Section 6 – Industry Forum

In each issue of *The SAR Activity Review*, representatives from the financial services industry offer insights into some aspect of compliance management or fraud prevention that presents their view of how they implement the Bank Secrecy Act (BSA) within their institutions. Although the Industry Forum Section provides an opportunity for the industry to share its views, the information provided may not represent the official position of the United States Government.

Transaction Monitoring & Reporting for Money Services Businesses

By: Peter Ziverts, on behalf of the Non Bank Funds Transmitters Group

Money Services Businesses (MSBs) come in a wide variety of sizes and shapes. They range from sophisticated, publicly traded money transfer companies and check cashing chains to 'mom and pop' grocery stores.

They also vary in the types and scope of services they provide. Western Union, for example, is an MSB by virtue of its role as a "wholesaler" of money transfer services and money orders. Wholesale, or primary, MSBs typically do not interface directly with consumers at the point-of-sale (though they generally provide telephone customer service support). Instead, they provide their financial services and systems to retailers – also MSBs – which sell them to the end user. Retail MSBs serve as the direct consumer interface and vary widely within their category, ranging from independent 'mom and pop' locations to national grocery chains.

What these businesses have in common is that they all offer a host of much-needed financial services to individuals – both with and without banking relationships – and businesses. And, as financial institutions, they also have a common responsibility under the BSA to implement and maintain an effective anti-money laundering compliance program that is reasonably designed to prevent them from being used to facilitate money laundering or the financing of terrorism. Clearly, transaction monitoring and reporting – both SARs and CTRs – are vital components of this responsibility.

It is through their transaction monitoring and reporting responsibilities that these vastly different types of businesses have a critical nexus in protecting our nation's financial system from potential abuse. Viewing individual and aggregate transaction activity through different lenses serves as the basis for filing meaningful reports, which provide valuable assistance in law enforcement investigations.

Transaction Monitoring: A Dual View

MSBs identify and report suspicious activity to the IRS on a SAR-MSB form. Much like banks, a SAR-MSB must be filed if an MSB knows, suspects, or has reason to suspect that a transaction or series of transactions involves money laundering, violation of the BSA (including structuring), terrorist financing, other violation of criminal law, or serves no apparent lawful purpose.

Primary MSBs and their agents each have a responsibility to monitor and report suspicious activity, which they do on two levels: 1) subjectively, at the agent MSB level through direct consumer contact and 2) at the primary MSB level through objective, data driven analysis.

At the agent level, employees are trained to identify suspicious activity by monitoring consumer behavior, such as:

- Hurried, nervous or evasive consumers
- Consumers who know too much about BSA reporting and recordkeeping rules
- A consumer who is aggressive or uncooperative
- Someone who is reluctant to provide ID when requested
- Someone who provides inconsistent information when asked questions
- Consumers who conduct multiple transactions just below reporting or recordkeeping thresholds
- A consumer who offers a bribe or "tip" to bend the rules
- ID documents that appear to have been altered or forged
- Multiple consumers who approach the store together, but ignore each other and conduct separate transactions once inside
- Different consumers sending funds to the same person

Agent MSBs file SARs based on subjective consumer behavior and transaction activity, and they can support this view through software provided by the primary MSB. For example, Western Union provides its agents with software that allows them to monitor their transaction activity on an aggregated basis, looking for additional suspicious activity by examining principal, volume and frequency patterns, among other clues.

Such tools provide several options. An agent's Compliance Officer can identify suspicious activity by reviewing raw transaction data alone. Another option is the creation of *internal* suspicious transaction reports, which, after several days or a week, a Compliance Officer can review alongside general transaction activity, and copies of consumer forms and receipts, to identify potential suspicious activity and file SARs accordingly.

The key to successful agent level suspicious activity reporting is: 1) employee training and 2) regular review. Primary MSBs should have tools to facilitate and encourage a robust agent suspicious activity review and reporting process. Such support can be provided through analytical software, agent training assistance and periodic review of the agent's internal procedures.

In contrast to an agent's localized view, primary MSBs have a view of their entire network and can objectively analyze aggregated transaction data to identify, for example, basic structuring or smurfing activity, as well as more nuanced activity such as one person sending funds to multiple jurisdictions, many senders concentrating funds to one recipient or linked transaction patterns.

Because monitoring is one of the most effective ways for a primary MSB to "know its customers" they should have sophisticated analytical software that can identify transactional "red flags", i.e. structuring, as well as allow for customized research. Most monitoring systems review single day activity as well as activity over longer periods of time to allow for the identification of patterns. Taking this longer term look will provide law enforcement with more meaningful reports.

And the world is a big place – especially when it comes to keeping track of millions of transactions. Even though suspicious activity reporting is required in only a handful of countries, an MSB's systems should not only be capable of reviewing U.S.-centric activity, but also allow for the monitoring of off-shore activity, particularly in higher risk jurisdictions.

This dual, or holistic, view to transaction monitoring provides a comprehensive system for understanding consumer activity and identifying suspicious activity, which serves as the backbone for meaningful reporting.

Assessment & Control: It's All About Risk

Having an effective view over transaction activity serves as a *gateway* to filing meaningful reports. Once inside the gate, it takes thoughtful transaction analysis to: 1) know what activities and patterns to look for and 2) understand and determine what information will be useful to law enforcement in a SAR filing. Thorough analysis depends on robust systems for risk assessment and control, which lie at the heart of a robust MSB anti-money laundering compliance program.

Based on the nature of the MSB, risk profiles incorporate many factors. Primary MSBs consider such factors as:

Products

What is the purpose of each product and what is its inherent risk - that is, the level of risk before the application of controls, systems, and processes used to reduce the risk?

For example, on a given risk continuum, money orders – because of their potential for anonymity – are generally considered riskier than consumer-to-consumer money transfers, which require a certain level of sender and receiver information. On the same continuum, consumer-to-consumer money transfers are generally considered riskier that consumer-to-business money transfers because the primary MSB has an ongoing subscriber relationship with the receiving entity – on which it has conducted due diligence – and collects certain information from the sender. The increasing popularity of prepaid debit cards – which can have some similarity to money orders – are giving rise to new risk considerations and questions.

Sender/Receiver Relationship

The relationship between the sender and the receiver offers another risk touch point: consumer-to-consumer, consumer-to-business, business-to-consumer and business-to-business. Each of these carry different risk profiles based on the relationships each has to the other and the relationship each has with the primary MSB.

Geography

Agent locations and transactions taking place in High Intensity Financial Crime Areas (HIFCAs) and High Intensity Drug Trafficking Areas (HIDTAs) also affect risk, although the HIFCA and HIDTA designations have become so general that their practicality is questionable. Better yet, is review and analysis of money transfer corridors, which can provide deeper insight into questionable activity.

Agents

Agents also play a role in risk assessment because large agents – national or regional chains – will have a greater degree of anti-money laundering compliance sophistication and more resources than the small 'mom & pop' agents. This consideration plays a significant role in the frequency and depth of agent anti-money laundering program reviews by primary MSBs, and the banks that provide their banking services. The inherent risk of agents with high transaction volumes is mitigated by more frequent program reviews. And, certain agents – perhaps those in former Non-Cooperative Countries and Territories – warrant consistent monitoring and transaction analysis.

Rating Risks

Alas, all risks are not created equal. Individual risks should be rated using a risk rating methodology, which can be a complex task. Risk rating systems can look any one of the following ways – or more:

- High – Medium – Low
- Extremely High – Moderate High – Medium – Moderately Low – Extremely Low
- Number rating 1-5 or 1-10
- Acceptable – Unacceptable

Applying such systems depends on defining each risk rating and identifying which characteristics qualify as high, medium or low. Criteria for defining the ratings can vary by business and the type of service being provided.

For one business, High Risk might mean the regulatory requirement is complex, carries potentially large fines, has changed recently and no updated controls are in place, no training has been done, and the monitoring process used is entirely manual.

On the other hand, Low Risk could still mean the existence of complex regulatory requirements and fines, but the product has an inherently lower risk consumer-to-business business model, supported by robust monitoring and control systems and extensive agent training.

All of the factors can vary based on an MSB's anti-money laundering sophistication, systems/automated monitoring capability and management commitment to anti-money laundering compliance.

At The End Of The Day … It's About The People

However, computers, software and risk assessment are just the foundation of an effective monitoring program. The real 'Intelligence' comes from the analyst. While a computer may flag activity for review, it is the person looking at the screen who should determine whether a series of transactions is a reportable event.

Therefore, analysts should be highly trained and motivated. They should fully understand the MSB's business model, its customer base and cultural diversity, as well as the BSA and typical money laundering schemes. This knowledge set can be gained through formal seminars, in-house training/on-boarding and on-the-job mentoring and coaching. New analysts can start by reviewing large currency transactions and graduate to standard SAR reviews. However, customized reviews and those encompassing higher risk jurisdictions should be handled by senior-level analysts, preferably ones familiar with the geopolitical and cultural characteristics of the areas in question. Such senior level analysts can also act as liaisons to law enforcement, thereby increasing their own understanding of what to look for and how to better report it.

Finally, an effective risk-based monitoring program will collect intelligence from every possible source, above and beyond mere transaction data. Law enforcement contacts are essential to addressing potential risk and knowing where to point the telescope. Continued dialogue with the MSB's business people, sales staff and agent base can provide early warnings to anomalies later detected in the system.

By thoroughly understanding the risks associated with various consumers, services and geographies, MSBs can develop an effective suspicious review mechanism. This mechanism – part machine, part human and driven fully by management's unwavering commitment to anti-money laundering compliance – can help ensure that MSBs can address and mitigate risks effectively as we as provide law enforcement with meaningful information to protect our nation's financial system.

###