To Risk Or Not To Risk

5 Questions to ask yourself before attempting to "de-risk" your institution.

We have been getting mixed signals about a new anti-money laundering trend of banks 'de-risking" undesirable accounts. Rumors started in 2013 and made public in early 2014 that financial institutions were facing regulatory scrutiny, criticisms and fines over banking higher risk businesses. Soon the term "Operations Choke Point" was being whispered throughout the industry as the process of eliminating businesses perceived to be "too risky" by choking off their access to financial services.

This was being accomplished by having bank examiners place pressure on banks to do more when it came to due diligence of higher risk businesses. Institutions unwilling or understaffed or unequipped to take on this additional monitoring were closing these businesses in order to avoid regulatory fines.

The operation which started with third party payment processors, payday lenders and online lenders, has now expanded to businesses such as; money service businesses, gun dealers, credit repair services, adult entertainment businesses, pharmaceutical sales, telemarketing, tobacco sales and travel clubs. The majority of these businesses are legal entities that provide legitimate services. Strangely enough very little mention has been made to marijuana related businesses.

Mixed Signals

So while examiners are scaring institutions into closing these accounts, FinCEN is emphasizing the need to provide services to these industries. FinCEN Director Jennifer Shasky Calvery said in her remarks at the 2014 Mid-Atlantic AML Conference in Washington, DC in August*:*

"It is not the intention of the AML regulations to shut legitimate business out of the financial system. I think we can all agree that it is not possible for financial institutions to eliminate all risk. Rather, the goal is to provide banking services to legitimate businesses by understanding the applicable risks and managing them appropriately."

She further stressed that the only way law enforcement can get the information they need to assist with their job is for these businesses to have bank accounts so that their activity can be monitored and reported if determined to be suspicious.

She did admit that signals were mixed when she further stated they are asking financial institutions to help them keep dirty money from contaminating the financial system. The message she imparted was that institutions have to find a balance between maintaining the accounts so that law enforcement can receive good BSA reporting and effectively managing the risk of maintaining these accounts.

So before an institution decides to begin de-risking there some questions they need to ask themselves.

1. Are all high risk categorized customers the same?
Another comment Director Calvery made in August was "just because a particular customer may be considered high risk does not mean that it is "unbankable" and it certainly does not make an entire category of customer unbankable."

For example, not all money service businesses provide the same services or have the same volumes. Consider the local grocery that sells money orders and sends Western Union money transfers versus the check casher with activity aggregating over a million dollars monthly. Or the third party payment processor that provides payroll services versus one providing services to the adult entertainment industry. Not all higher risk business types carry the same level of risk and so due diligence necessary to mitigate the risk should be balanced.

If you do decide that you want to bank a certain classification of clients, it does not mean you have to bank them all. Be choosy...ask questions up front. It is important to understand the diversity, volumes and services. Have each relationship vetted by properly trained designated parties. Then do ongoing due diligence to monitor for any changes to their risk.

2. What is the risk to my bank if I bank these businesses?
There are three areas of risk an institution needs to consider; compliance, fraud and reputation.

Compliance: Institutions have to comply with the Bank Secrecy Act and other state and federal laws. This includes collecting information upfront in order to "know your customer", filing currency transaction reports, record keeping requirements, ongoing due diligence of their customer base as well as the reporting of suspicious activity.

Fraud: Institutions have an obligation to their customers and to themselves to reduce the risk of fraud that may be conducted through their institution. While probably impossible to eliminate all possible fraud, controls need to be established. For each type of "risky" business, conduct a threat analysis to determine; what are the risks, what controls do they already have or can put in place and balance these with their pain threshold of possible losses.

Reputation: Institutions also worry about the public perception if it became known that they were banking less desirable customers. Many shy away from opening accounts for tobacco producers, gun manufacturers, adult entertainment businesses and even porn stars. There have been multiple reports about porn stars and their family members having bank accounts closed or being denied accounts due to compliance issues or moral reasons. Reputation risk is real and a bank with a bad public image may drive away customers and shareholders.

3. Is it profitable to my bank?
Believe it or not....financial institutions are in business to make a profit. However they often state that the costs associated with keeping these accounts outweigh the benefits. If the relationship does not make money then why even attempt to maintain it. Have you priced it accordingly? You can charge more for businesses that require more resources to maintain. Chances are if they try to go elsewhere they will still have to pay for the privilege to maintain

the account. Think about how much the account will cost to do proper risk mitigation and put in a margin for a profit as well.

4. What businesses will my bank absolutely positively not bank?
There will probably be some business types you will not want to bank regardless of risk or mitigation. For example porn shops or other adult entertainment business, online payday lenders, online gambling businesses, or the actual retail stores that sell marijuana. Work with your board or senior management to determine exactly who you will or will not bank. Make sure they understand all the risks and what resources will be needed to mitigate the risk. Make a list, make it clear in your policy and procedures and make sure your compliance, operations and front line staff are kept in the loop.

5. Do I have the resources for proper risk mitigation?
There is a reason why these institutions are being targeted. There is risk associated with them and detailed policies and procedures need to be documented as to how this will be addressed for each of the higher risk categories you decide to bank.

Luckily there are resources available. The FFIEC BSA/AML Examination manual lists the risks associated with most high risk businesses. They even go on further to list many possible controls, policies and procedures that may be implemented to reduce the risk. How cool is that! There is even technology and automation available to help you manage the extra obligations and workload.

The majority of these businesses serve a legitimate purpose, however you might decide that they do not fit into your culture, business model or ethics or you are not prepared to handle the extra due diligence and scrutiny that is involved with banking these businesses. This is a risk and reputation based, (morally wrapped) decision that each financial institution will have to address.