case status

CASE STUDY:

Enhancing Client Communication Security in Legal Practice

Introduction

In the digital era, law firms increasingly rely on older electronic communication methods, such as email and SMS text messaging, to interact with clients. However, these channels pose significant security and compliance challenges, particularly concerning the American Bar Association's (ABA) Model Rule of Professional Conduct 1.6 (and more specifically the opinions and guidance of state bar associations), which mandates the protection of client confidentiality.

This case study examines the limitations of traditional electronic communication methods, explores the recommendations from The Florida Bar as a specific example, and highlights the proactive measures taken by one law firm, Loyd J. Bourgeois Injury & Accident Lawyer, to safeguard client information with Case Status.

Since 2020, 750,000 cyber-attacks on law firms have been reported

In a recent episode of **Ethical-ish** (a podcast that looks behind the curtain at what makes a modern law firm compliant and ethical), Law Professor **Constance Anastopoulo**, who specializes in teaching ethics course at **Charleston School of Law** and UCLA School of Law, describes potential implications when law firms fail to navigate the intersection of ethics and technology. **She notes that since 2020, 750,000 cyber-attacks have been reported by law firms.** She shares a case study of a firm that suffered a phishing attack (via the client's email), leading to data loss, ransom payments, and mandatory client notifications—ultimately damaging their credibility.

More stats support this trend. According to the **2023 ABA Legal Technology Survey Report**, nearly 30% of firms experienced a security breach last year, a slight increase from the previous year. Communication methods and human fallibility continue to be the best tool used by bad actors.

Email & SMS Text in Legal Communications

When looking at how bad actors operate, you can usually find them using methods that are universally accessible. Email and SMS Text are ubiquitous in legal communications due to their high use rates by clients and firms. However, these platforms are vulnerable to unauthorized access, interception, and phishing attacks, potentially leading to data breaches and compromising client confidentiality. These factors create a perfect storm for bad actors.

The ABA's Model Rule 1.6(c) emphasizes that lawyers must "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." **(americanbar.org)** Given the inherent security risks associated with email and SMS, reliance on these methods may not satisfy the "reasonable efforts" standard set by the ABA.

Professor Anastapoulo applies these guidelines to the classroom noting that in the age of the cloud, the law firm and the attorney are 100% responsible for the privacy and protection of their clients' data. She offers tips for hiring third-party providers (avoid focusing on the cheapest vendor) and new lawyers (ask what they know about the role of technology in the practice). In this evolving landscape, she encourages all lawyers to become familiar with the ABA model rules for professional conduct in their jurisdiction and to take seriously the responsibility of due diligence. Keeping law firms out of the headlines is good for everyone!

> ***While some principles of legal ethics remain constant, technology has changed the practice, and ethics have to keep up with it***
>
> *Constance Anastopoulo*

SMS TEXT MESSAGING:

A High-Risk Communication Method

Recent reports, including a Forbes article discussing the FBI's concerns over SMS security, have highlighted the vulnerabilities of text messaging as a communication tool. SMS messages are unencrypted, making them susceptible to interception by hackers, SIM-swapping attacks, and unauthorized access through compromised phone networks. The article warns that text messages can be easily hijacked, allowing attackers to impersonate trusted contacts and steal sensitive information. (forbes.com)

In December 2024, the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) issued a warning about a sustained cyber-espionage campaign linked to Chinese hackers, referred to as "Salt Typhoon." These hackers have been infiltrating telecommunications systems to steal user data and, in some instances, record phone calls. The agencies emphasized the vulnerabilities inherent in unencrypted text messaging systems, which are widely used by millions of Americans.

To mitigate these risks, the FBI and CISA recommend adopting end-to-end encrypted messaging applications

Messaging Applications such as Signal, WhatsApp, and Telegram. These platforms ensure that messages remain accessible only to the sender and recipient, effectively thwarting interception attempts by malicious actors. Security experts have long advocated for the use of encrypted communications to protect against unauthorized surveillance and data breaches.

FBI warns Americans to keep their text messages secure: What to know

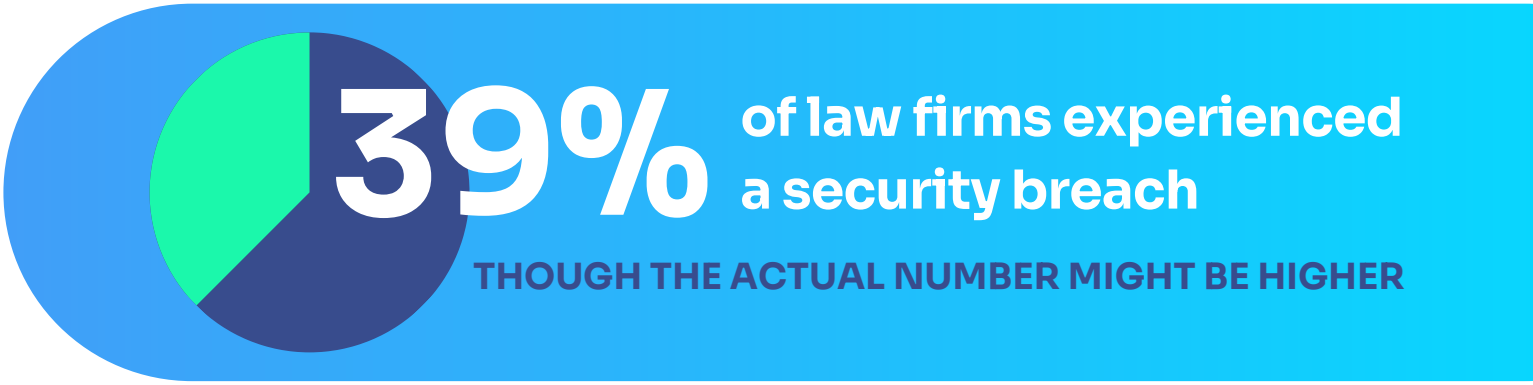
For law firms, the use of SMS presents a serious ethical risk under ABA Model Rule 1.6, as messages containing confidential client information could be intercepted or misdirected. Additionally, the inability to verify sender authenticity in SMS communications increases the risk of phishing attacks targeting clients. Given these risks, legal professionals should avoid SMS for any client communications involving sensitive or privileged information.

EMAIL:

A High-Risk Communication Method

Law firms are increasingly targeted by cybercriminals due to the sensitive client information they possess. A significant portion of these cyberattacks exploit vulnerabilities in email systems, with phishing and business email compromise (BEC) being among the most prevalent methods. These attacks often involve deceptive emails that trick employees into revealing confidential information or initiating unauthorized financial transactions.

The prevalence of cyber breaches in the legal sector is notable. According to the **American Bar Association's 2023 Cybersecurity TechReport**, 29% of law firms reported experiencing a security breach, an increase from 25% in 2021. Furthermore, a survey highlighted by **Legal Dive** revealed that 39% of law firms experienced a security breach, though the actual number might be higher due to undetected incidents.



To mitigate these risks, law firms are advised to implement costly cybersecurity strategies that still rely on human fallibility. This includes regular employee training to recognize phishing attempts, deploying advanced email security solutions, and establishing robust protocols for verifying the authenticity of email communications. Such measures often fall short to protect client data and maintain the firm's integrity in the face of evolving cyber threats.

SPECIFIC OPINIONS:

Guidance from The Florida Bar

The Florida Bar has acknowledged the challenges posed by electronic communications and has provided best practices to address these concerns. Their publication, "Best Practices for Professional Electronic Communication," underscores the importance of managing expectations, setting boundaries, and being cautious with electronic communications. While the document offers comprehensive guidelines, it highlights the need for lawyers to be vigilant about the security limitations of traditional communication methods. **Below is a specific excerpt from the Florida Bar from April 2025:**

Technology Considerations of Email

When sending attachments, be aware that they may contain metadata that could disclose unwanted information to the recipient.

Attachments may contain malicious software code. Use scanning software for both outbound and inbound emails.

If you use email as a form of confidential communication, you should know the risks and be familiar with the options of sending secure/encrypted messages.

There is always a chance that your email may be intercepted. Many of these risks are mitigated if not entirely eradicated when using an encrypted email service.

Secure client portals are an emerging and safe alternative to email. There are many case and practice management systems that offer a client portal component. You should seriously consider this option as a method of communication for confidential information.

The above is just an example. Most State Bars have similar language shared with their members that offer similar guidelines.

CLIENT PORTALS:

A Step Towards Enhanced Security

As suggested in the Florida Bar example, client portals are becoming more common. To mitigate the risks associated with email and SMS, many law firms have adopted client portals—secure online platforms designed to facilitate confidential communication and document sharing between attorneys and clients.

While client portals represent a significant improvement in safeguarding client information, it's crucial to recognize that...

NOT ALL PORTALS OFFER THE SAME LEVEL OF SECURITY.

Many portals are just a combination of an email or SMS service that directs the user to a web browser portal. Because logging into a web browser is problematic for users since they cannot remember urls, usernames and passwords, these providers are still sharing sensitive data in the email or SMS text message. **Thus you should review if the portal provider still relies on email or SMS notifications. If they are, you are accepting unnecessary risk and putting your clients confidentiality in jeopardy.** Inadvertently exposing your sensitive client information through less secure channels will not alleviate you from the pain and cost of a breach.

CASE STATUS:

Leveraging Encrypted Communications

Case Status, a client engagement platform, addresses these security concerns by utilizing a dedicated (native) mobile application that employs 2-factor mobile authentication and encrypted push notifications as the primary means of communication.

UNLIKE TRADITIONAL EMAIL OR SMS,

Push notifications sent through the secure app are much less susceptible to interception,

thereby enhancing the confidentiality and integrity of client communications. Part of the key of success is Case Status removes the reliance on email and SMS text. By putting its suite of communication tools right into the Case Management Platform, the staff can initiate communications from a single source. Moreover, because Case Status can get 80-85% adoption on the App, these messages are guaranteed to reach the client securely via the Push Notification on the mobile device.

APPLIED USE CASE OF CASE STATUS:

Loyd J. Bourgeois Injury & Accident Lawyer

Loyd J. Bourgeois Injury & Accident Lawyer, a Louisiana-based law firm, recently invested in the Case Status platform to enhance the client experience while at the same time simplifying communication for the staff. With security top of mind, the idea of reducing email and SMS text significantly with a SOC 2 Type 2 Certified company was icing on the cake. The firm was able to quickly onboard and migrate existing clients from legacy email and text to the platform. With high client adoption of the mobile App achieved in a very short onboarding period, the firm experienced an incident where a staff member's email account was hacked and compromised. Recognizing that this was still a potential risk to client confidentiality for the contacts in the users inbox, the firm acted swiftly by utilizing the Case Status platform to send a secure, mass notification to their entire client base within two minutes. This prompt communication advised clients not to open any emails from the compromised account, effectively mitigating potential harm and demonstrating the firm's commitment to protecting client information. In parallel the firm took action to address the email threat. The combination of minimizing the use of email and the ability to securely communicate via Case Status was key to this issues resolution. The matter was resolved with little to no impact. Unfortunately, the 750,000 other firms since 202 have not been so fortunate.

As a client-first practice, we are always looking for ways not only to improve the client experience and case journey for our clients, but also to look at how we can employ technology in a way that protects our relationship in every way. That philosophy brought us to making an investment in the Case Status. Their secure engagement platform is SOC 2 and HIPAA certified and integrates directly and securely into our Filevine case management system. We were so grateful that Case Status was in place when our team member's email was compromised. The ability to cut off a bad actor proactively and within 120 seconds was absolutely an amazing experience! We look forward to moving more of our internal and external communications onto this platform.

Loyd J Bourgeois,
Attorney and Founder
Injury & Accident Lawyer

LOYD J BOURGEOIS INJURY & ACCIDENT LAWYER

Conclusion

The vulnerabilities associated with email and SMS communications underscore the necessity for law firms to adopt more secure communication methods in compliance with ABA Model Rule 1.6. While client portals offer a viable solution, it's imperative to assess their security features critically. Platforms like Case Status, which utilize encrypted push notifications, exemplify the proactive steps firms can take to enhance client communication security. The experience of Loyd J. Bourgeois Injury & Accident Lawyer serves as a compelling example of how leveraging secure communication platforms can effectively protect client confidentiality and maintain trust in the attorney-client relationship.

LOYD J BOURGEOIS
INJURY & ACCIDENT LAWYER

About Loyd J Bourgeois

Injury & Accident Lawyer

Loyd J Bourgeois Injury & Accident Lawyer is a law firm fighting for fair compensation for people injured in an accident or denied disability benefits. We have a proven track record of successfully representing clients and getting them the compensation they deserve. When you work with our team, you can expect personalized attention and compassionate support every step of the way. We work tirelessly to help our clients navigate the legal process and ensure their rights are protected.

case status

About Case Status

Case Status is the leading legal tech company for client engagement with a vision to redefine how law firms interact with their clients. Our innovative, secure software platform and intuitive 5-star rated app simplify client engagement by providing real-time updates, secure messaging, and AI-powered insights to keep clients informed every step of the way. Seamlessly integrating with case management systems, Case Status streamlines communication, boosts client satisfaction and drives positive reviews and referrals. Our goal is simple: to enhance the experience for both clients and attorneys.

CASE STUDY:

ENHANCING CLIENT COMMUNICATION SECURITY IN LEGAL PRACTICE