ACAMS® TODAY

The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field

SARS AND THE ONBOARDING PROCESS

One of the principle tenets of an effective anti-money laundering (AML) compliance program is implementing a thorough customer onboarding process. Section 326 of the USA PATRIOT Act establishes the minimum standard for all financial institutions to implement a Customer Identification Program (CIP) with specific guidance as to how CIP should be structured. CIP is part of the preventive component of the internal controls, policies and procedures pillar of AML compliance programs. Applying the minimum CIP requirements (legal name, government identification number, physical address and date of birth for individuals) is extremely important, but not always performed correctly. In addition, basic CIP may fail to provide a complete picture of a customer's activities and normal course of business, which is why enhanced due diligence is important in filling any missing pieces of the risk puzzle during the customer onboarding process.

But are financial institutions getting onboarding right? If not, then why not?

The suspicious activity report (SAR) numbers indicate that the answer is "No," so we are left with the "Why not?" to analyze.

The Numbers

One way to measure onboarding effectiveness is to look at the number of SAR filings related to issues with identification documents, which are an indicator of poor onboarding practices and failure to periodically conduct know your customer initiatives for long-term customers.

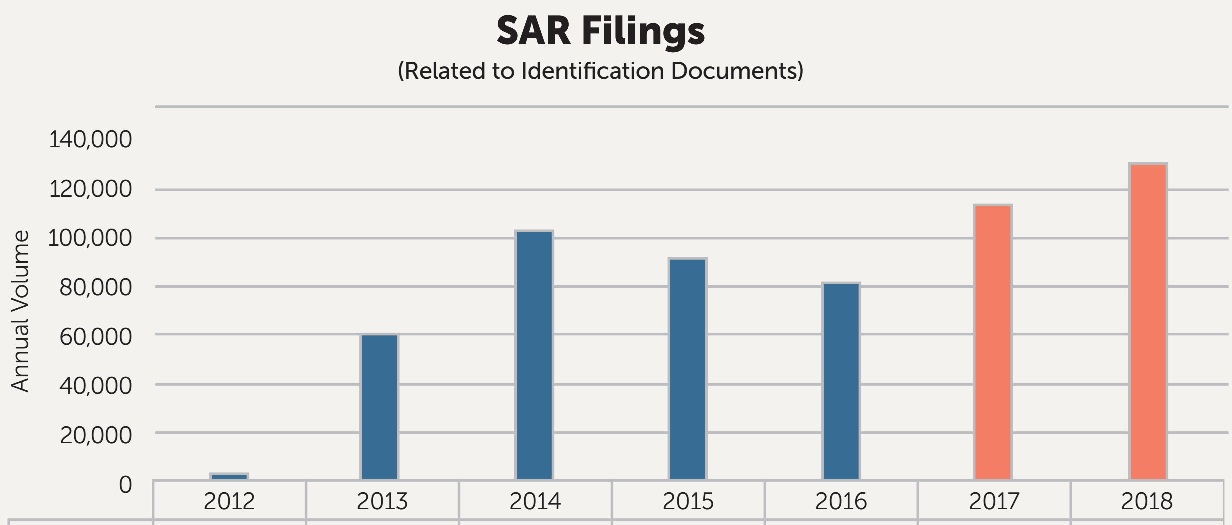
According to Graph 1, from 2012 through 2014, SAR filings related to identification documents increased by 342 percent, then tapered off by 21 percent through November 2016.[1] While that reduction over the past two years is a positive indicator of onboarding effectiveness, a deeper look into industry types paints a bleaker picture aside from depository institutions.

As shown in Graph 2, identification-related SAR filings have seen sharp increases for securities firms, money services businesses (MSBs), and financing and loan companies.[2] Most

[1] Data pulled from https://www.fincen.gov/reports/sar-stats. Filters used: Suspicious Activity Category/Type: *Identification Document; Industry Type: Depository Institutions, Insurance Companies, Loan or Finance Companies, Money Services Businesses, Securities/Futures;* Year and Month: *All*

[2] Data not available for all years in all categories.

Graph 1



	2012	2013	2014	2015	2016	2017	2018
Values	3,002	60,258	102,565	91,408	81,300		
Forecast						112,702	129,428

striking is the 216 percent increase among MSBs, which pose a significant money laundering risk because of their “relationships with foreign agents and counterparties to facilitate the movement of funds into or out of the United States.”[3] One reason for this negative shift for MSBs could be due to improved onboarding at depository institutions (fewer SARs), and the ease of which MSBs can provide access to the U.S. financial system in comparison.

So, why not?

There are many potential reasons that financial institutions fail to properly onboard new customers. First and most obvious, it is too easy not to. New customers mean new revenue, and it is counterintuitive for a salesperson to undertake an extensive review of onboarding documents and customer profiles that may result in declining a customer’s business. Next, your AML personnel are not the people making initial contact with new customers—that is what the sales team does! Sales team members may simply assume that an institution’s monitoring systems will immediately catch suspicious activity (reactive) than thoroughly research customer information and assist in forming a risk profile (proactive). Most people are bigger fans of making more money doing less work than making less money doing more work. Here we observe that high-risk MSBs may be seeing the results of not having the will or capacity to vet their customers due to volume and fee-based revenue structures.

Other potential causes (every organization will have unique issues) result from a lack of a risk observant culture, or a failure to codify and/or implement a robust onboarding or CIP process. The latter issue is likely a much easier fix in the short term. Changing an entire company’s culture in order to meet compliance standards is a bit more challenging. After all, financial institutions exist to gain and serve customers and to create profit—not to catch bad guys.

What Can Be Done

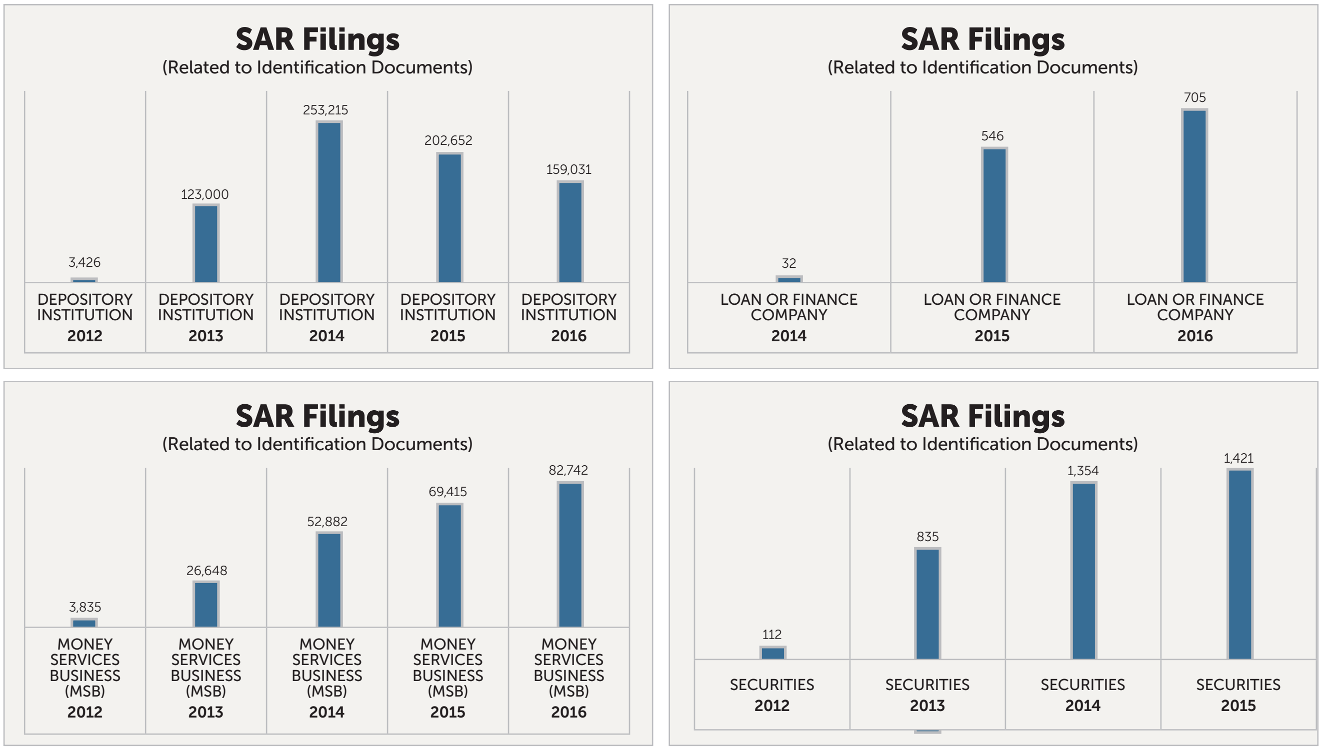
Many other people have proposed the following recommended possible solutions, many times before. The problem is not the ideas, but more often the willingness to implement change that can place short-term revenue at risk. That stated, let us reinforce some potential solutions:

- Incentivize sales teams to identify high-risk customers. For example, rewarding employees for identifying high-risk characteristics during onboarding.
- Pair your sales teams up with compliance teams. Enable your AML experts to help sales teams identify red flag characteristics and perform efficient due diligence. AML teams can also assist with training.
- Avoid click-through web training when possible and make it meaningful.
- Conduct independent testing of your onboarding processes.
- Implement a CIP familiar with identification documents,[4] verification of those documents, physical address confirmation, in-person verification, potential customer risk factors and safeguards to prevent non-verified persons from opening an account.
- Emphasis from top leadership will enable a more risk observant culture in the organization. That

[3] “FinCEN Issues Guidance to MSBs on Anti-Money Laundering Program Requirements for Dealing With Foreign Agents and Foreign Counterparts,” FinCEN, December 8, 2004, https://www.fincen.gov/news/news-releases/fincen-issues-guidance-msbs-anti-money-laundering-program-requirements-dealing

[4] Jacqueline van den Top, “The Challenges of ID Verification When Accepting Clients,” *ACAMS Today*, December 2015-Februray 2016, http://www.acamstoday.org/challenges-id-verification-when-accepting-clients/

Graph 2



emphasis can be demonstrated through action in enacting incentives, communicating successes in your AML program (especially the preventative successes), and providing meaningful training.

- Finally, implement a CIP process that, in accordance with Section 326 of the USA PATRIOT Act, enables the financial institution to form a reasonable belief that it knows the identity of each customer. The components of that process should include (at minimum) information verification, information screening, record keeping and documentation,[5] a method to escalate discrepancies and red flags prior to account opening.

Potential Results

In the past five years, there have been an average of 196,794 SAR filings related to issues with identification documents. That includes the low end outlier of 2012. Let us assume that each SAR filing takes eight hours of labor to analyze, document, create and review—a conservative estimate to be sure. Let us also assume that employees involved in the SAR process make $65,000 a year (feel free to play with these numbers). The annual cost for financial institutions to file this type of SAR equates to over $49 million, which does not take into account any costs or fines incurred from off-boarding customers or regulatory actions.

Now let us say you implement a more effective client onboarding program and are able to prevent 25 percent of the clients that will create SAR filings related to issues with identification documents. That is an industry-wide savings of over $12 million, which does not seem like much, unless you happen to be an MSB or other high-risk financial institution that will likely be targeted by regulatory authorities. In addition, the prevention of more high-risk customers being onboarded has positive second and third order effects on monitoring efforts, reputational risk and other costs of compliance.

Conclusion

Giving due consideration to the onboarding stages of the client lifecycle reduces reputational risk to the financial institution, lowers overall costs of AML programs by reducing the number of SAR filings and potential regulatory action, and supports the intent of AML and counter-terrorist legislation. Applying resources within an AML program in a risk-preventative manner, reinforcing a culture of compliance, and evaluating the people, processes, and technology that serve as the institution gatekeepers are likely to make your onboarding programs more effective, and reduce the negative consequences of ineffective CIP.

Mike Carter, CAMS, Manager, Alvarez & Marsal, Jacksonville, FL, USA, mcarter@alvarezandmarsal.com

[5] Brian Arrington and Ann Broeker, "Sanctions and the New Due Diligence Standards," *ACAMS Today*, December 2016-February 2017, http://www.acamstoday.org/sanctions-and-new-due-diligence-standards/