RGS GLOBAL ADVISORS
1441 Broadway, Suite 6057, New York, NY 10018
390 North Orange Avenue, Suite 2300, Orlando, FL 32801

FinCEN's Advisory on Illicit Activity Involving Convertible Virtual Currencies

May 2019

The Financial Crimes Enforcement Network (FinCEN) realizing the risks posed by Virtual Currencies issued an advisory (FIN-2019-A0003) earlier this month, cautioning the financial institutions to the heightened risks posed by criminals, who continue to exploit Virtual Currency for supporting their illegal activities and for laundering money. This activity endangers U.S. national security and the FinCEN's advisory is aimed at assisting financial institutions in identifying and reporting suspicious activity relating to Virtual Currencies (VCs), particularly Convertible Virtual Currencies (CVCs) involving darknet marketplaces, peer-to-peer exchangers, foreign Money Service Businesses (MSBs), and CVC kiosks.

While financial institutions are required to maintain their anti-money laundering/countering the financing of terrorism (AML/CFT) programs, FinCEN reminds the financial institutions that persons accepting and transmitting CVC are required to comply with anti-money laundering/countering the financing of terrorism (AML/CFT) program, recordkeeping, and reporting requirements. FinCEN's guidance regarding Application of FinCEN's Regulations to Businesses Involving CVCs (FinCEN-2019-G001) also clarifies various regulatory obligations, including registration, for persons deemed to be money transmitters.

Why is it important to understand risks related to Virtual Currencies and implement controls?

According to FinCEN, its analysis of BSA and other data have revealed that illicit actors have been using CVCs to facilitate criminal activity such as human trafficking, child exploitation, fraud, extortion, cybercrime, drug trafficking, money laundering, terrorist financing, and to support rogue regimes and facilitate sanctions evasion. Additionally, cyber intrusions are targeting legitimate users and financial intermediaries with an aim of stealing CVC, which has become one of the principal payment and money transmission methods in online darknet marketplaces that facilitate the cybercrime economy.

FinCEN's advisory explains the risks, includes typologies and red flags – all aimed at enabling the financial institutions in identifying unusual activities, that are observable either during routine screening and/or during transaction reviews.

What should the financial institutions do?

- ✓ Ensure that they do not engage in transactions prohibited by OFAC.
- ✓ Understand the red flags and evaluate their risks related to VCs.
- ✓ Implement monitoring and screening processes that would enable them in identifying unusual or suspicious activities using VCs.
- ✓ Provide training to appropriate personnel regarding identification of unusual activities involving VCs.
- ✓ Provide training to their personnel involved in preparing and/or reviewing Suspicious Activity Reports (SARs), so that they can identify all relevant information that is required to be included on SARs for making them useful to law enforcement.

RGS Global Advisors is a leading cost-effective provider of Internal Audit, Risk Management, Cybersecurity, and BSA/AML/OFAC Compliance Consultancy services to Financial Institutions.

For further guidance or assistance contact us at: info@RGSGlobalAdvisors.com