Signature Parsing and Data Enrichment

Updated March 2024

Client Sense

As the use of personal information becomes an increasingly important and hot topic, law firms have a heightened responsibility to protect their clients and act ethically as a part of their business conduct. It is not difficult to see how easily a law firm could generate headlines in this space for any form of misstep, which is why “data enrichment” or trusting a third party with any client communication (privileged and confidential) should be considered an unacceptable and unnecessary risk.

1. Any ERM product must scan the whole email to find and read the signature block, because it is a part of the email body. Where signature processing does not reside within the firm (digital or as a human task), and a third party Is used, then that third-party provider becomes privy to confidential and privileged communications. If a third-party provider asserts that they encrypt the shared email communication so they cannot see it, how does their system read the signature block?

   This is where Client Sense stands out. We process signatures ***within the firm’s security environment***, thereby securely processing client communication to assess signature blocks and storing the resulting data within the firm's control. To our knowledge, we are the only company doing this.

2. Some companies tout their “data enrichment” capabilities. It's important to note that this is not the same as reading the signature block provided to the firm by an individual. In obtaining this personal information, the firm may not be the intended recipient or rightful custodian of the data they have purchased or obtained through such an approach. This means that the firm could be handling data it doesn't have the legal right to possess, potentially leading to legal complications and breaching client confidentiality and or legal privilege.

   If a company offers data enrichment relating to individual contacts and/or companies, it is important to consider the following:

   - Does the firm have the legal right/license to use this information in any way they like, including for marketing purposes?

   - For any individuals where their details are being sold/provided through a “data enrichment” approach, have these individuals provided consent for their information to be used? For what purposes and by whom?

In summary:

1. Confidential and privileged client communication cannot and should not be shared with any third party (including software providers) without the explicit consent of each client potentially impacted.

   Client Sense has been developed from the outset to honor this.

2. Even when a client openly provides the firm with their information via a signature block or on a business card, the firm still needs to comply with GDPR and anti-spam regulations. The collection of data, along with the right to use that data, should be distinct.

3. Purchasing personal information, otherwise marketed as "data enrichment,” places a significant burden on the firms using this information, particularly where these third-party providers do not stipulate how they collect this personal information, from where, and with what consent. Non-compliance with data protection regulations can lead to severe penalties and damage to your firm's reputation.