UNDERSTANDING DIGITAL TOKENS

Consumer Protection Considerations and Guidelines

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

FIRST EDITION • AUGUST 2019
CHAMBER OF DIGITAL COMMERCE

The Chamber of Digital Commerce is the world’s largest trade association representing the blockchain industry. Our mission is to promote the acceptance and use of digital assets and blockchain technology. Through education, advocacy, and working closely with policymakers, regulatory agencies, and industry, our goal is to develop a pro-growth legal environment that fosters innovation, jobs, and investment.

TOKEN ALLIANCE

The Token Alliance is an industry-led initiative of the Chamber of Digital Commerce, developed to be a key resource for the emerging industry surrounding the generation and distribution of tokens using blockchain technology. Comprised of more than 400 industry participants, the Alliance includes blockchain and token and legal experts, technologists, economists, former regulators, and practitioners from around the globe. The Token Alliance develops community-driven guidelines for the responsible development of tokens.

CHAMBER OF DIGITAL COMMERCE INDUSTRY INITIATIVES & WORKING GROUPS

SMART CONTRACTS ALLIANCE
Promotes real-world application of smart contracts to enhance the way business is conducted.

GLOBAL BLOCKCHAIN FORUM
Working with the world’s leading blockchain policy experts to develop industry best practices and help shape global regulatory interoperability.

BLOCKCHAIN ALLIANCE
The public-private forum for the blockchain community and law enforcement to help combat criminal activity.

BLOCKCHAIN INTELLECTUAL PROPERTY COUNCIL
Balancing the protection of proprietary information with the openness necessary for innovation.

DIGITAL ASSETS ACCOUNTING CONSORTIUM
Developing accounting and reporting standards for digital assets and blockchain-based technologies.

STATE WORKING GROUP
Engaging with state and local governments on the regulation and implementation of blockchain technology.

CHAMBER OF DIGITAL COMMERCE CANADA
Promoting the acceptance and use of digital assets and blockchain-based technologies in Canada.
# TABLE OF CONTENTS

I. ACKNOWLEDGEMENTS .................................................. 4

II. INTRODUCTION ......................................................... 7

III. CONSIDERATIONS AND GUIDELINES FOR CONSUMER PROTECTION .......................................................... 9

   I. FEDERAL CONSUMER PROTECTION AUTHORITY ........................................ 10
      A. FEDERAL TRADE COMMISSION ........................................ 10
      B. CONSUMER FINANCIAL PROTECTION BUREAU ........................... 12
      C. DEPARTMENT OF JUSTICE ........................................ 15

   II. STATE CONSUMER PROTECTION AUTHORITY ................................. 15
      A. STATE ATTORNEYS GENERAL ........................................ 15
      B. STATE BANKING AUTHORITIES ...................................... 17
      C. NEW YORK STATE BITLICENSE ...................................... 19

   III. GUIDELINES .......................................................... 22
I. ACKNOWLEDGEMENTS

TOKEN ALLIANCE CO-CHAIRS

PAUL ATKINS
Chief Executive Officer, Patomak Global Partners

JAMES NEWSOME, PH.D.
Founding Partner, Delta Strategy Group
TOKEN ALLIANCE LEADERSHIP COMMITTEE

The Chamber of Digital Commerce would like to recognize the following individuals for their thought leadership, contributions and support to the Token Alliance in the production of this report.

KEVIN BATTEH  
Partner,  
Delta Strategy Group

PERIANNE BORING  
Founder and President,  
Chamber of Digital Commerce

JOE CUTLER  
Partner,  
Perkins Coie LLP

DAX HANSEN  
Partner,  
Perkins Coie LLP

CHRIS HOUSSER  
Co-Founder,  
Polymath

JONATHAN JOHNSON  
President,  
Medici Ventures

AMY DAVINE KIM  
Chief Policy Officer,  
Chamber of Digital Commerce

KARI LARSEN  
Partner,  
Perkins Coie LLP

BRIAN LIO  
Chief Executive Officer,  
Smith + Crown

RUMI MORALES  
Partner,  
Outlier Ventures

MATTHEW ROSZAK  
Chairman and Co-Founder,  
Bloq

BILL SHIHARA  
Chief Executive Officer,  
Bittrex

TOM SPORKIN  
Partner,  
Buckley LLP  
Strategic Advisor, Token Alliance

JOSHUA STEIN  
Chief Executive Officer,  
Harbor

COLLEEN SULLIVAN  
Chief Executive Officer,  
CMT Digital
EXPERT CONTRIBUTORS

The Chamber of Digital Commerce would like to thank the following individuals and organizations for their valuable contributions to the Token Alliance in the production of this report.

We would also like to extend a special thank you to Greg Strong of DLx Law LLP and Elizabeth McKeen of O’Melveny & Myers LLP for helping to lead the development of this report.

THOMAS BORREL
Polymath

PAUL BRIGNER
Chamber of Digital Commerce

KENDRA HAAR
Perkins Coie LLP

OLGA MACK
Quantstamp

ELIZABETH MCKEEN
O’Melveny & Myers

DIVIJ PANDYA
Chamber of Digital Commerce

GREG STRONG
DLx Law LLP

COLLEEN SULLIVAN
CMT Digital

DAWN TALBOTT
RiskSpan

LILY WONG
Trust Token
II. INTRODUCTION

This new installment of our series of reports is an important addition to the overall regulatory and market consideration of the token ecosystem. The way in which digital tokens operate is complex and can maintain multiple characteristics – from an investment contract, to something necessary for utilizing a digital platform, to a form of payment or exchange, to name just a few. We are in a moment when technological advancement is pushing the boundaries of decades-long established law – law that was made at a time when tokenized assets and instantaneous digital transfers of value were not contemplated. It is exciting to be a part of it, but it also entails risks.

To facilitate the development of token businesses as well as minimize incidents of fraud and compliance challenges, the Chamber embarked on a plan to tackle each of the issues impacting this ecosystem. This journey started with a publication of guidelines for digital tokens that were intended to operate outside Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC)-regulated products and services laws (so-called “utility tokens” and associated platforms).

Those Guidelines also sought to provide legal context by detailing the legal landscapes governing digital tokens in five countries – the United States, Canada, the United Kingdom, Australia, and Gibraltar. Taking up a sizeable portion of the Report, the description of the vast number of potential legal requirements and government oversight demonstrated that this is a regulated industry, no matter where you fall in the spectrum of token categorization.

Finally, we provided an economic perspective on the industry with an analysis of market trends. The sheer volume of capital raised demonstrates the passionate interest of so many around the world in the potential of these markets – whether as a way to make money, a way to use new and better services, or other reasons.

This installment expands on those initial resources to balance out the conversation around utility tokens to discuss the rules, regulations, and resulting considerations for those who wish to issue or trade tokens that are or otherwise represent securities. This sector of the market is growing with entrants from new technology companies as well as established institutional financial services providers. The securities laws are complex, generated in the 1930s and developing substantial legal and regulatory precedent. In some cases, that precedent has endured because it is principles-based. In others, it has become outdated as it no longer sufficiently contemplates the types of securities that can be created, issued, held, and traded digitally.
We are excited to introduce these guidelines for consumer protection related to digital tokens. This complements our recent work on securities and non-securities tokens. But we can’t stop there. More areas need to be considered and addressed with thoughtful analysis. In the coming days and weeks, we also intend to publish guidelines around cyber security and anti-money laundering. We will be supplementing our legal landscape on a rolling basis with the introduction of additional countries and the laws that apply to digital tokens.

We hope you enjoy these publications and that they serve to help guide your analysis and views of the evolving digital token ecosystem. We look forward to sharing this series as we roll out these publications throughout the coming weeks!

A few words of caution:

**THIS REPORT DOES NOT CONSTITUTE LEGAL ADVICE**

» Specifically, nothing in this report should be construed as advice regarding the law of the United States or any other jurisdiction.

» This report’s analysis of the criteria under which it is determined that tokens constitute securities or commodities do not constitute a restatement of law.

» This report, including its suggested guidelines, merely express the general views of the Token Alliance, and compliance with such guidelines cannot assure that the distribution or trading of tokens will fully comply with the laws discussed herein.

» These views are being offered for discussion purposes only, and they have not been sanctioned by the SEC, CFTC, or any other regulator or government agency.

**CONSULT LEGAL COUNSEL BEFORE DISTRIBUTING OR HOSTING TRADES OF DIGITAL TOKENS**

» Token Sponsors and associated parties seeking to generate or distribute a blockchain-based token should seek independent legal counsel with expertise in this area before proceeding with their project, particularly given the fast-paced nature of this industry and the quickly evolving legal landscape.

» Counsel can help consider the facts and circumstances surrounding particular issues within the contours of then-current regulatory and enforcement activity.

» This report does not attempt to address any individual case, and the thought leadership contained herein is not appropriate for use as a substitute for independent counsel.

» Further, the digital token market is rapidly shifting and therefore the cases and regulatory interpretations discussed in this report may be overtaken by future events.

The Token Alliance will continue to study the issues surrounding the appropriate regulation for tokens and it will offer additional insights, as appropriate, when new developments arise.
III. CONSIDERATIONS AND GUIDELINES FOR CONSUMER PROTECTION

Consumer protection laws may apply to digital tokens in certain circumstances. In this report, we identify those circumstances most likely to result in the application of consumer protection laws to activities involving digital tokens, describe the source and scope of federal and state consumer protection authority, and provide guidelines to help token sponsors and token trading platforms avoid running afoul of consumer protection laws.

Federal and state consumer protection laws may apply to activities involving digital tokens. At the federal level, the Federal Trade Commission (“FTC”), the Consumer Financial Protection Bureau (“CFPB”), and the Department of Justice (“DOJ”) all have consumer protection authority. The FTC has the authority to enforce the Federal Trade Commission Act (“FTC Act”) which prohibits unfair or deceptive acts or practices (“UDAP”) in or affecting interstate commerce. The CFPB has the authority to enforce the Consumer Financial Protection Act (“CFPA”) which prohibits unfair, deceptive, or abusive acts and practices (“UDAAP”) engaged in by any person offering or providing a consumer financial product or service. The Civil Division of the DOJ has a Consumer Protection Branch that coordinates with the FTC, CFPB, and other federal agencies to enforce consumer protection statutes throughout the United States.

At the state level, state Attorneys General (“AGs”) have broad consumer protection authority to protect their citizens from unfair and deceptive acts and practices. State money-transmission licensing laws have consumer protection aspects that may apply in the context of transmission activities involving digital tokens. Additionally, the New York Department of Financial Services’ virtual currency regulations contain a consumer protection component. This section will examine each agency in more detail.

---

3 See 28 C.F.R. § 0.45(j) (setting forth the Consumer Protection Branch responsibility for litigation under principal federal consumer protection laws).
I. FEDERAL CONSUMER PROTECTION AUTHORITY

A. FEDERAL TRADE COMMISSION

The FTC has the authority to enforce the FTC Act, which prohibits unfair and deceptive acts or practices in or affecting commerce. An act or practice that “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition” is unfair. A consumer injury must be substantial, and not merely trivial or speculative, in order to trigger application of the FTC Act. Typically, substantial injury involves financial harm, and in some cases health and safety risks can also constitute substantial injury. Subjective types of harm are usually not enough to cause substantial injury.

The injury must also not be outweighed by countervailing benefits to consumers. For example, if providing complex disclosures to consumers regarding a product would cause the price of the product to increase, the consumer benefit of a lower price would be weighed against the potential harm associated with the lack of disclosure and the net effect considered. Finally, the injury must not be reasonably avoidable by consumers. Most actions alleging violations of Section 5 of the FTC Act are brought to address seller behavior that impedes individual consumer choice and decision making. An act or practice that unjustifiably interferes with the ability of consumers to make their own free and informed purchasing decisions will usually be unfair for purposes of the Act.

Misrepresentations or deceptive omissions of material fact also constitute deceptive acts or practices prohibited by Section 5(a). There are three elements of deception cases considered by the FTC: 1) a misrepresentation, omission, or practice that is likely to mislead the consumer, 2) the act or practice must be viewed through the lens of a reasonable consumer, and 3) the misrepresentation, omission, or practice must be material. A misrepresentation requires a representation that is likely to mislead and is material to the reasonable consumer. An omission of material information occurs when information necessary to prevent a claim, practice, or sale from being misleading is not disclosed. Practices related to marketing and point of sale representations can also be deceptive practices if they are likely to mislead consumers. Situations in which inaccurate or incomplete information is provided to prospective consumers in marketing materials or at the point of sale may constitute deceptive practices. The act or practice must be viewed through the objective lens of the reasonable consumer.
If an act or practice would be likely to mislead a reasonable consumer, it is deceptive.\(^{19}\) A consumer interpretation of an allegedly misleading act or practice that is not reasonable, but subjective, is not enough to deem the act or practice deceptive.\(^{20}\) Finally, the representation, omission, or practice must be material – meaning it must be related to information that is important to consumers in making consumer decisions.\(^ {21}\)

**ELEMENTS OF DECEPTION PRACTICES**

1. **A MISREPRESENTATION, OMISSION, OR PRACTICE THAT IS LIKELY TO MISLEAD THE CONSUMER**

2. **THE ACT OR PRACTICE MUST BE VIEWED THROUGH THE LENS OF A REASONABLE CONSUMER, AND**

3. **THE MISREPRESENTATION, OMISSION, OR PRACTICE MUST BE MATERIAL**

In or affecting commerce means “commerce among the several States or with foreign nations, or in any Territory of the United States or in the District of Columbia, or between any such Territory and another, or between any such Territory and any State or foreign nation, or between the District of Columbia and any State or Territory or foreign nation.”\(^ {22}\)

1. **AUTHORITY OVER TOKEN SPONSORS AND TOKEN TRADING PLATFORMS**

   The FTC has not yet used its authority under the FTC Act to pursue an action alleging violations with respect to initial or secondary sales of digital tokens. However, the agency has released several consumer advisories regarding virtual currencies\(^ {23}\) and filed several actions involving companies in the virtual currency industry alleging violations of the FTC Act. An action against Butterfly Labs alleged violations of Section 5(a) of the FTC Act for failure to deliver computers designed to mine virtual currency to consumers after they had paid for them.\(^ {24}\) The violations were based on misrepresentations or deceptive omissions of material facts in connection with the advertising, marketing, promotion, offer, or sale of products or services.\(^ {25}\) The matter was resolved with the entry of a Stipulated Final Order for Permanent Injunction and Monetary Judgment.\(^ {26}\)

---

19. Id.
20. Id.
21. Id.
25. Id.
An action against Equiliv, d/b/a Prized, also alleged violations of Section 5(a) of the FTC Act and violations of New Jersey state consumer protection laws in connection with a rewards app that implanted malware on users electronic devices that then used the computing power of those devices to mine bitcoin without notice or authorization. 27 One alleged violation was based on misrepresentations in connection with the advertising, marketing, and promotion of the Prized mobile application that were misleading and deceptive. 28 Another violation alleged unfair conduct in connection with infecting and taking control of consumers’ mobile devices with malware because that conduct caused, or was likely to cause, substantial injury to consumers that they could not reasonably avoid and was not outweighed by countervailing benefits to consumers. 29 This action was also resolved with the entry of a Stipulated Order for Permanent Injunction and Monetary Judgment. 30 Finally, an action against Bitcoin Funding Team and My7Network alleged violations of Section 5(a) of the FTC Act in connection with a multi-level marketing scheme promoted as an opportunity for consumers to generate income and accumulate wealth by purchasing and donating bitcoin to earlier “upline” participants and by recruiting others to do the same. 31 These chain referral schemes were alleged to be deceptive acts or practices in violation of Section 5(a) of the FTC Act in part because the scheme offered no products or services and income was derived solely through payments by later participants. 32 This action is pending in the Southern District of Florida as of June 3, 2019.

The FTC could in the future use its authority to address allegedly unfair or deceptive acts or practices that are potentially harmful to consumers in the context of the generation and distribution of digital tokens. Such an application of this authority would likely be limited to the sale or distribution of tokens that are not subject to an alternative regulatory scheme, such as the securities laws or the commodities laws. If the FTC were to bring such an action, it would likely be with respect to a digital token that it believes to be a consumer good and neither a security nor a commodity.

B. CONSUMER FINANCIAL PROTECTION BUREAU

The CFPB has authority pursuant to the CFPA to address unfair, deceptive, or abusive acts and practices (“UDAAP”) with respect to financial products offered primarily for consumer use by “covered persons” as defined by CFPA. 33 To date, the CFPB has not pursued a case alleging a violation of the CFPA in the context of a transaction in digital tokens and thus far has declined to extend Regulation E, governing electronic fund transfers involving consumers and financial institutions, to

28 Id.
29 Id.
32 Id.
virtual currencies.\textsuperscript{34} It has released several consumer advisories regarding virtual currencies and the newly created Office of Innovation has proposed a product sandbox, trial disclosure sandbox, and revisions to the no-action letter policy in attempts to facilitate innovation and engagement with entrepreneurs.\textsuperscript{35}

The scope of CFPB authority in this area is narrow. Several key restrictions limit the scope of potential CFPB enforcement actions pursuant to the CFPA in connection with transactions involving digital tokens. First, the UDAAP provisions of the CFPA only apply to financial products offered or provided for consumer use.\textsuperscript{36} The definition of “financial product or service” contains a list of products that fall within the definition and which are subject to CFPB jurisdiction when offered to consumers.\textsuperscript{37} Although the list is long, it is difficult to imagine how most of the products or services might apply in the context of digital tokens. One type of service on the list which might be applicable includes “engaging in deposit-taking activities, transmitting or exchanging funds, or otherwise acting as a custodian of funds or any financial instrument for use by or on behalf of a consumer.”\textsuperscript{38} “Transmitting or exchanging funds” means receiving currency, monetary value, or payment instruments from a consumer for the purpose of exchanging or transmitting the same by any means, including transmission by wire, facsimile, electronic transfer, courier, the Internet, or through bill payment services or other businesses that facilitate third-party transfers within the United States or to or from the United States.\textsuperscript{39}

Second, CFPB jurisdiction is limited to covered persons who are generally providers of consumer financial products or services.\textsuperscript{40} The term “covered person” means— (A) any person that engages in offering or providing a consumer financial product or service; and (B) any affiliate of a person described in subparagraph (A) if such affiliate acts as a service provider to such person.\textsuperscript{41} The term “service provider” means any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service, including a person who— (i) participates in designing, operating, or maintaining the consumer financial product or service; or (ii) processes transactions relating to the consumer financial product or service (other than unknowingly or incidentally transmitting or processing financial data in a manner that such data is undifferentiated from other types of data of the same form as the person transmits or processes).\textsuperscript{42} In addition to covered persons, any person who knowingly or recklessly

\textsuperscript{34} Electronic Fund Transfers (Regulation E), 81 Fed. Reg. 70,319 (Nov. 14, 2016).
\textsuperscript{36} 12 U.S.C. § 5531(a).
\textsuperscript{37} 12 U.S.C. § 5481(5) and (15).
\textsuperscript{39} 12 U.S.C. § 5481(29).
\textsuperscript{40} 12 U.S.C. § 5531(a).
\textsuperscript{41} 12 U.S.C. § 5481(6).
provides substantial assistance to a covered person or service provider in violation of the provisions of Section 5531 shall be deemed to be in violation of that section to the same extent as the person to whom such assistance is provided.\textsuperscript{43}

Third, persons registered with or regulated by the U.S. Securities and Exchange Commission (“SEC”) or U.S. Commodity Futures Trading Commission (“CFTC”) are explicitly excepted from CFPB jurisdiction as long as they are acting within the scope of their registered or regulated capacity.\textsuperscript{44}

The standards for unfair and deceptive acts and practices in CFPA are informed by the standards for those terms in the FTC Act, which are discussed above.\textsuperscript{45} Accordingly, there are significant similarities with respect to the conduct prohibited by both the FTC Act and CFPA.

In the CFPA, unfair is defined as: “an act or practice that causes or is likely to cause consumers substantial injury that is not reasonably avoidable and if the substantial injury is not outweighed by countervailing benefits to consumers or to competition.”\textsuperscript{46} The standard for unfairness here is almost identical to the standard for unfairness in the FTC Act. The same is true for deception, which constitutes an act that: 1) misleads or is likely to mislead consumers; 2) the consumer’s interpretation is reasonable under the circumstances, and 3) the misleading act is material.\textsuperscript{47}

The UDAAP also prohibits abusive acts or practices.\textsuperscript{48} What constitutes an abusive act or practice is less clear because it is not covered in the FTC Act, but such a practice must be one that:

» materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or

» takes advantage of —

• a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service;

• the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or

• the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.\textsuperscript{49}

“Abusive acts or practices may also be unfair or deceptive,” but each is distinct and “governed by separate legal standards.”\textsuperscript{50} The CFPB is considering addressing the abusiveness standard in future

\textsuperscript{43} 12 U.S.C. § 5536(a)(3).
\textsuperscript{44} 12 U.S.C. §§ 5481(20) – 5481(21).
\textsuperscript{46} 12 U.S.C. § 5531(c).
\textsuperscript{47} CFPB Bulletin 2013-07, supra note 45, at 3.
\textsuperscript{48} 12 U.S.C. § 5531(a).
\textsuperscript{49} 12 U.S.C. § 5531(d).
\textsuperscript{50} CFPB Bulletin 2013-07, supra note 45, at 4.
rulemaking, but it has only pursued an action alleging abusive practices alone in the rarest of circumstances – most actions to date alleging abusive practices have alleged either unfair or deceptive practices as well.

As described in detail above, the scope of CFPB authority in this space is narrow. The CFPB is constrained to regulating consumer financial products offered by covered persons that are not otherwise regulated by the SEC or CFTC. Accordingly, for the CFPB to assert jurisdiction, it would have to be with respect to a digital token that is neither a security nor a commodity, that constitutes a financial product, and is offered to consumers.

C. DEPARTMENT OF JUSTICE

The Consumer Protection Branch of the Civil Division of the Department of Justice (the “CPB”) plays a role in U.S. federal consumer protection statute enforcement as well. The CPB handles consumer protection case referrals from client agencies, either directly or in coordination with a local United States Attorney’s Office. The Civil Division is specifically assigned to handle consumer litigation arising under the FTC Act in certain circumstances. The FTC is a client agency of the CPB and the CPB is responsible for civil and criminal actions brought under the FTC Act, which generally fall within three categories: 1) enforcement actions for civil penalties and injunctive relief based on violations of final orders issued by the FTC; 2) enforcement actions for civil penalties and injunctive relief based on violations of FTC trade regulation rules; and 3) prosecutions for criminal violations of the FTC Act, and for violations of district court orders obtained under the FTC Act.

The DOJ also works closely with the CFPB as a partner agency. The CFPB and the DOJ coordinate with respect to investigations and proceedings involving federal consumer financial laws and may choose to bring coordinated enforcement actions in federal district court when appropriate. Most of the coordination to date between the CFPB and the DOJ has involved the Civil Rights Division and coordinated actions to enforce fair lending laws such as the Equal Credit Opportunity Act. Future coordination of investigations and enforcement between the CFPB and DOJ in the area of digital tokens is possible pursuant to these procedures.

II. STATE CONSUMER PROTECTION AUTHORITY

A. STATE ATTORNEYS GENERAL

State AGs typically have broad authority to protect consumers from unfair and deceptive acts and
state consumer protection statutes generally apply to consumer transactions involving products or services. These statutes are typically principles-based rather than rules-based, allowing them to be flexible, adaptable, and applicable to address a wide range of alleged misconduct. For example, state consumer protection statutes prohibiting unfair or deceptive acts or practices have been used in coordinated enforcement actions by state AGs to address activities as diverse as off-label marketing of drugs, unfair debt collection, misrepresentations regarding diesel emissions, and misrepresentations regarding credit ratings, to name a few.

Given the sweeping use of consumer protection authority by state AGs, it is likely that there will be investigations or actions involving digital tokens in the future. There have been no such actions to date and the activity with respect to digital tokens has been limited to consumer advisories about virtual currency. State consumer protection laws may be applied to digital tokens when they fall within the statutory definition of a good, service, or merchandise and there is a consumer transaction in a digital token that is alleged to have been unfair or deceptive. Notably, many state statutes include commodities in the definition of merchandise.

Certain states have the authority to use consumer protection statutes to address unfair or deceptive practices involving securities. For example, the Insurance and Financial Services Division of the Massachusetts Attorney General’s Office routinely uses its consumer protection authority with respect to matters involving securities. In certain circumstances, state AGs have also sought to address alleged misconduct involving securities by bringing both securities and consumer protection claims. For example, in a series of coordinated actions against rating agency Standard and Poor’s (“S&P”) for alleged misconduct in connection with its ratings of structured finance securities, certain state AGs alleged that S&P violated both consumer and securities laws. Accordingly, issuers of security tokens should be mindful of the potential for investigations or enforcement actions brought pursuant to state consumer protection authority.

State AGs also have the authority to enforce certain provisions of the CFPA, including, most importantly, the UDAAP provision. State AGs can take enforcement actions in federal court to enforce this provision whenever they believe that an unfair, deceptive, or abusive act or practice has
occurred in connection with the offer of a consumer financial product or service.⁶⁷ State AG authority is equal in scope to CFPB authority in this regard,⁶⁸ and in some states the ability to enforce the UDAAP provision of the CFPA increases the scope of consumer protection authority beyond what is provided for in the state consumer protection statutes alone. This potentially gives certain state consumer protection regulators the ability to address conduct through enforcement of the CFPA for which there would not be an otherwise viable action at state law. State AGs have coordinated with the CFPB on several CFPA enforcement actions.⁶⁹ As discussed, above, the applicability of the CFPA with respect to digital tokens is very narrow - the CFPA only applies to covered persons, offering a financial product or service when that product or service is offered to consumers. In addition, and unlike the state law authority outlined above, persons regulated by the SEC or CFTC are excluded from the coverage of the CFPA (which, from a policy perspective, makes sense in order to avoid subjecting entities to overlapping and duplicative regulatory schemes). Accordingly, a UDAAP action pursuant to the CFPA with respect to a security token is unlikely, whether pursued by the CFPB or State AGs.

B. STATE BANKING AUTHORITIES

State banking regulators generally regulate money services businesses including money transmitters.⁷⁰ Money transmission under state law generally means “selling or issuing payment instruments, stored value, or receiving money or monetary value for transmission.”⁷¹ State regulatory requirements are focused on consumer protection issues, in addition to ensuring the safety and soundness of money transmitters and adherence to Bank Secrecy Act and anti-money laundering requirements.⁷² State law generally requires money transmitters to be licensed, in part for the protection of consumers.⁷³

If you are engaging in the issuance, sale, redemption, storage, or trading of a digital token that functions as a store of value or medium of exchange, you may need to be licensed as a money transmitter in the states in which you operate. An analysis of your business model, the payment flows associated with your business, and the flow of digital tokens associated with your business should be completed with respect to each state in which you operate. In addition, consultation with an attorney with respect to this analysis is recommended so that a determination can be made with respect to any licensure obligations that may exist.

While specific laws vary from state to state, money transmitter licensing regimes typically include requirements that are designed, at least in part, with a consumer protection focus.⁷⁴

---

⁶⁷ Id.
⁶⁸ Pursuant to 12 U.S.C. § 5552(b), a state attorney general or state regulator must provide notice to the CFPB prior to initiating any action pursuant to 12 U.S.C. § 5552(a)(1).
⁷⁰ See CSBS supra note 5.
⁷² Conference of State Bank Supervisors, supra note 70, at 4.
⁷³ Id. at 5.
⁷⁴ Id. at 7.
Surety Bonds — Nearly every state requires a surety bond and nearly every state’s statute or regulations permit the regulator to adjust the amount of the bond required based on the applicant’s perceived risk. The bond serves as a form of insurance that will help repay customers if a licensee’s business fails or the licensee commits fraud. Bond amounts vary from state to state, and the Uniform Money Services Act, section 204(a) proposes a bond in the amount of $50,000 plus $10,000 per location with a maximum addition of $250,000.75

Permissible Investments — Many states require licensees to maintain permissible investments with a market value equal to or greater than the aggregate amount of outstanding payment instruments and stored value obligations.76 State regulators generally have the authority to limit the types of investments that are considered permissible, except for cash and certificates of deposit.77 Several states have taken the position that a company who offers cryptocurrency wallet services must hold the equivalent value in cash; the majority of states permit a company to hold value in like-kind assets. For instance, if a company is storing $1 million worth of bitcoin on behalf of customers, if the company has $1 million in bitcoin on hand, that should satisfy the permissible investment requirement. Permissible investments requirements are a means of safeguarding funds to protect consumers.

Financial History & Projections — States protect consumers by requiring applicants for money transmission licenses to submit audited financials for prior years.78 This requirement may be particularly difficult for new companies entering the digital asset industry as they may have limited operating history. Until recently, very few accounting firms would audit a company’s records that included cryptocurrencies and digital assets. States want to see a proven track record of a financially healthy business that anticipates financial health in the future when state residents are going to be depositing money with a licensee.

Background Checks — States also attempt to protect the consumers of the state by checking the background of the applicant and the control persons behind the applicant. Specifically, the state is looking for any criminal convictions, bankruptcies, and the personal financial health of the leaders of a business. Applicants for money transmission licenses are generally required to provide this type of information in their application.79 In addition, the regulator will typically conduct an investigation into these issues in connection with the evaluation of an application, which may include an on-site examination.80

75 Uniform Law Commission, supra note 71, at §204(a).
76 See id. at § 701(a).
77 Id.
78 See Uniform Law Commission, supra note 71, at § 202(c)(6).
79 See id. at § 202.
80 Id. at § 205(a).
C. NEW YORK STATE BITLICENSE

1. REGULATED PERSONS AND ENTITIES

On June 24, 2015, the New York State Department of Financial Services (“NYDFS”) began requiring that persons or entities engaged in certain activities involving virtual currency in New York or involving a New York resident obtain a business license referred to as a “BitLicense.”81 In September 2015, NYDFS issued its first BitLicense; since then, it has issued only sixteen more BitLicenses, for which NYDFS charges a $5,000 application fee.82

The BitLicense regime applies to business activities involving virtual currency, defined as “[a]ny type of digital unit that is used as a medium of exchange or a form of digitally stored value.”83 This includes centralized and decentralized virtual currencies, as well as virtual currency that can be mined.84 The definition expressly excludes digital units that exist solely within an online game and cannot be redeemed for fiat currency or real-world goods and services.85 It also excludes digital units associated with customer rewards programs, even if those units can be redeemed for real-world goods and services, so long as they cannot be converted to fiat currency.86

The BitLicense regime regulates a wide range of business activities, including: (i) transmitting virtual currency; (ii) storing, holding, or maintaining custody or control of virtual currency on behalf of others; (iii) buying and selling virtual currency as a business; (iv) performing exchange services for customers; and (v) controlling, administering, or issuing virtual currency.87 The types of activities most likely to be subject to regulation are those that involve e-wallets, token trading platforms, payment-processors, dealers, and virtual currency ATMs. Merchants who accept virtual currency in exchange for goods or services, miners of virtual currency, and virtual currency software developers are unlikely to be subject to BitLicense regulation.

2. CONSUMER PROTECTION REQUIREMENTS

One of the principal aims of the BitLicense is to protect consumers in the burgeoning market for virtual currencies. The BitLicense accomplishes this through a variety of strategies.

First, the BitLicense requires that licensees make numerous disclosures to consumers, both before and after engaging in any transaction. For example, licensees must disclose in writing to new customers prior to any transaction “all material risks associated with its products, services, and activities and Virtual Currency generally.”88 The regulation specifies ten such risks that,

---

84 See id.
87 See N.Y. Comp. Codes R. & Regs. tit. 23, § 200.2(q).
“at a minimum,” must be discussed, including that virtual currencies are not legal tender, that transactions in virtual currency may be irreversible, and that virtual currencies are volatile. Licensees must also disclose in writing to new customers prior to any transaction “all relevant terms and conditions.” The BitLicense specifies a minimum set of terms that must be disclosed, including customer liability for unauthorized transactions and the licensee’s right to disclose information about the customer’s account in certain circumstances. Finally, at the time of each transaction, licensees must disclose in writing the terms of the transaction, including at least the amount of the transaction, the amount of any fee(s), the type and nature of the transaction, a warning that the transaction may not be undone, and “such other disclosures as are customarily given” in such transactions. Notably, the BitLicense requires that these written disclosures be made in English, as well as in any other predominant language(s) spoken by the customers.

Second, the BitLicense requires that all licensees establish and maintain written policies for resolving complaints. A licensee must also disclose on its website and in any physical business locations the contact information for its complaint department and inform consumers that they may also bring their complaint to NYDFS.

Third, to enhance licensees’ paper trail, the BitLicense requires licensees to provide a detailed receipt to customers. The receipt must specify the licensee’s name and contact information, the type, value, date, and time of the transaction, the fee and exchange rate, and statements about the licensee’s liability for non-delivery or delayed delivery and its refund policy. The licensee must also be prepared to provide its receipt form to NYDFS upon request.

Fourth, the BitLicense requires that licensees take “reasonable steps to detect and prevent fraud, including by establishing and maintaining a written anti-fraud policy.” The licensee’s anti-fraud policy must include, at minimum, an identification and assessment of fraud-related risk areas, procedures and controls to protect against the identified risks, a description of the allocation of responsibility for monitoring risks, and procedures for the periodic evaluation and revision of the anti-fraud procedures, controls, and monitoring mechanisms.

Finally, the BitLicense regulates licensees’ advertising and marketing efforts. For example, licensees must include in advertisements their name and the fact that they hold a BitLicense. Licensees must also retain all advertising and marketing materials for seven years.
3. ADDITIONAL REQUIREMENTS

The BitLicense also requires licensees to establish and maintain certain additional programs to protect the licensee and its customers.

**Cybersecurity Program.** BitLicense requires licensees to have an effective cybersecurity program protecting its systems and customers’ accounts, including a written cybersecurity policy addressing a wide range of concerns and a comprehensive audit function for the program. Licensees must also designate a Chief Information Security Officer, submit an annual report to NYDFS assessing the cybersecurity program, and employ and train cybersecurity personnel.

**Anti-Money Laundering (“AML”) Program.** The BitLicense requires licensees to have an AML program based on annual risk assessments conducted by licensees and submitted to NYDFS. It must include, at minimum, a system of internal controls, policies, and procedures to ensure compliance, and must designate a qualified individual to oversee compliance with the AML program, and provide ongoing training for employees. Licensees must also maintain detailed records of all virtual currency transactions, and notify NYDFS within 24 hours of conducting any transaction in virtual currency valued at over $10,000 not subject to currency transaction reporting requirements under federal law.

**Business Continuity and Disaster Recovery (“BCDR”) plan.** Finally, the BitLicense requires that licensees have a BCDR plan that: (i) identifies documents, data, infrastructure, personnel, and competencies essential to the licensee’s business; (ii) identifies personnel responsible for implementing the BCDR plan; (iii) includes a plan for communicating with necessary personnel during an emergency; (iv) includes back-up system maintenance procedures; (v) includes data back-up procedures; and (vi) identifies third parties necessary to continue operation. This BCDR plan must be provided to employees and tested annually.
## III. GUIDELINES

The consumer protection laws outlined above aim to prevent potential consumer harm or to remedy such harm. Digital token sponsors and trading platforms should consider conducting an internal risk evaluation to assess the risk of potential consumer harm associated with the digital token(s) they distribute or trade and evaluating the sufficiency of controls in place to mitigate any such harm. Given the broad scope of the consumer protection laws discussed, it is likely that most digital token sponsors will have some degree of risk in this space, but understanding the components of that risk and the controls in place may permit digital token sponsors and trading platforms to better manage that risk.

Below is a non-exhaustive list of factors to consider in connection with an assessment of risk.

| » What is the marketing strategy for your token? |
| » How are you advertising and marketing the token? |
| » Are all advertisements, marketing materials, and other consumer-facing representations regarding the token reviewed for clarity, accuracy, and completeness? |
| » Are all advertisements, marketing materials, and other consumer-facing representations regarding the token worded in a way that prospective consumers can understand? |
| » How is the token priced? |
| » How will the token be sold? |
| » If there are salespersons involved in the process, does salesperson compensation avoid promoting improper sales practices? |
| » How complex is the token and the blockchain-based platform on which it operates? |
| » What are your target customer demographics? |
| » What role, if any, do third parties play in connection with the sale or distribution of tokens? |
| » What role, if any, do third parties play in connection with the operation of the platform? |
| » What steps have been taken to establish a compliance policy that includes consumer protection considerations? |
How is that policy enforced?

How is compliance with the policy monitored, both internally and with respect to any third parties involved in the platform?

What other steps have been taken with respect to regulatory compliance?

Are there policies in place to effectively handle consumer complaints regarding the digital token or the operation of the platform?

Conducting an internal risk assessment will help in following the below general guidelines.

Avoid activity that might be viewed as unfair or deceptive in connection with the sale of digital assets.

- Ensure that all advertising, representations to consumers, and legal documents clearly, accurately, and fully describe all of the facts material to the prospective purchase of the digital assets being sold.

- Adhere to the policies and procedures (and marketing promises) you set out in all advertising, representations to consumers, and legal documents (do what you say you do).

Token trading platforms should endeavor to avoid unfair, deceptive, or abusive acts or practices.

- Ensure that all advertising, representations to consumers, and legal documents accurately and fully describe all of the facts material to the prospective purchase of the digital assets being sold.

- Avoid any representations that might materially interfere with a consumer’s ability to understand a financial product or service (abusive acts or practices).

Entities engaged in Virtual Currency Business Activity involving New York or a New York resident will need to be licensed and comply with the consumer protection (as well as other) provisions of the BitLicense law.