# Everything You Need to Know About Communicating With Your Clients Via Text: The Good and the Bad

Robert Joyner October 20, 2020

Do you want to hear some scary facts? In 2014, 500 million Yahoo users were compromised. In 2016, 57 million Uber customer accounts and profiles were breached, and in 2017, 143 million social security numbers were stolen from Equifax. Breaches to this scale may not happen every day, but smaller ones do. And as the prevalence of cyber threats grow, smaller companies are now being targeted at a much higher rate.

Between January 2015 and December 2016, there was an approximate 2,370% increase in identified exposed losses. Email scans were reported in all 50 states and from 2013-2016, the Internet Crime Complaint Center reported exposed losses of more than $2 billion. As privacy concerns continue to grow, governments are now instituting laws that require companies to report every incident of hacking and data breach.

Let's take a look at the threats your firm faces, the obligations you have with your clients when you communicate through text, and how to protect yourself while you communicate in today's day and age.

## Threats Firms Face

According to a Legal Technology Survey Report that the American Bar Association released in 2016, more than one-quarter of firms with more than 500 lawyers admitted they experienced some type of breach. Approximately 40% of those firms reported significant resulting business downtime and loss of billable hours. 25% recounted hefty fees to correct the problems and one in six reported loss of important files and information.

Today, 25% of all law firms have been subjected to, or experienced, some form of a data breach involving hackers. Computer-oriented crimes span a wide variety of actions, intentions, and

goals, and no company is too large or too small to be affected by a cyberattack.

So why are firms being targeted? Lawyer's handle very sensitive information for their clients, intellectual property, financial information, and legal strategies, all of which are incredibly valuable for malicious third parties.

As this continues to become a problem, rules that govern the legal industry are changing. Let's dig deeper.

## Types of Threats

What are some of the challenges that law firms face?

1. **Ransomware**: It is exactly what it sounds like. An attacker will infect a computer or network with malicious software that encrypts data and hold it for ransom. The files held by the attacker cannot be destroyed without a mathematical key that only the attacker has. In these cases, it is a heft financial payment is made in exchange for the information. And this goes without saying, but if you do not have access to your work or matter files, you can't function as a firm. The average cost of a ransomware attack on a business is $133,000. The cost of ransomware attacks surpassed $7.5 billion in 2019, according to Emsisoft.
2. **Phishing:** The second threat is called phishing. This attack is classified by hackers contacting an attorney via phone or email and posing as specific individuals to trick them into sharing confidential or sensitive information. In some cases, attorney's will even be convinced to give out unauthorized access to networks.
3. **Malware:** Malicious 3rd party software that is installed to gain unauthorized access to or otherwise damage a network. This malware is installed via a hacked wifi connection, a hard drive, or a link in an email that is opened. This type of attack results in a heavy financial burden to restore or repair the network.

Unfortunately, even with the advancements in firewalls and encryptions that we see today, people are the largest weakness in a firm's security network. Whether it's due to failure to follow protocols or insufficient training, social engineering hacking is on a rise.

## Communicating With Your Clients

### Texting

The rise of texting is undisputed. It is our primary means of communication. 81% of Americans are sending and receiving texts, with 27 trillion texts being sent every year. According to Nielsen, on average, Americans text twice as much as they call and for Americans under the age of 50, sending and receiving text messages is the most prevalent form of communication. The need and ability to send and receive communication instantly is a primary reason for the rise of this communication method. I'm sure you're familiar with this; people want what they want and they want it now, no questions asked. Today, if it takes longer than thirty minutes to respond to a text (and even that's generous!), some eyebrows will inevitably be raised. As this trend has evolved, advanced, and continued its way throughout the 21st century, the legal field has slowly started to capitalize on the advantages of the fast and easy communication style too.

There are three compelling reasons why lawyers turn to texting their clients as a dominant means of communication.

1. **Ease:** Most clients are already texting, so they don't have to go to their email, sift through a list

of ads, open the message, read it and then respond and they don't have to listen to missed voicemails. Texting makes it easy for lawyers to communicate with their clients and for clients to provide their legal team with the information they need quickly. Today, technology is so advanced that there is software that will even allow you to bill for the time texting, whether it's inbound or outbound.

2. **Efficiency:** It doesn't matter where the client or attorney is, a text message can be sent instantly and from anywhere. This not only increases communication with your clients, but it also allows you to bill for more time. Not to mention a huge benefit to texting is the conversation trail it leaves behind. Unless purposefully deleted, a client-attorney conversation can be saved forever.
3. **Effective:** It is in real-time, you can scroll back up through past messages and you have a frame of reference for where you last left off.

And if all of that isn't enough to compel you, how about the fact that 78% of people wish they could have a text conversation with a business. You don't have to be good at math to know that's a lot of people.

Of course, with all this being said, there are downsides to communicating in this modern and rapid way; those being ethical obligations, confidentiality concerns, over accessibility, record preservation, and simplicity. As the legal field continues to evolve, and texting becomes more and more commonplace, there is a framework of rules that all lawyers should abide by as they continue to utilize this form of communication. Doing so, will not only enhance your customer experience but will also protect everyone from malicious third-party threats.

## Framework for Communicating Via Text

### Duty of Competence

As a lawyer, you have a duty of competence that you must provide to your clients. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

### Duty of Confidentiality

Back in the 90s, when email came onto the scene, the ABA said that lawyers had a reasonable expectation of privacy in communications made by all forms of email, but they also included that the encryption of emails sent over the internet was unnecessary, despite some risk of interception and disclosure. So twenty-some years ago, you didn't have to worry about

protecting your communications. But in 2020, with the rise of breaches and personal information being exposed, the ABA adjusted its statement to include that 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. Today, it is a lawyer's duty to keep abreast of the knowledge and changes in the law and its practice, including the benefits and risks associated with relevant technology. Now, all lawyers are required to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and inadvertent disclosure of information.

## Protecting Your Client's Communications

The first thing every law firm and lawyer must be able to do is to understand the nature of the threat. Being able to identify what kind of threat is being imposed will help you determine how you should communicate with your staff about combating it.

Not only should you be able to understand the potential threats, but you should also have an understanding of how your confidential information is being stored and transmitted. How does your firm store information? Are you cloud-based or on a physical hard drive?

Next, you must know how to use reasonable security measures to protect what you're communicating with your clients. This means you also need to determine how your electronic communications and client matter is being protected. It goes further than your IT department making a unilateral decision, it's your responsibility to make the decision to protect your clients.

Lastly, firms must train their lawyers and staff in technology and information security and conduct due diligence on vendors providing communication technology. This includes how vendors process and handle your data, whether or not it complies with your ethical obligation, vendor conflict check, and understanding how they do business. Additionally, it is important to note whether or not these vendors are storing your information overseas, what jurisdiction they have over that data, and in the event of a breach, what are the steps to mitigate or resolve the hack?

## Reasonable Efforts Standards

The factors to be considered in determining the reasonableness of lawyers efforts include:

- The sensitivity of information- Are you discussing meeting dates and times or attorney-client privilege information? If the latter, that needs to be protected.
- The likelihood of disclosure if additional safeguards are not used- This means the potential threat of your network or data being breached. Based on the data, the threat is much higher now than it was in the 90s.
- The cost of employing the additional safeguards- How expensive is it to put in the systems to protect your communications and data.
- The difficulty of implementing the safeguards.
- The extent to which the safeguards adversely affect your clients- Are your clients able to navigate the additional safety measures? Do they hinder your bi-directional communication?

As you move forward and continue to grow your firm and expand your client list, it is best practice to speak with your clients and discuss their expectations for communication. What suits them best? Are they comfortable with communicating back and forth via text and are they aware of the security risks and threats in today's day and age?

## Is Texting Ethical?

Simple answer, yes. You may send texts to and receive texts from clients. There are no statutes prohibiting this, however, there are regulations around data security and confidentiality as mentioned above.

If you're trying to solicit new clients via text there are some standards you must follow. For example, the first line of your text must say that what you're sending is an advertisement. You must track who received the texts and what content they are specifically receiving. You must ensure that the prospective client is not responsible for the data costs by working with cell phone service providers and you must have a method for prospective clients to opt-out.

If all that sounds like a hassle to you, consider this: the average open rate for text message campaigns is 98%, compared to a 20% open rate for email campaigns. SMS response rates are 295% higher than phone call response rates and 75% of people wouldn't mind receiving an SMS text message from a brand if they opt-in for the service. All this data leads to the undeniable fact that texting yields the highest rate of response.

## Law Firms at Risk

The information you handle every day is critical, because of this, firms all across the US are at risk. Any firm relying on existing non-secure messaging systems to communicate with clients is

putting themselves and their clients' confidential information at risk.

## Steps to Protect Yourself

In today's world, protecting yourself, your firm, and your clients is critical. Here are some basic measures and steps you can take to protect yourself.

- Password protection
- Multi-Factor authentication
- Hardware firewalls
- Encryption protocols for data sharing
- Training
- Testing to ensure compliance
- Move to the cloud

To learn more, check out our blog, Data Security for Law Firms: Everything You Need to Know