Why Improving Billing Security Improves Client Experience

By Saurabh Mehra, *Oddr*

May 15th, 2024

What's interesting here is not so much the errors that have taken place in the past, but how little technology has come along to solve the problem for law firms and their clients, to significantly improve that critical aspect of client service that happens during the delivery of the clients' invoice—until now.

Every law firm wants their clients to have exceptional experiences of their services, from intake through invoice delivery because client service is often the key differentiating factor in winning new business as well as retaining and expanding existing.

Client service, however, has changed over the years. It's no longer a story of handing clients prestigious, 50-yard-line football tickets; rather, much of what clients consider to be client service today has to do with data and security.

In fact, year over year, the ACC Chief Legal Officers' survey shows that CLOs site security and data management as their number one priority when working with outside counsel; and as security threats evolve, so too the areas for which law firms should be scrutinizing for heightened security as part of that business-critical client service.

Consider, for instance, the security threat posed by the current process of sending clients their invoices in PDF format as an attachment in an email. There are notable and infamous examples of hard-working billers who have fallen prone to wrong recipient mistakes, including instances where trade secrets have been revealed, conflicts of interest, and more.

What's interesting here is not so much the errors that have taken place in the past, but how little technology has come along to solve the problem for law firms and their clients, to significantly improve that critical aspect of client service that happens during the delivery of the clients' invoice—until now.

Before we get into the solutions, however, let's dig more into the security problems in current invoice delivery.

The Increased Risk of PDF Attachments

Traditionally, billers prepare and send invoices as PDF attachments, a manually intensive process that in and of itself is very error prone. The firm's billers may be sending out thousands of invoices, a process which involves what may seem to be an army of people;-: text gets copy and pasted, modified, manually typed, autocorrected, and at some point the biller goes to a network drive to grab one of thousands of files to drag it into the email for sending.

Even in less extreme cases than the infamous ones cited above where trade secrets or conflicts of interest were revealed as a result of a wrong recipient failure, invoices contain loads of sensitive financial information that expose the firm and breach confidentiality when unintended recipients receive it.

Wrong recipient is not the only risk firms run with the sending of PDF attachments. When billers send invoices as a PDF, these PDFs go into a "black box": the biller—and the firm—simply lose all visibility and control over it. That PDF can now go to 20 people or 20,000 people and the firm would be none the wiser, nor would the firm be able to take any action to stop a malicious act of this kind. A PDF cannot be recalled and cannot be changed.

Even when PDF invoices are sent successfully and there is no malfeasance, yet another layer of client service arrives in the form of remittance. Remittance information is often in the footer of the PDF which must be copied and pasted into a new tab, or somehow the account and routing numbers must be carried over to multiple windows to remit payment—it's simply not a clean, single click experience.

If the PDF does, in fact, find itself in malicious hands, there have been many incidences that more than one firm has disclosed, that hackers can easily swipe the payment information the PDF invoices contain for other types of attacks.

In these instances, hackers are able to impersonate the law firm to the client leveraging the key financial information found in the PDF to increase the authenticity of the malicious payment requests.

These are not siloed examples of malicious attacks happening to small law firms, but rather a pattern of behavior across the Am Law 100 and 200 as well. Cyber criminals are organized and intelligent about their attacks; they know where there are weaknesses in financial systems and, unfortunately, are relentless about expositing those weaknesses.

How Law Firms Can Deliver Secure Billing

Law firms cannot afford the reputational or financial damage these embarrassing and costly episodes may incur. Security is paramount for clients; to that end, law firms should be stepping up and offering their clients the most secure solution available on the market to protect every aspect of communication — and that includes billing.

Today, there is innovative technology that can help law firms gain control over bill delivery that radically improves the firms' ability to remain in control of the invoice, enable the firm to take action if the invoice is mishandled or maliciously attacked, and ultimately gain visibility over invoice status throughout the entire lifecycle of the invoice at the client—and, of course, removes PDF email attachments from the process entirely by providing either a secure link along the lines of a DocuSign platform or a secure client portal.

In the first scenario, innovative technology similar to DocuSign is leveraged to deliver a secure invoice link from the law firm to the client. With the advent of secure invoice links, firms have ultimate control over the viability of the invoice, can create time dependencies, update the URL or remove information in near real time if the link is compromised.

With secure links billers gain visibility over the invoice status: they are able to see whether the invoice has been viewed and by whom and where. Predictive analytics can add layers of security by informing billers if atypical behaviors have been engaged with a recent invoice link such as an end user viewing the invoice from an atypical geography.

With this advanced technology, firms for the first time can also audit what is happening with their invoice links. If someone at the client shares or views or forwards the email, advanced technology can automatically audit that activity throughout the entire invoice lifecycle from the time it's generated until the moment it is paid. We have an automatic audit of everything that happens on it, including what's happening on the client side that no one else can provide.

And because the advanced technology framework can supports it, invoices links can be recalled at the click of a button — and that's something a PDF will never be able to do.

Another option that can radically transform the security of client billing is to provide a secure client portal.

In this scenario, clients are invited by invitation-only to a "client.org" portal where clients can then see and manage all invoices, essentially eliminating emails from the equation entirely. Passwords, too, are cumbersome and can be mishandled and so, OTP based logins can be created where users essentially enter their unique email and are sent a unique code for each unique login.

In the client portal scenario, not only are current invoices and statements ready for viewing, but historical information as well, a modernized way to communicate with clients about invoice statuses and empowering them to self-serve information on demand.

In both scenarios, the last piece of the puzzle is payments. One of the most surprising disconnects of current billing and collections processes is the lack of integrated payments: addresses for snail mail delivery of paper checks, payment information that must be typed into other windows across different platforms — all of these actions slow down the ultimate goal of billing which is for the firm to get paid for its work.

Users are increasingly sophisticated and have grown accustomed to seamless payments in every other aspect of their lives and business interactions; to not have integrated payments as part of billing and collections is increasingly a failure of client service.

Integrated payments provide that perfect win-win for the firm—a superior client experience that is seamless, but also helps the firm get paid faster. And that's what it's all about.

Conclusion

Client service doesn't end — hard stop. And it certainly doesn't end before the invoice goes out. Every interaction is an opportunity for the firm to provide the best experience current knowledge and technology is able to deliver — and since security is a key component of what clients want, security needs to be part of that equation.

About Oddr

Oddr is the legal industry's only AI-powered invoice-to-cash platform. Oddr's AI-powered platform centralizes, streamlines and accelerates every step of billing + collections — from bill preparation and delivery to collections and reconciliation – enabling new possibilities in analytics, forecasting, and client service that eliminate revenue leakage and increase profitability in the billing and collections lifecycle.

Get in touch

Contact us now to find out how the Oddr platform can help optimize your firm's invoice to cash process.

oddr