Schnader
ATTORNEYS AT LAW

Schnader Harrison Segal & Lewis LLP

CALIFORNIA DELAWARE JAKARTA* NEW JERSEY NEW YORK PENNSYLVANIA WASHINGTON, D.C.

CRIMINAL DEFENSE AND INTERNAL INVESTIGATIONS ALERT

OCTOBER 2018

HOW BUSINESSES CAN DEAL WITH CRYPTOCURRENCY RISKS

By Danielle T. Bruno and Laurel Gift

How can businesses safely utilize blockchain technology and cryptocurrency, while avoiding potential cyberattacks, criminal activity, regulatory violations and financial losses? The news headlines could scare any business leader away from utilizing distributed ledger systems. Reports of theft, fraud, tax evasion, criminal convictions and government fines related to these technologies may discourage companies from pursuing the opportunities presented by blockchain and cryptocurrencies.

Given the general consensus that blockchain presents significant advancements and future benefits among many different industries, companies must find ways to overcome the range of challenges in order to engage and profit from the new technology. These systems are driving innovation and revolutionizing the fields of logistics, supply-chain management, data security and many other areas of commerce. Large online retailers now accept virtual currency as payment, including Microsoft, Overstock and Expedia. Government agencies at the federal and state levels have launched programs both to encourage these innovations and regulate against misconduct and abuses. Thus, businesses that are unable to adjust may miss out on the opportunities and growth offered by these innovative technologies.

Businesses need to effectively evaluate and manage the risks associated with blockchain. Cryptocurrency, in particular, requires a cautious approach, informed decision making and attention to detail. Businesses can deal with most of these risks and uncertainties by following many of the same best practices they commonly employ throughout their operations for research, documentation, compliance, training and contracting. This article identifies various ways businesses can manage cryptocurrency risks while still engaging in the innovation and advantages these technologies offer.

Do Your Homework

Blockchain and cryptocurrency may sound somewhat mysterious, but business leaders must devote time to learn about these fields. Do your homework to fully protect business interests. Be acutely aware of the risks and opportunities.

When considering investing in or accepting cryptocurrency as a method of payment, learn about the options for storing virtual currency. Recognize that since cryptocurrencies are not backed by a centralized government or government agency, there are no underlying protections for investors in the event of fraud, theft, or a breach of security by hackers.

If planning to rely on a cryptocurrency exchange, learn about its operations and inquire as to what that platform has done to secure accounts and prevent cyberattacks. Find out whether an exchange has been the subject of a hack in the

past, and if so, how it responded to prevent similar issues from occurring in the future. Many experts argue that "end to end" wallets – meaning wallets that exchange from party A to party B directly without the use of an exchange or other third-party service – may be the safest way to ensure that funds will be protected. There have been instances of fraud by the exchanges themselves, and a still-evolving regulatory environment means it could be difficult to retrieve investments if an exchange holds your funds hostage. However, due to the relatively early stage of the technology, new approaches are constantly being developed, as well as services that provide more security for users.

The 2014 hack of Mt. Gox provides a cautionary example. Mt. Gox was one of the world's largest Bitcoin exchanges at the time. The exchange alleged that approximately 850,000 Bitcoins were stolen by online hackers, leading to Mt. Gox filing for bankruptcy in Japan where the exchange was headquartered. Tech-gurus have argued that Mt. Gox was not fully prepared for cyberattacks, citing insufficient security infrastructure, sub-par accounting protocols and weak protections on "transaction malleability" (which is a technical description of the way that transactions between users are exchanged and recorded, in the simplest terms). However, Mt. Gox was not an isolated event. In 2016, Bitfinex (another large exchange) was hacked for approximately $66 million worth of Bitcoin in a cyberattack. Some of the funds subject to these attacks still have not been recovered.

Use Customary Effective Business Practices

The innovations presented by blockchain technology and cryptocurrency should not lead companies to forgo the best operational practices they utilize in other aspects of their business. In fact, exploring these new technologies presents an opportunity for businesses to review and strengthen their current policies and practices.

Extra vigilance is appropriate due to the uncertainties presented by distributed ledger technologies. Business leaders should demand high levels of research, investigation, documentation, security and ongoing monitoring, both for their own operations and for business partners. Hire, train and support highly trusted and knowledgeable professionals to manage and implement new initiatives. Develop and implement comprehensive internal operating procedures, compliance systems and contracting protocols. Trusted and independent legal counsel can play a key role.

Close attention to effective business practices is especially important due to the unfortunate fact that criminal actors have used blockchain and cryptocurrency vulnerabilities to target both individuals and entire businesses. These crimes have ranged from large scale trafficking and money laundering to crimes targeting specific individuals and businesses. For example, a criminal complaint filed by the New York City District Attorney's office at the end of 2017 details a targeted robbery that occurred in New York City, where the victim had invested early in Ether, and experienced his small investment grow to over 1.8 million dollars worth of the cryptocurrency. The victim was allegedly set up by a friend who told the victim he had purchased an uber to take him home, only to be robbed and kidnapped when entering the vehicle. When the victim went home, the USB drive required to access his Ether fortunes was stolen, along with a hidden piece of paper containing the 24-digit security passphrase that was used to protect the funds. The funds were almost immediately transferred out of the victim's account, about half of which have not been located. This individual could have easily been an employee in your business, handling similar sensitive materials essential to protecting your assets or investments.

This is just one example of the types of crime associated with cryptocurrency. There have been instances of hackers holding entire network systems hostage and demanding immediate anonymous cryptocurrency payments in exchange for the release of the company's system. Trafficking and money laundering are now widely associated with cryptocurrencies. The U.S. Justice Department and other federal and state agencies have also investigated, prosecuted and fined businesses for criminal activity and regulatory violations. In order to ensure that your business is

not flagged for potential criminal activity, it is essential to understand what prosecutorial offices are tracking, and how your company could potentially be linked to these problems.

Consult with Legal and Technology Experts

Legal professionals and technology consultants can help companies to identify risks, recognize options to protect business interests and assets, and make practical plans for what will work best over time. Having access to experts can accelerate the learning curve and guide business leaders through operational and regulatory hurdles. In the event of problems, legal and tech consultants are essential for minimizing damage to the business and implementing internal reforms needed to prevent future setbacks. Planning ahead can save time, money and reputation, but waiting for an issue to arise can be a disastrous mistake.

Make Plans for Dealing with Ongoing Innovation and Regulatory Uncertainty

The pioneering nature of blockchain technology and cryptocurrency means there will be some rough patches and unexpected developments. Businesses taking the precautionary steps described above will be positioned to deal with these risks, which is especially important for those planning to become involved with cryptocurrencies.

Business leaders should stay educated and up-to-date on developments in the field. Stay current on the state of government regulation. Perform periodic internal audits to ensure compliance and identify needed improvements in systems and training. Work with informed legal counsel and technology experts.

The regulatory environment presents an area of particular uncertainty. Government agencies are just beginning to more fully engage in oversight of blockchain and cryptocurrency operations. For example, companies must be aware of Internal Revenue Service policies raising a variety of business concerns:

- A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property.
- The character of gain or loss from the sale or exchange of virtual currency depends on whether the virtual currency is a capital asset in the hands of the taxpayer.
- Payments using virtual currency made to independent contractors and other service providers are taxable and self-employment tax rules generally apply. Normally, payers must issue Form 1099.
- Wages paid to employees using virtual currency are taxable to the employee, must be reported by an employer on a Form W-2, and are subject to federal income tax withholding and payroll taxes.

Additionally, many countries have begun to regulate ICOs (initial coin offerings), and each locale may treat cryptocurrencies differently. There is no uniformity of approach, so familiarity with how a country regulates cryptocurrencies is important to meeting business objectives while reducing risk.

The Main Takeaway: Careful Attention and Planning Are Key

As with many new technologies, the risks may be great, but so can be the rewards. In order for investors and business leaders to take advantage of the potential of blockchain technology and cryptocurrency, internal operating procedures, security and reliance on trusted professionals are required to reduce risk. Additionally, a willingness to learn about the technology and stay up to date on the different progressions (and set-backs) are necessary for security and staying in front of developments in the field. These revolutionary advancements will unquestionably change the face of many industries. But it's clear that all the kinks haven't been worked out quite yet.◆

obtain professional legal advice before taking any legal action.

For more information about these issues or to speak with a member of the firm, please contact:

Laurel Gift
Chair of Schnader's Criminal Defense and Internal Investigations Practice Group
412-577-5115
lgift@schnader.com

Danielle T. Bruno
Associate
412-577-5221
dbruno@schnader.com

** See: www.schnader.com/jakarta*