's expectation for outcome or result?
- ☐ From our experience, what is the best outcome or result?
- ☐ Communication preferences/methods (who/how/when)
- ☐ Who are the people who need information or who will participate in decisions?
- ☐ How do client guidelines influence our handling?

Focus on Resolution

- ☐ What are the key issues that need to be resolved by this litigation?
- ☐ Will this case like by settled?
    - What would prevent a settlement?
- ☐ At what stage of litigation do matters of this type typically resolve?
- ☐ What factors make this case unique when compared to similar matters that we have handled?
    - How will those unique factors influence how we handle this case?
- ☐ When will this matter likely be resolved?
- ☐ Are there related issues that are out of scope of our representation?
- ☐ What could cause our plans to change?
    - How will we address changes?

Controlling Staffing & Hours

- ☐ What work will we need to do to handle this case?
    - Big picture – Phases or Stages of litigation
    - Specific activities or documents
- ☐ What is the right team for this matter?
    - What specific roles will the team members have?
    - What specific tasks will the team members perform?
    - Are there external resources (local counsel, experts, vendors, etc.) that will be part of the team?
- ☐ What prior experience and work can be reused?

Managing Timeliness

- ☐ When does our client expect us to provide a comprehensive evaluation?
    - What do we need to do to provide that evaluation on time?
- ☐ Are there existing or expected deadlines?
- ☐ What is the best way for our team to coordinate so that tasks are started and finished on time?

Case Staffing and Timeline

Staff Members	Tasks	Start Date	End Date/Deadline

- ☐ Internal Expenses: _____
- ☐ External Expenses: _____

Tab G

ALIGN

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

ALIGN

Clients select Wilson Elser for more than the breadth of our substantive legal knowledge and trial experience. We are collaborative business partners who recognize efficiency, predictability and consistency as key contributors to legal service delivery on their business goals.

Wilson Elser ALIGN is our sustained initiative to maximize value to clients through innovative legal processes, including Legal Project Management and Legal Process Improvement. It's the way we practice our profession, and it's the way we deliver on our core values.

ALIGN drives results and service. We work with our clients to focus on outcome objectives and then collaborate to define the right strategy, staffing and actions to efficiently deliver best outcomes.

Legal Project Management is our systematic approach to scoping, planning and managing legal work. From single cases to national portfolios, from routine to highly complex assignments, we work closely with our clients to match resources and activities to the desired results. This approach supports predictability in terms of how the assignment is handled, the cost and the time frame to resolution.

Legal Process Improvement embraces business disciplines of Lean Six Sigma within a culture of continuous improvement. We listen to our clients. Their "voice" guides initiatives targeted at delivering service with lower cost and cycle time. We also recognize the power of our national team and develop consistent approaches that are linked to best outcomes, because sharing information allows us to replicate strategies and approaches that have already proved their value.

WILSON ELSER ALIGN

ALIGN IN ACTION

ALIGN at the Case Level

Legal Project Management's application is most obvious at the individual case level.

- **Scoping:** Early discussions with the client are focused on confirming goals and objectives and ensuring there is an effective communication plan factoring in all the stakeholders.
- **Planning:** Strategic planning identifies not only key activities but also the staffing, timetable and projected expense. We express plans in financial terms – a budget. As an adjunct to the planning process, we consider potential risks that might impact strategy, timing or expenses.
- **Execution:** Cases are managed to plan and budget. Changes are addressed proactively.
- **Matter closure:** We welcome and solicit feedback that can inform future work.

ALIGN at the Client Program Level

Many clients depend on Wilson Elser to handle a portfolio of cases.

- **Managing to client metrics:** Acknowledging that clients are interested in more than data, we detect trends before they become performance issues and encourage behaviors that positively influence key metrics.
- **Developing program-level staffing models:** We combine best practices, key metrics and likely interactions in designing effective staffing models that align with distinct matter types.
- **Employing process-improvement techniques:** We use data and experience to create a superior new process or improve on an existing process.
- **Managing project benchmarks:** Recognizing that even the best project plans can go awry, we continually evaluate progress against benchmarks to help ensure completion on time and on budget.
- **Supporting alternative fee arrangements:** Many pricing options are available that can be customized to the needs of individual clients.

ALIGN at the Firm Level

Innovative approaches to legal service delivery and ensuring consistency of our customer's service experience is supported by Legal Process Improvement.

- **Process mapping:** By mapping distinct parts of a process, we better manage resources, reduce costs and optimize benefits.
- **Best practices:** We identify and migrate practices that consistently produce good outcomes.
- **Leveraging the firm's experience:** When it best serves our clients' objectives, we draw on relevant experience and skill sets throughout Wilson Elser's extensive office network.