Managing Regulatory Compliance and AML Risk in a Virtual Currency World

Issue

When you first think of virtual currency (also known as digital currency), the video gaming industry may be what first comes to mind. The reality is, though, that virtual currency has value beyond the virtual world. A proliferation in recent years of different types of virtual currencies (see figure below for types of virtual currencies) has led to growing risks in the areas of financial crime, regulation and information technology.

Virtual currencies, which are alternative currencies, exist in digital form and are not regulated like e-money, which is simply traditional currency exchanged electronically. However, regulatory expectations and guidance on risk management of virtual currencies are starting to emerge, and failing to meet these expectations may have serious consequences, including potential civil and criminal penalties if money is laundered through the virtual currency system.

Virtual currencies have increasingly received attention from governmental and regulatory bodies. China, for instance, prohibits the use of virtual currency to purchase real products, and the Financial Action Task Force (FATF) has issued reports regarding the use of virtual currencies and other new payment methods in money laundering. In more recent news, a U.S. federal agency seized the bank account of a virtual currency exchanger. These funds were maintained by an online payment provider.

---

1 The European Central Bank’s report, “Virtual Currency Schemes,” issued in October 2012, identified three types of virtual currencies based on observed characteristics. These classifications may become outdated as the virtual currency system characteristics may evolve.
Companies and individuals dealing with virtual currencies have two key questions to consider: Am I a money services business (MSB)? And if so, what do I need to do to comply with AML requirements?

Recently, the U.S. Financial Crimes Enforcement Network (FinCEN) issued guidance on virtual currency in the context of the Bank Secrecy Act (BSA) and AML laws and regulations. As of March 18, 2013, FinCEN requires certain people and entities that deal with virtual currencies to register as an MSB and comply with relevant BSA regulations. The guidance also identifies three groups involved in a virtual currency system – user, exchanger and administrator – and defines them as follows:

- **User** – A person that obtains virtual currency to purchase goods or services;
- **Exchanger** – A person engaged as a business in the exchange of virtual currency for real currency, funds or other virtual currency; and
- **Administrator** – A person engaged as a business in issuing (putting into circulation) a virtual currency and who has the authority to redeem (withdrawing from circulation) such virtual currency.

Under FinCEN guidance, convertible virtual currency administrators and exchangers that accept and transmit a convertible virtual currency or buy or sell convertible virtual currency for any reason are money transmitters and are required to comply with the laws and regulations pertaining to MSBs, unless one of six exemptions applies.

Given the lack of historical regulatory oversight, these virtual currency MSBs may not have the depth of experience when dealing with the BSA requirements and developing and implementing an AML program.

**Challenges and Opportunities**

Virtual currency MSBs have a unique set of regulatory requirements that transcend AML compliance. Regulatory requirements for cross-border operations and AML programs and technology systems are among a number of key risks that MSBs need to understand in order to manage the regulatory environment effectively. Key challenges and opportunities include:

**Cross-Border Operations**

*Ease of funds movement* – The ease of transferring virtual currency across borders with anonymity presents companies with the challenge of tracking and tracing suspicious activities associated with crime. Nevertheless, companies can establish a strong understanding of customer behavior and transactions that can be used as key performance or risk indicators and can provide meaningful customer analytics.

*Data privacy* – Since customer information must be maintained and stored as part of the BSA requirements, a virtual currency MSB must understand, apply and then meet multifaceted country requirements from a data privacy perspective. This adds additional complexity to business operations. A virtual currency MSB could take the opportunity to establish a leading program that understands and complies with regulatory requirements and provides the company with the ability to operate internationally with reduced regulatory risks.

---

2 A money services business is a type of business that provides various money-related services to its customers. This includes check cashing, wiring money through Western Union or bill payments. The United States Treasury Department defines an MSB more specifically in 31 C.F.R. § 1010.100(ff)(1-7).

3 FinCEN’s regulations define “person” as “an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities.” 31 C.F.R. § 1010.100(mm).

4 FIN-2013-G001.

5 31 C.F.R. § 1010.100(ff)(5)(ii)(A)–(F).
AML Program

AML compliance program – Virtual currency MSBs may not have an AML compliance program in place since they have not been regulated previously and there are no industry-leading practices pertaining to these virtual currencies and AML requirements. This could allow virtual currency MSBs to develop a program without legacy concerns or processes that can be modeled based on best practices and existing MSB AML programs.

Customer due diligence – Virtual currency MSBs may be required to collect certain identifying information. In the virtual world, anonymity is easily obtained with the use of avatars and public spaces. Additionally, the speed at which funds can be transferred across boundaries makes it difficult to identify the origin of the funds. Due to the online nature of the business, verification of the customer’s true identity presents a challenge. Collecting customer information will not only address some money laundering concerns, but also will provide companies with better data with which to perform risk assessments and to obtain a more accurate picture of their customer base and footprint, which could lead to improved business ideas and additional products to fit certain demographics, enhancing monitoring activities and other benefits to additional analytics.

Sanctions – Virtual currency MSBs need to establish a program to screen and stop transactions with sanctioned countries and individuals. This proves more difficult in practice, as user information may be limited or inaccurate and companies may not have control over where customers redeem their virtual currency. Developing controls, as mentioned above, to collect customer information upfront will help virtual currency MSBs implement sound controls to prevent sanctioned entities and limit transactions with entities that have been sanctioned by government entities.

Training and awareness of risks – Staff who may not be aware of AML risks must be trained. A virtual currency MSB will need to provide AML training similar to the training provided by other MSBs. Providing training to staff will increase awareness of money laundering risks and decrease the risk of the company unknowingly facilitating money laundering. Establishing and strengthening controls based on best practices reduces the risk of civil and criminal repercussions.

Technology

System weaknesses – Buyers of virtual currencies often must create a unique online identity within the virtual currency system. While key to the virtual currency system, technology presents multiple challenges, including but not limited to system weaknesses whereby a user can artificially generate additional virtual currency, account takeovers, and users with out-of-date software that contains security gaps. Requiring valid user information during account setup and establishing a process for validation provide additional assurance that the virtual currency is being used legitimately, as fraudulent users cannot hide in anonymity.

Varying regulatory requirements – Countries may have different requirements around safeguarding customer information, including credit card information or other personal information that may be used in the process of purchasing virtual currency. These companies could use credit card information to collect customer information that may not be otherwise available in order to gain a better understanding of the customer profile.

Our Point of View

There are several considerations to take into account in order to establish an effective AML program. First, there needs to be a designated individual responsible for leading and maintaining the program and establishing a control framework. Companies that have developed a strong risk framework may be able to leverage their governance structure to address emerging risks from virtual currency and non-compliance with regulations, while newer companies may require more resources to establish the governance framework needed to develop an AML program. A virtual currency MSB should establish an overall governance risk and compliance structure, perform a risk assessment, develop a customer due diligence platform, ensure proper recordkeeping, monitor transactions for sanctions violations and suspicious activity, provide reporting to management, and provide training.
Following are key questions that virtual currency MSBs should ensure are addressed in order to meet regulatory requirements.

**Developing a Governance Risk & Compliance Framework**
- Have you developed a governance body for providing oversight that includes objective and strategy-setting, delegation of authority, and monitoring and evaluation that allows for executive management to set overall business objectives and oversee progress toward those objectives?
- Have you developed a governance body to manage risk by identifying, sourcing, measuring, mitigating and monitoring risk in order to minimize impacts of extreme events and taking risks that would increase enterprise value while still complying with requirements?
- Have you established a governance body to ensure compliance with internal policies, and also to ensure that your policies and procedures comply with applicable laws and regulations and are performing as intended?

**Developing a Risk Assessment**
- Have you performed a risk assessment of your business considering the following risk factors: type of virtual currency you offer (e.g., closed system currency, unidirectional currency or bidirectional currency), the volume and dollar amount of transactions, customer type, amount and validity of customer information, and location of services?
- How have you addressed potential sanction violations due to the anonymous nature of the virtual currency industry and the potential currency use within sanctioned countries?
- Is your risk assessment based on both quantitative and qualitative factors, with documentation to provide justification for your conclusions?
- Are the results of the risk assessment used to establish adequate governance and internal controls to reduce the identified money laundering risks?

**Performing Customer Due Diligence**
- Do you collect and validate customer information commensurate with the risks identified in your risk assessment?
- Do you screen your new customers to ensure compliance with sanctions?
- Are your controls sufficient to protect sensitive customer information?

**Ensuring Record Retention**
- Do you know the record retention requirements for customer and transactional information in all the countries where you are regulated?

**Conducting Monitoring, Screening and Reporting**
- Do you understand what an average customer transaction looks like?
- Have you developed controls to monitor transactions and identify unusual activity?
- Do you have the right individuals with sufficient transaction knowledge to monitor these transactions and do the review results reach the right individuals and management?
- Do you perform customer or transaction monitoring to ensure compliance with sanctions requirements?
- Is suspicious activity being reported to the correct regulatory agencies in a timely manner?

**Providing Training**
- Do your employees, either internally or at retail locations, know the indicators for money laundering and do they know what to do when they identify this activity?
In addition to regulatory requirements for virtual currency MSBs, other financial institutions, such as banks, must also consider how to manage money laundering risks regarding their relationships with customers engaged in virtual currency. Protiviti will discuss financial institution considerations in a subsequent document.

**How We Help Companies Succeed**

Protiviti’s professionals can help your company achieve compliance and reduce risks of operating as a virtual currency MSB. Our integrated teams can review both compliance and regulatory concerns and also assess and address IT risks. Protiviti has unique skill sets and expertise to help clients deal with the risks associated with the digitization of real world money, proliferation of virtual currencies and regulatory expectations for MSBs.

**Example 1**

We were engaged by a global payment processor, which was newly registered as an MSB with FinCEN and expecting a review by its regulator, to review its AML compliance program. The purpose of the review was to identify any gaps and assist with remediating these gaps to develop a comprehensive AML program that met both U.S. and European regulatory expectations. Our review encompassed risk assessments, policies and procedures, organizational structure and staffing, transaction monitoring systems, customer due diligence, and the scope of audits and other independent reviews. We identified gaps in the global payment processor’s program based on regulatory expectations and leading industry practices. We then developed an executable project plan and framework to strengthen the AML compliance program. This included enhancing the company’s AML risk assessment, its policies and procedures, monitoring rules, and audit program. As a result, our client was able to put into place a robust AML compliance program to help prevent and detect suspicious activity, which led to a successful review by its regulator.

**Example 2**

We assisted a global company by identifying BSA/AML and Office of Foreign Assets Control (OFAC) risks within the organization’s global online gaming business, and also assisted in developing detailed BSA/AML and OFAC procedures. During the course of this project, we identified risks associated with the purchases of pre-paid cards, transactions within OFAC-sanctioned countries, and the potential for the product to be used in money laundering schemes. We coordinated with our client’s AML compliance officer and associate general counsel to understand the practices currently in place, and developed policies and procedures to remediate control gaps, thereby enhancing management’s ability to implement a strong program to meet regulatory expectations.
About Protiviti Inc.

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

Carol Beaumier
Managing Director
+1.212.603.8337
carol.beaumier@protiviti.com

Bernadine Reese
Managing Director
+44.20.7024.7589
bernadine.reese@protiviti.co.uk

Ricci Franklin
Associate Director
+1.213.327.1440
ricci.franklin@protiviti.com

Luis Canelon
Senior Manager
+44.20.7024.7509
luis.canelon@protiviti.co.uk

Amy Cho
Manager
+1.212.603.8340
amy.cho@protiviti.com

Andrew Paw
Manager
+44.20.7024.7571
andrew.paw@protiviti.co.uk