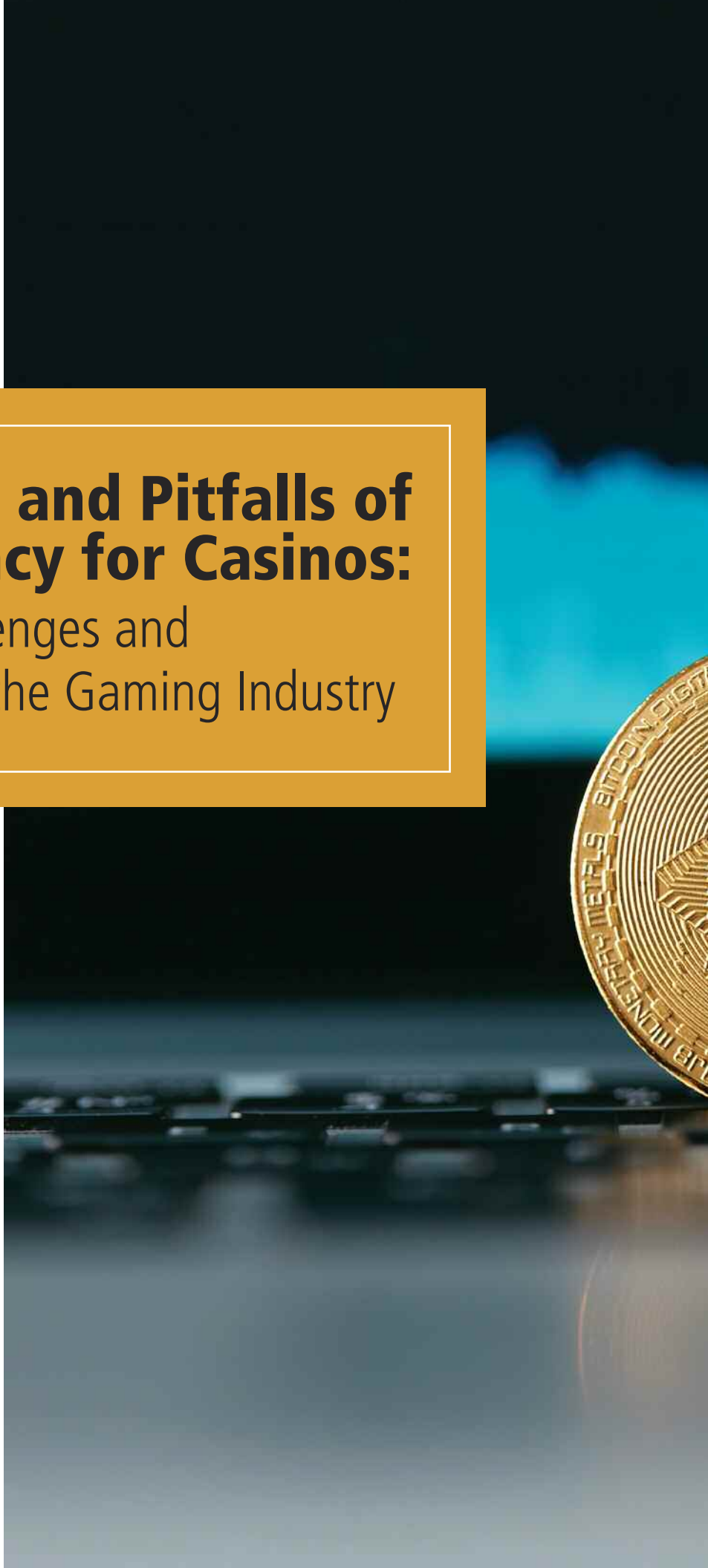
The Promises and Pitfalls of Cryptocurrency for Casinos:

Compliance Challenges and Opportunities for the Gaming Industry



By James F. Dowling, Gregory Lisa and Rebecca Umhofer

Over the past several years, the casino industry has experienced rapid growth and remarkable developments with new products, new marketing techniques, new approaches to payment, and innovation generally. Similarly, in the FinTech space, the cryptocurrency markets have increased dramatically in terms of adoption by customers, acceptance by financial institutions and other businesses, and overall market impact, footprint, and significance. Cryptocurrencies also facilitate more efficient payments and appeal to younger, more tech-savvy customers.

While the gaming and crypto industries are on their own parallel growth and innovation trajectories, there are inevitable intersections. As virtual currency customers and entrepreneurs consider how and whether to enter the casino industry, casinos themselves need to decide whether to incorporate cryptocurrencies into their business models--and if they do, they must address the compliance risks that follow.

In 2017, investment in initial coin offerings, or token sales exceeded $1.5 billion, a figure that does not capture Bitcoin, Ether, Litecoin, and over a thousand other cryptocurrencies. Within the last six months, the total cryptocurrency market cap has fluctuated between $250 and $500 billion; at its height, the total cryptocurrency market cap amounted to over $800 billion. The value of certain cryptocurrencies now exceeds that of several Fortune 50 companies and two of the world's largest futures exchanges, CBOE and CME, have launched Bitcoin futures contracts. Large banks that have been slow to embrace cryptocurrency due to concerns about fraud, volatility in the cryptomarkets, and regulatory uncertainty are now exploring how they can harness blockchain technology, which underlies cryptocurrencies, to make interbank settlements more efficient, more secure, and less expensive. Seven of the world's biggest banks—Barclays, Credit Suisse, Canadian Imperial Bank of Commerce, HSBC, MUFG, State Street, and UBS – are working towards these goals and envision a "utility settlement coin" that would be traded and verified electronically over a network of computers on a distributed ledger.[1]

Despite the growing appeal of cryptocurrencies and the blockchain technology they employ, law enforcement, regulators, established financial institutions, and the media continue to express concerns that cryptocurrencies may be used to facilitate criminal activities. These concerns relate to money laundering; tax evasion; sanctions evasion; the use of virtual currencies for transactions in drugs, weapons, and other contraband; and a host of other criminal activities that can be facilitated – or monetized—with potentially anonymous funds. Most recently, Special Counsel Mueller's indictment of twelve Russian intelligence officers noted that the defendants used Bitcoin to purchase infrastructure in furtherance of the alleged hacking. The director of Europol recently estimated that around 4% of all criminal proceeds in Europe (as much as $5.5 billion) is funneled through virtual currencies like Bitcoin—and he expects this figure to increase.[2] In July, Chairman Powell of the U.S. Federal Reserve testified before the House Financial Services Committee that "cryptocurrencies are great if you're trying to hide or launder your money."

Cryptocurrencies may be attractive to criminals for several key reasons: they can be traded quickly across national borders; their ubiquitous

nature allows them to be spent in various areas; and they are pseudo-anonymous or in some cases almost entirely anonymous. Anonymity is key to criminals engaged in money laundering who aim to avoid linking their identity to their financial transactions. Anonymity is also important to traders wishing to avoid international sanctions. In recognition of the latter, the U.S. Department of Treasury has recently announced that it may soon start adding cryptocurrency addresses to its sanctions lists.[3] Although these identified addresses will likely be quickly abandoned by individuals targeted with sanctions, a former Department of Treasury official explained that an identified digital address could be used to "build out the sanctioned person's network and potentially identify the new address that a sanctioned person is using."[4]

This may be particularly true for Bitcoin, the most frequently traded cryptocurrency. Although it has a reputation for anonymity, all Bitcoin transactions are publicly visible to anyone with internet access. This transparency actually provides more visibility into a Bitcoin trader's activities than is available for transactions in traditional currencies,[5] and law enforcement agencies have successfully analyzed the blockchain to track criminal activity and illicit money flows.[6]

Given the transparency of Bitcoin's ledger, criminals may prefer alternative cryptocurrencies such as Monero, Dash, and Zcash, which utilize ledgers that retain less traceable information and thus provide greater anonymity. Alternatively, they may utilize tumblers and other technologies to conceal and obscure transactions in virtual currency. Even if virtual currencies become more anonymous because their ledgers are less transparent than Bitcoin's, that anonymity is not complete because law enforcement agencies might still detect the eventual exchange of such cryptocurrencies once they are converted into fiat.[7]

Cryptocurrencies and Casinos' Compliance Operations

Despite these challenges, cryptocurrencies clearly have appeal to investors and others (including one of the authors of this article) who are not criminals, terrorist financiers, tax cheats, sanctions evaders, fraudsters, or Russian intelligence operatives.

As enforcement agencies begin to regulate cryptocurrencies' use, businesses such as banks, restaurants, and automobile dealerships are considering whether and how they should support cryptocurrency transactions. Many businesses, including those in the casino industry, aiming to increase their appeal with tech-savvy customers may find that accepting cryptocurrency is one way to do so. For instance, the D and Golden Gate hotels announced they will accept Bitcoin payments for dining, hotel reservations, and purchases made in their gift shops. Co-owner and CEO of those establishments, Derek Stevens, explained that he is "proud that the D and Golden Gate will be the first casino properties to accept Bitcoin. We're located in the growing high-tech sector of Downtown Las Vegas, and like all things Downtown, we're quickly adaptive to new technology."[8]

Certain foreign regulatory authorities, such as the Malta Gaming Authority, have expressed an interest and have solicited feedback as to whether cryptocurrencies should be accepted by their gaming licensees. Several gambling websites allow users to wager using Bitcoin, other cryptocurrencies, or specifically-designed tokens for gambling. But whether U.S. casinos will eventually be allowed to accept and redeem cryptocurrencies directly for gaming-related business—in other words, whether casinos will be authorized to permit gambling using cryptocurrency—will depend on

state gaming authorities (and, potentially, federal regulators). And once that happens, those arrangements will present their own sets of risks. In the meantime, even the proximity of cryptocurrency businesses, customers, and virtual-to-fiat currency exchanges may introduce a new set of compliance issues to financial institutions, including gaming institutions.

For decades, casinos have been considered "financial institutions" under the Bank Secrecy Act (BSA). As such, they must employ robust, risk-based anti-money laundering (AML) compliance programs designed to prevent transactions that involve proceeds of illegal or terrorist activities and transactions designed to finance such activities. Key components of a casino's AML compliance program are: a system of policies, procedures, and internal controls; a compliance officer to handle day-to-day compliance; independent testing of the program; training for appropriate employees; procedures to use all available information to determine and verify patron identification information, suspicious activity, and whether certain records must be made and maintained; and for those casinos that have automated data processing systems, use of such systems to aid in assuring compliance.

A casino's AML program serves several purposes, including informing its decisions about when it is necessary to file a suspicious activity report (SAR). The BSA requires that casinos file a SAR if the casino knows, suspects, or has reason to suspect that a transaction or attempted transaction (or a pattern of transactions) aggregating to $5,000 or more: (1) involves funds derived from illegal activity or is intended to disguise funds or assets derived from illegal activity; (2) is designed to avoid BSA reporting or recordkeeping requirements; (3) involves the use of the casino to facilitate criminal activity; (4) has no economic, business or apparent lawful purpose; or (5) is unusual for that particular patron and the casino knows of no reasonable explanation for the transaction.[9]

Multiple Bitcoin ATMs populate the Las Vegas strip and surrounding areas, including those within certain casinos. Several others have proliferated at or near other gaming institutions; and individuals across the country offer informal (though well-advertised) arrangements to convert cash to cryptocurrency and vice-versa through face-to-face meetings, through the mail, and over the internet. Thus, it is certainly possible for gamblers who arrive at casinos to gamble with cash recently converted from cryptocurrency, including funds converted overseas from an illicit source, which are then placed into a virtual currency e-wallet, and then quickly and efficiently reconverted to U.S. dollars.

For SAR monitoring and reporting purposes, casinos must conduct the same analysis regardless of whether a casino patron spends funds that came through a cryptocurrency account, his or her personal bank account, or some other source. Of course, the fact that a patron holds or has held and recently cashed out cryptocurrency does not in itself indicate that those funds were derived from illegal or terrorist activity. Casinos will have to look at numerous pieces of information to determine whether a particular patron's transactions raise red flags. Just as with cash, incoming wires, or any other form of payment, the fact that a patron is using funds that passed through a cryptocurrency account may be one component of this analysis. But conducting this analysis for such patrons may be uniquely challenging, because the source of funds that were at one time held in cryptocurrency may have become opaque because cryptocurrency transactions are not subject to traditional SAR methods of inquiry, analysis, and monitoring.

Casinos are not working alone to track the source of their patrons' funds when they pass through cryptocurrency exchanges. FinCEN made clear starting in 2013 that digital currency exchanges and administrators constitute money transmitters, a species of "money services businesses" (MSBs) under the BSA.[10] Check cashers, dealers in foreign exchange, prepaid access providers, and others are also MSBs. The BSA requires that all financial institutions (depository and non-depository institutions) comply with the general BSA regulations under Title 31, Section 1010. Casinos have additional regulatory requirements under Section 1021, while MSBs (including exchangers and administrators in virtual/cryptocurrency) have additional regulatory requirements under Section 1022. Although both MSBs and casinos (and card clubs) are types of financial institutions, the rules governing them are somewhat different (just as they are different for banks). By way of example:

- The AML program requirement for MSBs consists of four requirements, or "pillars" (namely, having policies and procedures, a compliance officer,

independent review, and appropriate training), while casinos have certain additional requirements;

- Although casinos have a SAR reporting threshold of $5,000, MSBs have a threshold of $2,000 (and some MSBs – notably, check cashers, are not required to file SARs);
- Most types of MSBs are required to register as such with FinCEN and failure to register may bring civil and criminal penalties.

How Can Casinos Embrace Cryptocurrencies?

Several casinos offer check-cashing, as well as credit card or debit card advances at their property. In many instances, casinos use third parties to manage these services while some smaller casinos offer their own check-cashing services. Under the federal regulations and guidance, casinos could offer their own cryptocurrency exchange under their casino license much as they do for traditional MSB services. However, casinos must still assess whether such practices are consistent with state licensing rules. Alternatively, casinos could contract with an external MSB who would facilitate a cryptocurrency exchange with casino patrons. Finally, casinos could arrange to use a Bitcoin Merchant Service Provider (BMSP) or similar cryptocurrency service provider to enable patrons to pay for goods and services in cryptocurrency. Risks and rewards attach to each approach.

If a casino accepts cryptocurrency directly, it must be prepared to address additional compliance considerations. The current BSA program would need to be retooled to include detailed procedures for the onboarding of customers and proper know-your-customer requirements. In addition, the casino's compliance team should consider potential source of funds issues, as well as enhanced due diligence surrounding any third-party payments. Depending on what services are offered, the introduction of cryptocurrencies at casinos also might draw the scrutiny of other regulatory agencies, including the Federal Trade Commission (FTC), the Internal Revenue Service (IRS), and state regulators.

The FTC has authority to prevent "unfair or deceptive acts or practices in or affecting commerce" and has made it clear that it will wield its authority to regulate cryptocurrency transactions.[11] The IRS also has issued guidance making it clear that for tax purposes, the IRS treats Bitcoin transactions as property transactions. Thus, businesses exchanging cryptocurrencies could be required to keep extensive records tracking the "basis" in the cryptocurrency to compute gains and losses. This tax treatment makes it impractical for many businesses to exchange cryptocurrencies for goods and services, because the basis in each individual coin could be different depending on the market price at the time of the transaction. Casinos accepting cryptocurrency also would need to take steps to ensure they do not conduct transactions with virtual currency addresses included on the sanctions lists.

If, on the other hand, a casino contracts with a third-party MSB to provide cryptocurrency exchange services to casino patrons, these external companies likely would shoulder some of the regulatory burden. Many casinos already have entered into contractual agreements with external MSBs to

provide patrons with check-cashing services and/or credit card advances. These external companies offer casino patrons the convenience of these services with less financial and regulatory risks to the casino. Although it is not possible to "outsource" an institution's legal and regulatory liability, casinos could enter similar contracts to include the provision of cryptocurrency exchange services to ensure that the third party performs diligence on customer transactions prior to those funds reaching the casino.

Another consideration is that many businesses that "accept" cryptocurrency payments do not actually ever take possession of the cryptocurrency. Instead, they utilize a BMSP, which intermediates between a business and a customer wishing to pay in Bitcoin. BMSPs provide a range of services, including accepting Bitcoin and paying the merchant in dollars, which eliminates a number of regulatory concerns to the merchant. In at least one instance, a casino-hotel that advertises itself as accepting Bitcoin at its restaurant uses a BMSP to process such transactions.

Utilizing the services of a BMSP allows a casino to offer its customers Bitcoin payment options without having to receive, convert, or maintain custody of virtual currency. This may help to avoid the complex accounting and record-keeping obligations associated with the IRS guidance about cryptocurrencies, as well as the licensing and regulatory requirements for money transmitters. A casino that accepts Bitcoin only through one of these BMSPs (or other cryptocurrency service providers) might also insulate itself from the volatility of the price of Bitcoin, because the exchange rate for the cryptocurrency is locked in at the time of the transaction.

While using an independent MSP to provide cryptocurrency exchange services or a BMSP to accept payment for goods or services avoids some regulatory issues for casinos, any gaming establishment that enters into a contract with an MSP or BMSP should take steps to ensure those entities comply with applicable regulations. To do so, the casino might inquire whether the entity:

- Is properly registered in compliance with FinCEN regulations and has an appropriate AML compliance program;
- Complies with any applicable state registration requirements;
- Makes sufficient disclosures to customers about the transaction and the role of the MSP or BMSP, including any appropriate consumer protection notices and warnings;[12]
- Has similar privacy practices as the casinos and whether such practices are properly disclosed to customers;
- Has a refund process that is consistent with all required laws; and[13]
- Can provide casino compliance personnel with full transparency regarding the source of the funds.

Conclusion

Any form of payment, funds transfer, or representation of value—especially cash—may be used for criminal purposes. Virtual currency is hardly an exception, and may carry with it unique risks which must be addressed with novel approaches to compliance and transparency. As a casino becomes exposed to these risks, directly or indirectly, it must adapt to these risks and tailor its compliance program accordingly. As cryptocurrencies gain popularity and obtain a greater footprint in usage and markets, casinos may find themselves indirectly exposed to their risks even if they make no intentional effort to court younger, tech-savvy cryptocurrency users. Law enforcement agencies, regulators, and others continue to express significant concerns regarding the role of virtual currency in money laundering, fraud, and illicit finance transactions generally. Whether such concerns are

wholly accurate, dramatically overblown, or completely underestimated, the perception may drive the legal and regulatory response as much as the reality.

With sufficient retooling and continuous improvement, casinos with robust, thoughtful compliance operations are well-positioned to implement procedures that meet their regulatory obligations and expectations. In so doing, casinos will be able to serve patrons interested in spending their cryptocurrency, and (as some banks have done) consider ways of using cryptocurrency and distributed ledger technology to gain efficiencies, offer new products, and increase their market share.

James F. Dowling, Managing Director, Dowling Advisory Group ("DAG") has more than 30 years' experience in the areas of fraud, anti-money laundering (AML) and risk management. He was a Special Agent with the IRS Criminal Division and a Managing Director at KPMG. Jim also served as the AML Advisor for the White House Drug Policy Office and worked closely with law enforcement and the intelligence community. Jim has also testified numerous times as a Fact and Expert Witness in state and federal courts regarding money laundering and fraud related issues. He is also an Adjunct Professor at USC, Leventhal School of Accounting where he teaches Forensic Accounting in the graduate program and is on the Board of Directors for ACMS, Southern California chapter.

Gregory Lisa is a partner at Hogan Lovells, where he uses his extensive firsthand experience in anti-money laundering investigations to help financial institutions navigate the complex regulations and expectations or regulators, examination teams, and law enforcement agencies, civil and criminal. Before joining Hogan Lovells, Greg was the Interim Director of the Office of Compliance and Enforcement at the Financial Crimes Enforcement Network (FinCEN), the Treasury Department's Lead regulator for overseeing and enforcing anti-money laundering laws. Greg also served the Chief of the Money Services Businesses and Casino Section within FinCEN's Enforcement Division. While at FinCEN, he supervised and conducted a number of investigations, supervisory examinations, and enforcement actions across a broad range of industries, including casinos and card clubs. Prior to his time at FinCEN, Greg served in the Office of Enforcement at the Consumer Financial Protection Bureau, and for twelve years at the U.S. Department of Justice, including ten years as a federal prosecutor investigating and prosecuting organized crime and money laundering cases.

Rebecca Umhofer is a Knowledge Lawyer at Hogan Lovells where she provides value-added services to clients through thought leadership pieces, continuing legal education programs, client alerts, newsletters, and presentations. Rebecca was previously an associate at Hogan Lovells where she represented clients in antitrust investigations as well as whistleblower litigation involving the Anti-Kickback Statute and the False Claims Act.

[1] Martin Arnold, *Six Global Banks Join Forces to Create Digital Currency*, Financial Times (Aug. 31, 2017), https://www.ft.com/content/20c10d58-8d9c-11e7-a352-e46f43c5825d.

[2] Kieran Corcoran, *Criminals in Europe are Laundering $5.5 Billion of Illegal Cash Through Cryptocurrency, According to Europol, Business Insider* (Feb. 12, 2018), http://www.businessinsider.com/europol-criminals-using-cryptocurrency-to-launder-55-billion-2018-2.

[3] Samuel Rubenfeld, *Treasury May Place Cryptocurrency Addresses on Sanctions List*, The Wall Street Journal (March 20, 2018), https://blogs.wsj.com/riskandcompliance/2018/03/20/treasury-may-place-cryptocurrency-addresses-on-sanctions-list/.

[4] *Id.*

[5] Jason Bloomberg, *Using Bitcoin or other Cryptocurrency to Commit Crimes, Law Enforcement is On to You*, Forbes (Dec. 28, 2017), https://www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/#461fc2363bdc.

[6] In a high profile case, investigators were able to identify one payment received by a corrupt DEA agent as a likely bribe and then employ electronic tools to trace the history of the agent's Bitcoin payments and wallets through the Bitcoin ledger. *See* Cyrus Farivar and Joe Mullin, *Stealing Bitcoins with Badges: How Silk Road's Dirty Cops Got Caught*, Ars Technica (Aug. 17, 2016) https://arstechnica.com/tech-policy/2016/08/stealing-bitcoins-with-badges-how-silk-roads-dirty-cops-got-caught/.

[7] *Id.*

[8] *See* Golden Gate Hotel & Casino, *The Best Ways to Utilize Your Bitcoin in Vegas*, (Feb. 22, 2018), http://www.goldengatecasino.com/2018/02/best-ways-utilize-bitcoin-vegas/ (last visited June 19, 2018).

[9] 31 C.F.R. § 1021.320.

[10] FinCEN, *Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013), available at https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

[11] It did so as early as September 15, 2014 when it brought a complaint against Butterfly Lab charging that the company had engaged in deceptive practices by misleading consumers who prepaid for bitcoin mining machines. See Press Release, U.S. Federal Trade Commission, *At FTC's Request, Court Halts Bogus Bitcoin Mining Operation* (Sept. 23, 2014), https://www.ftc.gov/news-events/press-releases/2014/09/ftcs-request-court-halts-bogus-bitcoin-mining-operation.

[12] Merchants should review the Consumer Financial Protection Bureau's advisory to consumers using virtual currency and ensure that their disclosures appropriately address the agency's concerns. *See* Consumer Financial Protection Bureau, *Consumer Advisory: Risks to Consumers Posed by Virtual Currencies* (Aug. 2014), available at https://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf.

[13] Stephen T. Middlebrook, *Bitcoin for Merchants: Legal Considerations for Businesses Wishing to Accept Bitcoin as a Form of Payment*, Business Law Today (Nov. 2014) available at https://www.americanbar.org//publications//blt//2014//11//02_middlebrook.html.