Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Tension Between Privacy And 'Know Your Customer'

Law360, New York (May 4, 2016, 11:36 AM ET) --

Cheryl M. Lott

Ransomware, spyware, spoofing and phishing attacks, among other things, have made customers weary of sharing their information. Financial institutions, on the other hand, have a legitimate need for the very information that customers seek to protect. This tension between the customer's desire for privacy and the financial institution's need for information can strain the relationship.

Some "Know Your Customer" Basics

To comply with the KYC requirements, a financial institution, which is broadly defined (see 31 U.S.C. §5312), must run various searches and collect basic information about its customers; those who pose a higher risk require more detailed information. A customer's higher risk rating can be based on the customer's net worth, type of business, source of wealth, or a variety of other factors. The customer due diligence (CDD), of which KYC is a part, also requires certain levels of corroboration of the information based on the customer's risk rating. Obtaining information necessary for the customer identification process (CIP) is necessary for the KYC process and should be fairly easy as the vast majority of customers will understand that financial institutions require a certain level of identification in order to process transactions.

One of the consistently challenging areas of KYC is the specifics of the source of wealth for higher-risk-rated customers. This is also the area in which an institution will need to focus on the corroboration of the information it receives. Thus, the tension builds: where a customer is less likely to volunteer additional information is the area in which the financial institution needs evidence to support the information it receives.

Need for Information

The information a financial institution needs to corroborate a customer's source of wealth is the same information that customers are guarding more closely than ever. So how can financial institutions obtain the information they need without unduly disrupting the customer relationship?

First, one of the best opportunities to gather necessary information for the CDD process is at account opening. This is true regardless of whether the account is a single checking account or a complex loan transaction. At that point, gathering the information necessary for the CDD process serves a dual purpose: the institution is gathering the information that might be useful in determining what services and products would best suit the particular customer's needs, and also gathering at least some of the

information necessary for the CDD process. The same is true for periodic updates: have the customer's transactions varied from the stated account purpose? By what margin? What has changed in the customer's circumstances might alter the products and services the institution is providing or offering to this customer, and these changed circumstances may affect the ongoing CDD process.

These sorts of inquiries can certainly signal the need for new or additional services, but they can also signal the need for escalation, and a more detailed review, or even filing a suspicious activity report. When requests for information are framed as ways in which the institution is trying to better serve the customer, a customer may be more willing to provide information.

What do you do when you need information and the customer refuses? Or worse yet, the customer says no other institution is asking for this level of detail and that they might consider transferring their accounts to these other institutions if your institution keeps pushing for information. First, remember that all institutions are required to complete the KYC process and thus all institutions with which the customer is dealing should be gathering the same information. Second, if the process becomes that difficult, that can be a sign of trouble. Maintaining the integrity of one's personal information is a legitimate concern, but refusal to provide any detailed information could be a sign of possible issues with the client, his/her/its accounts, and/or the legitimacy of the source of the funds.

You can proactively attempt to address this sort of response by conducting publicly accessible searches for information on that particular customer. For example, third-party sources like the stock exchange, if the company is publicly traded, or trade publications may be a good source of at least some of the information you may need. It is best to conduct these searches before contacting a customer as it is often easier to have someone corroborate information you already have as opposed to requesting information, getting a customer refusal, and then going back to that same customer with information they did not provide.

Consequences of Actual or Perceived Noncompliance

The consequences of actual, or even perceived, noncompliance are wide-ranging and can be quite severe.

From a business perspective, having reliable customer information is simply good business. In a loan transaction, for example, one of the institution's primary concerns is loan repayment. Part of the compliance process is performing basic customer searches. If one of these searches reveals that your customer's name appears on an Office of Foreign Assets Control (OFAC) list, the funds in the customer's account should be transferred into a blocked account. If an institution does not conduct this search, the loan funds could end up in the customer's account at another institution that has cross-checked against the OFAC list, and those funds would be put into a blocked account. The likelihood of your institution being repaid on that loan is slim. The institution could then end up in a battle with the federal government over the funds, and worse yet, be the subject of regulatory investigation for not having conducted the search prior to lending.

If there is a federal investigation, the consequences can be far-reaching. Federal regulators have imposed onerous compliance terms and significant multimillion-dollar fines, and the Senate has conducted hearings calling bank officials and individual bankers to testify as to the nature of the system, and how it is that certain significant failures occurred. In some cases, the government has stripped officials of their ability to participate in any capacity in any financial institution, and financial Institutions have been criminally charged in relation to anti-money laundering/Bank Secrecy Act (AML/BSA) failures.

Other consequences are civil suits brought by victims of fraud schemes that, according to plaintiffs, should have been detected and reported by the financial institution. Plaintiffs claim that had the institution conducted the required due diligence, the plaintiffs either would not have been harmed by the scheme or the harm would not have been as severe. Some plaintiffs have gone so far as to claim that the financial institution was affirmatively aiding and abetting the fraudster's scheme.

All in all, compliance with these regulations is imperative to a financial institution's operations. Aside from compliance with federal regulations, it is simply good business.

—By Cheryl M. Lott, Buchalter Nemer PLC

Cheryl Lott is a shareholder in Buchalter Nemer's Los Angeles office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.