JONES DAY | One Firm Worldwide®

WHITE PAPER

September 2022

Digital Assets Defined: Consumer Protection and Cybersecurity Enter the Stage

In this latest *White Paper* on our Bill analysis, we underscore headline proposals in the Lummis-Gillibrand Responsible Financial Innovation Act (the "Bill") regarding consumer protection standards (Title V) and cybersecurity standards (Title VIII, Section 808). As for consumer protection standards, the Bill lays out the notices and disclosures that digital asset service providers must give customers, and the subjects that customer agreements must address. The Bill also covers rules for managing the accrual of gains to digital assets, the implementation of source code changes to digital assets, the enforcement of the standards laid out in the title, and customers' rights to individual management of their digital assets. As for cybersecurity standards, the Bill requires the Commodity Futures Trading Commission ("CFTC") and the Securities and Exchange Commission ("SEC") to develop guidance related to cybersecurity for digital asset intermediaries (as described in our previous *White Paper*).

We conclude this *White Paper* by highlighting important unresolved questions that should be the focus of future stakeholder efforts to refine the Bill before it—or aspects of it—becomes law.

CONSUMER PROTECTION STANDARDS FOR DIGITAL ASSETS

Scope of Permissible Transactions

A digital asset service provider, defined in the Bill as set forth below, must ensure that the scope of permissible transactions that it may undertake with its customers' digital assets is clearly disclosed in a customer agreement. Unlike other requirements for digital asset service providers in Title V, this requirement applies to both "persons" and "protocols" providing digital asset services. Under the Bill, a "person who provides digital asset services" includes: (i) a digital asset intermediary; (ii) a financial institution as defined in section 1a of the Commodity Exchange Act; and (iii) any other person conducting digital asset activities pursuant to a federal or state charter, license, registration, or other similar authorization, or a person who is required by law to hold such a license, registration, or other similar authorization. The Bill does not define "protocol," but based on the Bill's other references to protocols, it likely means decentralized applications such as decentralized finance ("DeFi") protocols.

Required Notices to Customers

A digital asset service provider must give clear notice to each customer, and obtain the customer's acknowledgement, of any "material"[1] changes to the source code version of a digital asset involved in the parties' contractual relationship.[2] Under the Bill, "source code version" means the source code version comprising a digital asset, and does not include the software used to manage or facilitate transactions in a digital asset.

The provider must generally give the required notice and obtain the required acknowledgement before the provider implements any material source code change. Notice and acknowledgement are not required in emergencies, however, such as when security vulnerabilities exist that require immediate changes to a source code version. It is unclear as to whether, in an emergency, notice and acknowledgement would be required *after* a source code version change is implemented. However, as laid out elsewhere in the Bill (*see* "Source Code Version of Digital Assets," *below*), a provider may specify that different standards for implementing source code version changes apply in emergencies, which could include giving notice and obtaining acknowledgement after a source code change is implemented.

In addition, a digital asset service provider must provide clear notice to each customer, and require the customer's acknowledgement, of the following:

- Whether the customer's digital assets are segregated from other customers' assets, and the manner of segregation.
- How the customer's assets would be treated in a bankruptcy or insolvency scenario, and the risks of loss (note that Title IV, Section 407 of the Bill, which will be discussed in a future Jones Day *White Paper*, enacts new requirements related to the bankruptcy treatment of digital assets).
- The time period and the manner in which the provider must return the customer's digital assets to the customer upon the customer's request.
- Any fees that apply to the contractual relationship between the provider and the customer (such fees could include transaction fees, or a monthly fee for custodying digital assets).
- The provider's dispute resolution process for any disputes that arise between the provider and the customer.

Subsidiary Proceeds

Except as otherwise specified in a customer agreement, all "ancillary or subsidiary proceeds" related to digital asset services provided by a digital asset service provider accrue to the customer's benefit. "Subsidiary proceeds" are defined to include proceeds arising from forks,[3] airdrops,[4] staking,[5] and other gains that accrue to a digital asset through market transactions, use as a financial asset, or being held in custody or safekeeping by a digital asset service provider. The use of "ancillary" appears to be redundant here, since there is no separate definition for "ancillary proceeds," and "ancillary" and "subsidiary" are related concepts. A digital asset service provider may elect not to collect certain subsidiary proceeds, if the election is disclosed in a customer agreement.

Assuming a digital asset service provider elects to collect subsidiary proceeds, a customer may withdraw its digital assets from the provider in a method that permits the collection of subsidiary proceeds. Further, if a customer desires, a digital asset service provider must enter into a customer agreement regarding the manner in which to invest subsidiary proceeds or other gains attributable to the customer's digital assets.

As used here in connection with "subsidiary proceeds," an "agreement" includes the digital asset service provider's standard terms of service. Thus, to the extent these standards on subsidiary proceeds require something to be disclosed in or agreed to through a customer agreement, it may be disclosed in or agreed to through the provider's standard terms of service.

Lending Arrangements

Digital asset service providers must ensure that any lending arrangements they have with customers related to digital assets are clearly disclosed to customers before any lending services take place, and that their customers consent to such arrangements.

Providers must also ensure that any lending arrangements with customers are accompanied by a wide variety of disclosures. Specifically, such arrangements must be accompanied by:

- Full disclosures of applicable terms (such as the loan's repayment period, monthly payments, and interest rate) and risk, yield, and the manner in which the yield is calculated.
- "Appropriate disclosures" related to collateral requirements and policies, including: (i) haircuts and overcollateralization;[6] (ii) collateral the provider accepts when calling for additional collateral from a customer, including collateral substitution; (iii) whether customer collateral is comingled with other customers' collateral or the provider's collateral; and (iv) how customer collateral is invested, and whether the yield belongs to the customer or the provider. The term "appropriate disclosures" is not defined here.
- Disclosures of mark-to-market and monitoring arrangements,[7] including: (i) the frequency of mark-to-market monitoring and how frequently the provider will call for additional collateral from a customer; (ii) the time period in which the customer must supply additional collateral to the provider after a collateral call; and (iii) whether the provider permits failures to deliver additional collateral, and if so, the period of time in which a customer must cure the failure before the customer's position is closed.

Further, providers must ensure that lending arrangements with customers are "fully enforceable as a matter of commercial law" and compliant with all applicable federal and state laws. In general, for a contract to be legally enforceable, there must be an offer, an acceptance, consideration, capacity to contract, and legality of purpose. Certain laws apply to lending arrangements in particular, including the Equal Credit Opportunity Act, which prohibits lenders from discriminating against borrowers on the basis of any protected class; the Truth in Lending Act, which requires lenders to disclose loan cost information to borrowers; and state usury laws, which prohibit lenders from charging unreasonable or predatory interest rates. Requiring providers to ensure that their lending arrangements with customers are "fully enforceable as a matter of commercial law" and compliant with federal and state lending laws could have a profound impact on DeFi protocols and decentralized autonomous organizations ("DAOs"), many of which employ smart contracts to effectuate loan transactions. Questions regarding the enforceability of the "agreements" underlying smart contracts—such as what source code controls and who the contracting parties are—have circulated for years without clear answers. Because it does not address these questions directly, the Bill, as written, would require DeFi protocols and DAOs to continue to answer these questions for themselves, and to incorporate the requirements of contract law in general, and lending laws in particular, into the smart contracts and related documents used for loan transactions.

Rehypothecation

Before a rehypothecating a customer's digital asset—that is, before pledging to a third party as collateral for a financial transaction a digital asset that a customer has pledged to the provider as collateral for a loan—a digital asset service provider must clearly disclose its polices on rehypothecation to customers, including a clear definition of "rehypothecation" that is accessible to consumers. The terms "clearly disclose," "clear definition," and "accessible" are not defined here. A provider must also obtain affirmative consent from a customer to rehypothecate that customer's digital asset.

In addition, when deciding to rehypothecate a customer's digital asset, a provider must consider the following factors to appropriately mitigate risk relating to rehypothecation:

- The liquidity and volatility of the digital asset.
- Past failures to deliver the digital asset.
- The concentration risk of the digital asset.[8]
- Whether an issuer or lender of last resort relating to the digital asset exists, including for virtual currency with a finite supply.[9]

- The provider's capital, leverage, and market position.
- The provider's legal obligations to customers and other digital asset service providers.

Source Code Version of Digital Assets

At the beginning of their contractual relationship, a digital asset service provider and its customer must agree in writing on what source code version will apply to each digital asset involved in that relationship, including for purposes of legal treatment. This agreement must include the treatment of each digital asset under securities laws and commodities laws, as well as under the Uniform Commercial Code ("UCC") applicable to the transaction.

A digital asset service provider may periodically implement a digital asset source code version that uses validation rules different from those of the source code version specified in the customer agreement. The term "validation rules" is not defined, but most likely refers to block-level validation rules (or "consensus rules"), which define what is permitted to be included in a block on a blockchain and require nonconforming transactions to be rejected from the chain.

A provider may implement a digital asset source code version with different validation rules even when it is not possible to predict in advance whether using the different source code will be in the "best interests" of the customer. However, this discretion leaves open the possibility that providers must consider how a source code change will affect customers' best interests if it is possible to do so. The "best interests" of the customer are not defined; what is in a customer's "best interests" could range from ensuring the maximum possible value of a digital asset, to ensuring the maximum possible liquidity of the digital asset, to ensuring that the digital asset can be used in future transactions.

A digital asset service provider must consider the nature of any proposed changes to the source code versions of a digital asset. Specifically, the provider must consider whether any proposed changes by third-party actors—such as within a DAO—could create different source code versions resulting in new networks that could create "economic value" for customers. The term "economic value" is not pegged to any particular standard here; perhaps it could be determined by the digital asset's price in the securities or commodities markets, or by the asset's liquidity and risk.

Although a digital asset service provider is allowed to implement a digital asset source code version that uses different validation rules, it is not required to support digital assets and source code versions that it has not agreed with customers to support. This issue may arise if customers are expecting or pressing a provider to change the source code version of a digital asset. At the same time, a digital asset service provider must not "capriciously" redefine a digital asset or corresponding source code or alter customer agreements as they relate to digital asset source codes. The term "capriciously" is not defined here.

A digital asset service provider must adopt and maintain standards for implementing digital asset source code versions with different validation rules from those of the source code version specified in a customer agreement. These standards must include customer notice and approval "as appropriate based on the circumstances"; this rule is not explained, and will likely be based on a fact-intensive inquiry and subject to court interpretation. Providers may specify that different standards for implementing source code version changes apply in emergencies, such as when security vulnerabilities exist that require immediate changes to a source code version.

Settlement Finality

Digital asset service providers and their customers must agree on the terms of settlement finality for all transactions between them. That agreement must address the conditions under which a digital asset may be deemed fully transferred as a matter of law. These legal conditions may be different from the operational conditions under which digital assets are considered transferred based on the distributed and probabilistic nature of digital assets. Therefore, digital asset service providers and their customers can choose to consider a digital asset as fully transferred as a matter of law, even if different from when it would be considered fully transferred in operation.

The agreement between provider and customer on settlement finality terms must also address the exact moment of transfer of a digital asset, the discharge of any obligations upon transfer of a digital asset, and conformity to applicable provisions of the UCC. Provisions of the UCC that relate to settlement finality include Article 2, Parts 3-5 (transfer obligations related to contracts for the sale of goods); Article 4, Part 2 (transfer obligations related to bank deposits and collections); Article 4A, Parts 2-4 (transfer obligations related to

funds transfers between banks); Article 8, Part 3 (transfer obligations related to investment securities); and Article 9, Part 2 (attachment obligations related to secured transactions).

Standards of Customer Notice and Enforcement of Consumer Protection Standards

When providing disclosures and carrying out other duties under 31 U.S.C. Subtitle VI, Chapter 98 (a new chapter created by the Bill), a person who provides digital asset services in or affecting interstate commerce must provide "higher" standards of customer notice and acknowledgement if there is likely to be a "material" impact on the "economic value" of a customer's digital asset. Again, the terms "higher" and "material" are not defined here. And, again, the term "economic value" is not pegged to any particular standard.

The Bill also instructs that the "standards" under 31 U.S.C. Subtitle VI, Chapter 98 shall be enforced "in an appropriate manner," commensurate with other consumer protection standards. Given the reference to "other consumer protection standards," the term "standards" most likely refers to the "consumer protection standards" laid out in Title V of the Bill. "[A]n appropriate manner" will most likely depend on how authorities would enforce consumer protection standards in other contexts. "Commensurate with" also indicates that enforcing authorities must not treat the consumer protection standards applicable to digital assets any differently from the consumer protection standards applicable to other types of goods or services.

The consumer protection standards under Title V applicable to digital asset intermediaries will be enforced by the federal or state licensing, registration, or chartering authority of the intermediary, while the standards applicable to depository institutions or other financial institutions will be enforced by the appropriate federal or state banking supervisor.

Right to Individual Management of Digital Assets

"[E]xcept as otherwise required by law," no person is required to use an intermediary for the safekeeping of digital assets that the person legally owns and either possesses or controls. An example of a law that requires a person to use an intermediary for the safekeeping of assets that the person legally owns and either possesses or controls is 17 CFR § 227.100, which requires a securities issuer to use an intermediary when relying on the crowdfunding exemption to securities registration requirements.

The Bill states it should not be interpreted as allowing a person to engage in market activity for which authorization is required under federal or state law. In other words, the fact that a person is not required to use an intermediary to safekeep that person's digital assets does not mean that person can use those digital assets for a market activity without being authorized to do so, if such authorization is required by federal or state law.

The Bill also states that it should not be interpreted as preventing a person from freely entering into an agreement for digital asset services with a third party. In other words, the fact that a person is not required to use an intermediary to safekeep that person's digital assets does not mean that person is prohibited from making an agreement to do so if desired.

Undefined Terms

As evident from the above discussion, the Bill's proposals related to consumer protection standards leave several crucial terms undefined. The meanings ultimately assigned to these undefined terms will likely be based on fact-intensive inquiries and subject to interpretation by courts and by a number of federal and state agencies. Some terms—such as "material" and "best interests"—may be interpreted consistently with their meanings in other contexts, such as whether there has been a misrepresentation or omission of "material" information to investors in the securities fraud context, and whether a broker-dealer's recommendation of a securities transaction or investment strategy involving securities is in the "best interests" of a retail customer. Other terms have no corollaries to reference, and will present issues of first impression.

It is also likely that some or all of the federal and state regulators responsible for enforcing the Bill's consumer protection standards (*see* "Standards of Customer Notice and Enforcement of Consumer Protection Standards," *above*) will promulgate rules or guidance interpreting these undefined terms in the future. Indeed, Title VIII of the Bill expressly contemplates that the CFTC and the SEC, among other federal financial regulators, will issue "individualized interpretative guidance" on the application of statutes, rules, or policies under their jurisdiction.

CYBERSECURITY STANDARDS FOR DIGITAL ASSET INTERMEDIARIES

On the topic of cybersecurity, the Bill requires the CFTC and the SEC, in consultation with the Secretary of the Treasury and the Director of the National Institute of Standards and Technology, to "develop comprehensive, principles-based guidance relating to cybersecurity" for digital asset intermediaries. This guidance must account for:

- The internal governance and organizational culture of the digital asset intermediary's cybersecurity program;
- The security operations of the digital asset intermediary, including threat identification, incident response, and mitigation;
- Any risk identification and measurement by the digital asset intermediary;
- The mitigation of risk by the digital asset intermediary, including policies of the digital asset intermediary, controls implemented by the digital asset intermediary, change management with respect to the digital asset intermediary, and the supply-chain integrity of the digital asset intermediary;
- Any assurance provided by, and testing conducted by, the digital asset intermediary, including penetration testing and independent audits so conducted; and
- The potential for digital asset intermediaries to be used to facilitate illicit activities including sanctions avoidance.

This guidance must be "developed," according to the Bill, no later than 18 months after the Bill is enacted.

CLOSING THOUGHTS

All told, the Bill sets out a thorough framework for regulating—or developing rules for regulating—important consumer protection and cybersecurity issues in the digital assets space. These include foundational matters such as customer notices, subsidiary proceeds, lending arrangements, and source code controls. At the same time, the Bill relies on key terms and concepts that it does not define, such as "material" changes to source code, "higher" standards of customer notice and acknowledgement, and "best interests" of the customer, to name just a few. Thus, in order for the proposed framework to be implemented in a manner that provides clarity for market participants, the Bill will have to become more specific, or agencies and courts may be left to fill in the blanks.

LAWYER CONTACTS

David E. Aron
Washington
+1.202.879.3876
daron@jonesday.com

Nathan S. Brownback
Washington
+1.202.879.3476
nbrownback@jonesday.com

Dorothy N. Giobbe
New York
+1.212.326.3650
dgiobbe@jonesday.com

Abradat Kamalpour
San Francisco
+1.415.875.5860
akamalpour@jonesday.com

Mark W. Rasmussen
Dallas
+1.214.220.3939
mrasmussen@jonesday.com

Joshua B. Sterling
Washington
+1.202.879.3769
jsterling@jonesday.com

Jayant W. Tambe
New York
+1.212.326.3604
jtambe@jonesday.com

Samuel L. Walling
Minneapolis
+1.612.217.8871
swalling@jonesday.com

Jonathan D. Guynn, Christina Mastrucci Lehn, John Paul Putney, and Collin L. Waring contributed to this White Paper.

ENDNOTES

1 The Bill does not define the term "material."

2 "Source code" refers to a set of instructions, written in programming language, directing a computer program how to function.

3 "Forks" are changes to a blockchain's protocol that cause the chain to split and produce an additional chain.

4 An "airdrop" is the delivery of a cryptocurrency, token, non-fungible token ("NFT"), or other type of digital asset to customers at no cost, generally as part of a promotion.

5 "Staking" is pledging digital assets to a platform for use in the proof-of-stake process for validating blockchain transactions in a proof-of-stake ecosystem, e.g., Ethereum.

6 A "haircut" refers to valuing a collateral asset as less than its fair market value, while "overcollateralization" refers to pledging a collateral asset worth more than the loan amount.

7 "Mark to market" is a method of measuring, based on current market conditions, the fair value of an account that can fluctuate over time.

8 "Concentration risk" is the risk of loss that may occur from a customer "concentrating" its investments in the digital asset, compared to the customer's overall portfolio.

9 A "lender of last resort" provides liquidity to a lender that urgently needs funding and has exhausted all its other options.