SBS
SAFE BANKING SYSTEMS

NEWS&VIEWS

June 2014

Taking the Game out of the Gaming Industry

Any casino that thinks it is in the entertainment industry and not held to the same regulatory standards as financial institutions should think again. Casinos are a 24x7, high-volume cash business that provide some of their best customers with bank-like services such as currency exchange, money transfer and check cashing. That makes them a natural target for money laundering. It also subjects them to the same requirements as financial institutions under the Bank Secrecy Act. They must report suspicious activity.

In her September 2013 speech to the American Gaming Association, Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network (FinCEN) staunchly reminded casino operators of their responsibility. "Casinos are the eyes and ears in the fight against terrorists and other bad guys, and your AML programs are the first line of defense from keeping these bad actors out of the financial system."

For any casino operator that underestimates its obligation or the weight of Shasky Calvery's words, the Las Vegas Sands and Caesars Palace cases should serve as a cautionary tale. In August 2013, Las Vegas Sands paid more than $47 million to the U.S. government to settle a money laundering investigation. The casino failed to report suspicious activity from one of its highest rollers, who was subsequently identified as a drug kingpin. Shortly after the settlement was announced, Caesars Palace was accused of alleged violations of the Bank Secrecy Act.

Casino operators have taken note. Many have shored up their AML and compliance operations as well put restrictions on money transfers and check cashing. That may not be enough. Accountability is trickling down to focus on individual customers.

Industry analysts believe Shasky Calvery's speech portends a new ruling from the U.S. Treasury Department that would require casinos to vet the source of their high rollers' funds rather than just report suspicious activity, as per current regulations. This could be a real game changer - no pun intended.

Casinos compete to attract "whales," those very profitable high rollers. Regulations requiring casinos to pry into the source of a whale's funds could alienate a casino's best customers as well as jeopardize the casino's profits and tarnish its reputation. However, given the rumblings in the industry, casino operators need to be prepared for stricter regulations. The ability to identify Reputationally Exposed Persons (REPs) found in adverse media could help casinos - as well as other organizations -- expose high-risk customers and meet compliance obligations. Contact SBS to learn more.

Five Downstream Impacts of the New Vendor Guidance

Financial institutions outsource myriad operations and core banking functions to third parties to reduce costs and improve resource allocation. As these arrangements have increased, so has concern that "the quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity of these relationships." In response, the Federal Reserve and the Office of the Comptroller of the Currency issued new third-party risk management and outsourcing guidance.

The guidance broadens the scope of managing vendor relationships by requiring banks to clarify responsibility and better understand and assess outsourced risk. No doubt it will impact banks and vendors

alike. Five changes to expect:

- A narrower playing field - More stringent vendor management requirements will reduce the pool of qualified providers, forcing banks to consolidate outsourced activities to a handful of key third-party relationships. The more critical the function, the greater the risk of relying on one vendor and the more detailed the vetting process is expected to be. Banks should also take a holistic look at their operations to determine which processes are best outsourced and which should remain in house to balance risk management and cost efficiency.

- Risk managers get a say - Supplier assessment is no longer controlled exclusively by a financial institution's purchasing, vendor management or procurement group. There is a growing trend for risk managers to have more direct involvement with the vendor approval process.

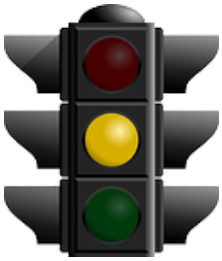
- Contracts are not sacrosanct - Financial institutions are revisiting contracts and requiring amendments that address the more stringent guidance for vendor management. Third-party providers who don't step up their game to meet these heightened requirements risk losing the relationship.

- Due diligence has an ongoing cost - The monetary cost to banks for the time and resources needed to more carefully vet third-party providers doesn't end when the contract is signed. Ongoing monitoring, oversight and reporting are expected throughout the life of the relationship. In spite of the additional costs, banks overall have welcomed the new guidance. It offers added protection to their business and their customers. More important, the cost of sloppy vendor management and its impact on risk (including operations, compliance and reputation risk) eclipses the cost of due diligence, making it just too great to ignore.

- Good guys don't always win - Banks are scrutinizing existing vendors to ensure heightened requirements for documentation, security, reporting, performance benchmarks and other criteria are met. In the end, a good relationship may need to be terminated if the vendor can't deliver - even if the relationship was solid and the product and service were excellent.

As with any regulatory change, the downstream impact of the third-party risk management and outsourcing guidance will continue to ripple through the industry for months to come.

Pot and Porn and Pawn - Oh My!



What do marijuana dispensaries, the adult entertainment industry and pawnbrokers have in common? They are all considered high-risk businesses in the eyes of financial institutions. That makes it difficult for legitimate operators in these industries to access capital, get a checking account or take advantage of other banking services.

Skittish from heightened regulatory compliance and hefty fines for lack of oversight, banks are reassessing customer risk and curtailing services to individuals and businesses that pose potential financial or reputational risk. Certain merchant categories, including drug paraphernalia, firearms sales, payday loans, pharmaceutical sales and pornography have been singled out. That has had significant repercussions for those industries.

JPMorgan Chase announced that it would curtail lending to pawn shops, payday lenders and other categories of legitimate, but high-risk businesses saying they are "risky to JPMorgan's reputation." And Chase, JPMorgan's consumer and commercial banking unit, made headlines by preemptively closing several accounts owned by customers identified as current and former porn stars.

While Chase's actions put them in the spotlight, declining to do business with any person or company deemed high risk is standard practice for financial institutions. Banks are not the only ones being cautious. PayPal, one of the world's largest payment processors, has an acceptable-use policy that bans transactions from adult businesses, legal medical marijuana providers and pawn shops - all of which they consider high risk. American Express and Discover have similar policies and won't allow customers to use an AmEx or Discover card to buy medical or recreational marijuana or to purchase online pornography.

Virtual currencies are another high-risk category that sends banks running for the hills. Just last month, National Australia Bank closed the accounts of digital currency providers stating they "pose an unacceptable level of risk, both to our business and reputation."

Restrictions from banks, payment processors, credit card companies and others have made it difficult on individuals and nearly impossible for upstanding, legal businesses in any of the high-risk areas to legitimize their operations. However, there is light ahead for some lucky high-risk categories. In February, the Treasury Department issued new rules that will make it easier for financial institutions to transact business with legal marijuana sellers (medical marijuana is legal in 22 states plus D.C. but is banned by federal law). Visa and MasterCard, who had previously canceled merchant agreements with medical marijuana providers, have recently loosened restrictions. They will now allow their cards to be used for legal marijuana purchases.

While the marijuana industry is making headway, other high-risk categories continue to struggle for access to financial services. At the same time, they present a conundrum for banks. Institutions that preemptively close all accounts or block business from a particular risk category may be sacrificing profit unnecessarily. With better information for assessing reputational risk, institutions can focus on entities and individuals that present the greatest risk rather than implement an across-the-board block of financial services to reputable customers just because they are in a high-risk category.

Learn how identifying Reputationally Exposed Persons (REPs) found in adverse media can help your organization make more informed decisions regarding existing and potential customers.

Case Study: Bringing Automated and Consistent Customer Due Diligence to Sterling National Bank

Sterling National Bank's legacy systems and labor-intensive processes needed to be replaced with robust technology that would streamline workflow, better identify risk and scale to accommodate growth while meeting regulatory requirements. The bank was able to achieve its goals by implementing SAFE Advanced Solutions®, SBS' integrated suite of software and services for list management, entity resolution, research, investigation and reporting.
Read more.

Highlights of the AML & Financial Crime Conference in Toronto

Approximately three hundred anti-money laundering and compliance professionals converged in Toronto June 9-10 to attend the ACAMS 2nd Annual AML & Financial Crime Conference. An impressive roster of speakers presented current AML topics such as risk assessments, data analytics and customer privacy; virtual currency and cyber fraud; and changing regulations. Using social media for interactive polling, attendees provided immediate feedback on issues under discussion for a real-time gauge of actual industry practices.

Of special note was the regulatory panel with Nicolas Burbridge, Senior Director of OSFI's AML and Compliance Division, Jamal El-Hindi, Associate Director of FinCEN's Policy Division and Bernard Gagne, Deputy Chief Compliance Officer in FINTRAC's Compliance Relations and Support. Recognizing that the U.S. and Canadian AML communities share common issues, ACAMS brought these three regulators together for the first time in a joint session.

The Canadian regulators spoke about Bill C31, which will require screening for domestic PEPs. The bill is not yet finalized but will clarify the definition of a domestic PEP and what the Canadian regulators will expect for group-wide compliance. Interactive polling on this topic indicated that slightly more than 60% of the audience were prepared to screen for domestic PEPs.

In order to reduce the impact of regulatory examinations on an institution, FINTRAC and OSFI conduct concurrent exams. However, each regulator approaches the exam with a different mandate. While FINTRAC focuses on reporting, OSFI's focus is on risk as stated in the Basel Committee's core principles. When asked how many in the audience would like FinCEN to participate in these concurrent exams, no hands were raised.

Risk assessments continue to draw the attention of all three regulators. The audience poll indicated that

67% use a manual process to assess risk while 33% have automated the process. Risk assessments continue to present problems for both Canadian and U.S. institutions, especially larger institutions with more complex products. All three regulators stressed that they are not necessarily looking for complicated processes but are expecting to see the identification of risk followed by enhanced due diligence.

Cross border electronic funds transfer was another common issue for both Canadian and U.S. institutions. The U.S. is currently evaluating Canadian rules as it formulates its own. Also discussed was the leveraging of data analytics to fine tune transaction monitoring. The panel of regulators all agreed that data analytics should be part of a strategic approach to turn data into information. Audience polling indicated that organizations are using data or data analytics in several areas of operations including OFAC/customer screening, transaction monitoring and risk assessments.

Information sharing was a common thread that ranked high on everyone's priorities. The industry continues to press for a broadening of information sharing within and among organizations despite the barriers presented by data privacy issues. FinCEN, for example, said that they are looking to make it easier to share SARs.

The quality of the speakers and presentations, relevance of topics and range of industry practitioners all helped to make the conference a big success. SBS would like to extend its thanks to ACAMS as well as to all the attendees who stopped by our table at the show.

About Safe Banking Systems

For more than 15 years, Safe Banking Systems, a technology enabled company, has been thinking ahead of the risks to combat financial crime and find the "bad guys." SBS' anti-money laundering and compliance solutions solve key Know Your Customer, Customer Due Diligence and Enhanced Due Diligence issues. These solutions provide financial and other institutions with a holistic framework for managing enterprise-wide risk in a data driven environment. SBS' flagship offering, SAFE Advanced Solutions®, combines a patented risk ranking methodology with a probability scoring model to bring actionable intelligence for entity resolution to clients worldwide. For more information, visit www.safe-banking.com.

View our profile on LinkedIn

Case Studies **Upcoming Events** **White Papers**