Client Alert

August 3, 2015

DOJ's Recent Guidance On Compliance For Virtual Currency Businesses

By Eugene Illovsky

What compliance expectations does the Department of Justice have for businesses entering the virtual currency space? How can a company meet those expectations to stay out of trouble with DOJ, or at least mitigate the effects of any criminal inquiry on it as well as its executives, employees, and investors? A recent speech by the Criminal Division head, Assistant Attorney General Leslie Caldwell, provides critical guidance on DOJ's "approach to the emerging virtual currency landscape" and expands on its view that "compliance and cooperation from exchanges, companies and other market actors can ensure that emerging technologies are not misused to fund and facilitate illicit activities."[1]

DOJ'S VIEW OF HOW VIRTUAL CURRENCIES ARE USED

DOJ is skeptical. While it knows virtual currency has "many legitimate actual and potential uses," its enforcement stance is informed by the observation that "the inherent features of virtual currencies are exactly what make them attractive to criminals."[2] For instance, virtual currency systems "conduct transfers quickly, securely, and with a perceived level of anonymity," have an "irreversibility of payments made in virtual currency and lack of oversight by a central financial authority" and the "ability to conduct international peer-to-peer transactions that lack immediately available personally identifiable information.

Virtual currency thus "facilitates a wide range of traditional criminal activities as well as sophisticated cybercrime schemes."[3] For instance, "online black markets" on the dark web offer a "wide selection of illicit goods and services" paid for in virtual currency, including "more traditional crimes such as narcotics trafficking, stolen credit card information, and hit-men for hire." But there has also been "a significant evolution in criminal activity." Virtual currency has funded "the production of child exploitation material through online crowd-sourcing." It has been used to "buy and sell lethal toxins over the internet," to make payments in "virtual kidnapping and extortion," and to allow "near-instantaneous transactions across the globe between perpetrators of phishing and hacking schemes and their victims."

VIRTUAL CURRENCY BUSINESSES AS FINANCIAL SYSTEM GATEKEEPERS

DOJ views these issues as a relatively small-scale problem now, because "[f]ew virtual systems currently can accommodate" the sort of "large-scale money laundering schemes involving government-issued currency." But

[1] Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the ABA's National Institute on Bitcoin and Other Digital Currencies in Washington D.C. on June 26, 2015 ("June 26 speech").

[2] June 26 speech.

[3] June 26 speech.

"as virtual currencies become more mature and better understood by criminals," DOJ expects "an increase in both individualized criminal activity and large-scale money laundering enterprises."[4]

This means "companies and individuals operating in the virtual currency ecosystem are at a crossroads." This is their chance "to help virtual currency emerge from its association with criminal activities." But in order to "ensure the integrity of this ecosystem and prevent its penetration by crime, the industry must raise the level of its game on the compliance front."

The government is thus enlisting this emerging business community as financial system gatekeepers. DOJ often notes that the country's banks "are our first line of defense against fraud, money laundering, terrorism financing and violations of sanctions laws."[5] It expects nothing less here: "[v]irtual currency exchangers and other marketplace actors comprise the front line of defense against money laundering and financial crime."[6]

And DOJ is not kidding. AAG Caldwell bluntly says, "industry participants are now on notice that criminals . . . make regular use of" virtual currencies. Robust compliance programs in virtual currency businesses are thus "essential to keeping crime out of our financial system." At a minimum, raising "the level of its game" will require the industry to exhibit "strict compliance with money services business regulations and anti-money laundering statutes."

THE COSTS OF COMPLIANCE—AND OF NONCOMPLIANCE

DOJ expects virtual currency businesses "to take compliance risk as seriously as they take other business risk." And they must think about compliance broadly. On other occasions, AAG Caldwell has noted that compliance efforts "are too often behind the curve" and fail to "prevent tomorrow's scandals" because they "target the risk of regulatory or law enforcement exposure of institutional and employee misconduct, rather than the risk of the misconduct itself."[7] DOJ wants the focus to be on the broader "compliance risk" and not the narrower regulatory risk.

What about the cost? DOJ "recognize[s] that new entrants in emerging fields may find that compliance requires a significant expenditure of resources" and promises to be "context-specific" in analyzing the adequacy of compliance frameworks.[8] Nevertheless, "a real commitment to compliance is a must, particularly given the significant risks in the virtual currency market." The bottom line: "[i]n the long run, investment in effective compliance programs will be well worth it, especially in the event a company has to interact with law enforcement."

---

[4] June 26 speech.

[5] Assistant Attorney General Leslie R. Caldwell Speaks at Treasury Roundtable on Financial Access for Money Service Businesses in Washington D.C. on January 13, 2015 ("[f]inancial institutions that have money services businesses as customers have a particular responsibility to be attuned to the risks involved and not turn a blind eye to suspicious conduct").

[6] June 26 speech.

[7] Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the Compliance Week Conference in Washington D.C. on May 19, 2015.

[8] June 26 speech.

That "interaction" with law enforcement may well involve DOJ deciding whether to indict a company (and individuals) or give it some kind of break. As AAG Caldwell says, "[i]f a money services business finds itself subject to a criminal investigation," DOJ will look to the so-called Filip factors in its Principles of Prosecution of Business Organizations. In particular, it will examine "the existence of an effective and well-designed compliance program" (Filip factor 5) and "a company's remedial actions, including steps to improve upon an existing compliance program" (Filip factor 6).

As for Filip factor 5, "effective anti-money laundering and other compliance programs must be tailored to meet the circumstances, size, structure, and risks encountered" by the business. For instance, "virtual currencies, with their perceived anonymity, pose risks that money transmitters such as Western Union do not face." The risks in the virtual currency arena may be difficult to deal with, but DOJ's view is simple: "Industry participants must address those risks, even when it may be costly to do so." Filip factor 6 requires that a company fix a problem if one occurs. That means not only that it must patch any hole in the compliance program, but also "replace responsible management," "discipline or terminate wrongdoers," "pay restitution," and "cooperate with the relevant government agencies."[9]

RECOMMENDATIONS

Here are some specific steps for emerging virtual currency businesses to consider when ensuring their compliance efforts align with DOJ's guidance and expectations:

It's Never Too Early. Anticipate compliance issues as soon as possible in the company's lifecycle. Develop a compliance system at the same time that you are refining your product or service (and well before you interact with customers).

People, People, People. It's hard to understand cryptocurrencies, and even harder to explain them well to skeptical law enforcement personnel. Make excellent compliance people part of your initial team and include them in important decision-making.

Money, Money, Money. There must be the financial commitment to compliance that is required in this industry space. While DOJ seems sympathetic to the "significant expenditure of resources," it will not likely go easy on those whom it concludes have skimped.

Think About the Technology's Regulatory Future. The technology of, and related to, your virtual currency will shape the government's expectations. Take bitcoins for example. Unlike dollar bills, say, every bitcoin carries its own transaction history. The block chain is a public ledger of all bitcoin transactions. And new products are being refined that can analyze that block chain and seek to determine every place a bitcoin has been and perhaps even who transferred or held it. It may become possible to give bitcoins a risk score, since those of suspicious provenance (for instance, those having once been through a mixer or in a dark wallet) could be separated from those that are squeaky clean.

[9] Principles of Prosecution of Business Organizations.

Instill a High-Integrity Culture Now for the Company You Will Become. The government has high expectations for those it views as running "gatekeeper" businesses. The regulatory bar is bound to get even higher as large banks and financial institutions—with their established and highly professional compliance staffs—develop their own virtual currencies. As "gatekeeper" businesses grow, they face pressures to be "ethical" and not simply to meet legal and regulatory minimums. Adopt a broad view of compliance risk that focuses on the risk of misconduct and on reputational risk and then communicate that view clearly and compellingly in the onboarding process.

CONCLUSION

Emerging virtual currency businesses will face progressively higher compliance expectations from DOJ. They can maximize their potential market value by acting early in their lifecycles to install compliance systems and instill a high-integrity culture that will enable them to meet those expectations.

Contact:

Eugene Illovsky
(650) 813-5818
eillovsky@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.