GAO Highlights

Highlights of GAO-14-496, a report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate

May 2014

VIRTUAL CURRENCIES

Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges

Why GAO Did This Study

Virtual currencies—digital representations of value that are not government-issued—have grown in popularity in recent years. Some virtual currencies can be used to buy real goods and services and exchanged for dollars or other currencies. One example of these is bitcoin, which was developed in 2009. Bitcoin and similar virtual currency systems operate over the Internet and use computer protocols and encryption to conduct and verify transactions. While these virtual currency systems offer some benefits, they also pose risks. For example, they have been associated with illicit activity and security breaches, raising possible regulatory, law enforcement, and consumer protection issues. GAO was asked to examine federal policy and interagency collaboration issues concerning virtual currencies.

This report discusses (1) federal financial regulatory and law enforcement agency responsibilities related to the use of virtual currencies and associated challenges and (2) actions and collaborative efforts the agencies have undertaken regarding virtual currencies. To address these objectives, GAO reviewed federal laws and regulations, academic and industry research, and agency documents; and interviewed federal agency officials, researchers, and industry groups.

What GAO Recommends

GAO recommends that CFPB take steps to identify and participate in pertinent interagency working groups addressing virtual currencies, in coordination with other participating agencies. CFPB concurred with this recommendation.

View GAO-14-496. For more information, contact Lawrance L. Evans, Jr. at (202) 512-8678 or evansl@gao.gov.

What GAO Found

Virtual currencies are financial innovations that pose emerging challenges to federal financial regulatory and law enforcement agencies in carrying out their responsibilities, as the following examples illustrate:

- Virtual currency systems may provide greater anonymity than traditional payment systems and sometimes lack a central intermediary to maintain transaction information. As a result, financial regulators and law enforcement agencies may find it difficult to detect money laundering and other crimes involving virtual currencies.
- Many virtual currency systems can be accessed globally to make payments and transfer funds across borders. Consequently, law enforcement agencies investigating and prosecuting crimes that involve virtual currencies may have to rely upon cooperation from international partners who may operate under different regulatory and legal regimes.
- The emergence of virtual currencies has raised a number of consumer and investor protection issues. These include the reported loss of consumer funds maintained by bitcoin exchanges, volatility in bitcoin prices, and the development of virtual-currency-based investment products. For example, in February 2014, a Tokyo-based bitcoin exchange called Mt. Gox filed for bankruptcy after reporting that it had lost more than $460 million.

Federal financial regulatory and law enforcement agencies have taken a number of actions regarding virtual currencies. In March 2013, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued guidance that clarified which participants in virtual currency systems are subject to anti-money-laundering requirements and required virtual currency exchanges to register with FinCEN. Additionally, financial regulators have taken some actions regarding anti-money-laundering compliance and investor protection. For example, in July 2013, the Securities and Exchange Commission (SEC) charged an individual and his company with defrauding investors through a bitcoin-based investment scheme. Further, law enforcement agencies have taken actions against parties alleged to have used virtual currencies to facilitate money laundering or other crimes. For example, in October 2013, multiple agencies worked together to shut down Silk Road, an online marketplace where users paid for illegal goods and services with bitcoins.

Federal agencies also have begun to collaborate on virtual currency issues through informal discussions and interagency working groups primarily concerned with money laundering and other law enforcement matters. However, these working groups have not focused on emerging consumer protection issues, and the Consumer Financial Protection Bureau (CFPB)—whose responsibilities include providing consumers with information to make responsible decisions about financial transactions—has generally not participated in these groups. Therefore, interagency efforts related to virtual currencies may not be consistent with key practices that can benefit interagency collaboration, such as including all relevant participants to ensure they contribute to the outcomes of the effort. As a result, future interagency efforts may not be in a position to address consumer risks associated with virtual currencies in the most timely and effective manner.