Analysis of the FinTech Policy Landscape

Introduction

The Milken Institute FinTech Program is tracking the ongoing development of FinTech-related legislation introduced in the 117th Congress. The corresponding FinTech policy landscape tracker displays the entire list of bills, grouping them directly or indirectly related to FinTech. The bills are then subcategorized within the direct and indirect categories based on the subject matter they most accurately reflect (Artificial Intelligence, Blockchain, Broadband, Lending, etc.). The tracker will be updated regularly as more bills are introduced. The tracker is a dynamic platform that allows users to interact with the information and inspect further details of the proposed legislation, including bill sponsors and co-sponsors, any related bills, the status of the bill, and more.

This policy landscape takes a closer look at a handful of the FinTech-related bills we are tracking. The purpose of this examination is to highlight trends, make connections among related pieces of legislation, and identify possible intended or unintended consequences.

The information contained in this document and displayed on the tracker will help inform the Milken Institute FinTech Program's efforts toward promoting access to capital, financial inclusion, and transparency and compliance. As the 117th Congress continues to take shape, many of the same themes and priorities from previous Congresses continue to reemerge, including cybersecurity, data privacy/protection, and digital assets.

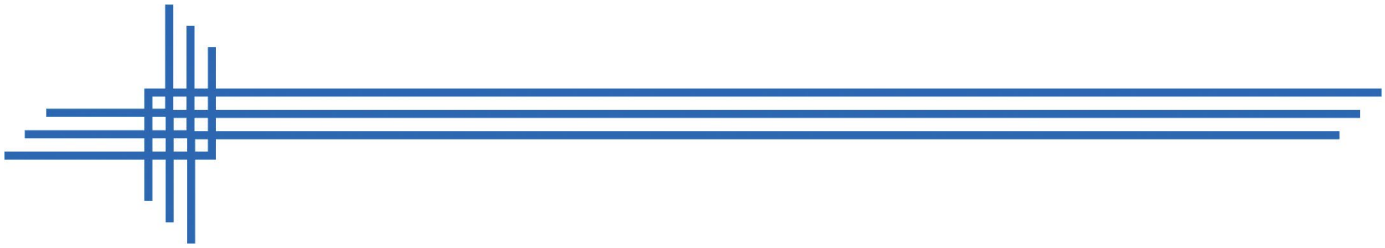
Cybersecurity

Related to cybersecurity and FinTech, H.R.296, Financial Technology Protection Act, proposes the establishment of an independent task force to research the "use of new financial technologies, including digital currencies" in illicit financing and provide policy recommendations based on their findings. These recommendations will be part of a larger effort to strengthen government Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) capabilities. Section 4 of H.R.296 proposes to establish a fund rewarding individuals who provide information to law enforcement officials that leads to the conviction of someone using digital currencies for terrorist activities. It remains unclear whether the increased whistleblower protections ratified by Section 8285 of the National Defense Authorization Act (NDAA) for fiscal year 2021 (H.R.6395) would apply under H.R.296 as the bill does not explicitly use the term "whistleblower." If whistleblowing is the intended outcome, policymakers may want to consider including specific protections such as anti-retaliation rules alongside monetary rewards.

H.R.296 also outlines an innovation program that would provide grant funding for individuals to develop tools and pilots that improve the government's ability to support AML/CFT efforts associated with digital currencies. The grant program would prioritize any open-sourced and nonproprietary technologies that support the regulatory standards of the Bank Secrecy Act.

Notably, this bill is very similar to the Treasury's plan for mitigating cyber-vulnerabilities of digital assets outlined in the 2020 National Strategy for Combating Terrorist and Other Illicit Financing. The Treasury plan describes the insufficiencies in our current framework by underscoring how "Laundering illicit proceeds through digital assets, often facilitated by the use of encrypted messaging applications, is frequently linked to cybercrime and other cyber-enabled crimes." The parallels between the Treasury's 2020 national strategy and this bill include leveraging technology to counter the financing of terrorism, promoting public-private coordination, investigating further regulatory oversight of digital assets, and improving global compliance enforcement. The task force and grant program proposed in H.R.296 could be an invaluable application of the Treasury's proposed strategy for combating terrorism and illicit financing.

However, the specific definitions in H.R.296 differ from those in the Treasury's plan. H.R.296 defines a digital currency as "a digital representation of value that is used as a medium of exchange, unit of account, or store of value; and is not established legal tender." Under Office of Foreign Assets Control (OFAC) sanctions, the Treasury's definition of a virtual currency is almost identical to the above definition of a digital currency. Under the same OFAC sanctions, the Treasury defines a digital currency as "sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency." An example of a digital representation of a fiat currency would be a Central Bank Digital Currency (CBDC), which does not fit with H.R.296's designation of digital currencies not representing legal tender. The definition used in this bill to explain a digital currency matches the Treasury's definition of a "virtual currency" but not a "digital currency." For operational clarity, sponsors of H.R.296 may want to swap their use of "digital currency" for "virtual currency" to better align with the Treasury's definition or widen the scope of their research to encompass other types of digital assets.



Above all, the bipartisan Financial Technology Protection Act is a powerful representation of how legislation can accomplish an important policy goal—in this instance, to strengthen the detection of illicit financing through digital currencies—without proposing overly burdensome regulations that may hamper legal and responsible innovations in digital currencies.

Data Privacy and Protection

Both the House (H.R.847) and the Senate (S.224) versions of the bipartisan Promoting Privacy Digital Technologies Act seek to endorse technology development that strengthens data minimization and de-identification practices. Section 3 of the companion bills outlines research to be conducted by the National Science Foundation "on technologies for de-identification, pseudonymization, anonymization, or obfuscation of personal data in data sets while maintaining fairness, accuracy, and efficiency." The specificity of the language used here sets these bills apart from other data privacy bills. Often the words de-identification, anonymization, and pseudonymization are used interchangeably when they do not mean the same thing regarding data privacy and protection standards. Other times, a specific standard for de-identification is not specified at all. It is valuable to denote the difference among these privacy standards, especially as they relate to maintaining the "fairness, accuracy, and efficiency" of the data.

Section 5 of H.R.847 describes a coordinated outreach between various public and private stakeholders to provide input on these technologies. It would be worthwhile for these stakeholders to reach a consensus around the degree of de-identification they hope to achieve. One framework for this standard could be modeled after the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule for De-Identification. This rule describes two different de-identification methods that both satisfy the HIPAA Privacy Rule. The first method, "Safe Harbor," removes 18 types of identifiers and almost entirely eliminates the possibility of patient re-identification. The second method, "Expert Determination," allows an expert to assess if certain identifiers can be used with a minimal risk of patient re-identification.

The "Safe Harbor" method of de-identification is the most secure, but it compromises how valuable the data are during research and analysis. The "Expert Determination" method of de-identification is slightly less secure, but it improves the utility of the data for researchers or anyone else inspecting the data sets. The National Science Foundation must determine through research and engagement whether their recommendations will prioritize the security of the data sets, the ability to analyze the data sets, or apply a hybrid approach modeled by the HIPAA Privacy Rule, which would allow different methods to be used situationally.

FinTech is a data-intensive industry by nature. Consumer data allow companies to innovate and strengthen their market offerings. Consumers are not threatened by the aggregation of large volumes of data alone. The research outlined in H.R.847 and S.224 should prioritize finding the right balance between safeguarding against the harmful use of personal data while also allowing companies that rely on robust consumer data to continue operating. When setting standards for de-identification, applying a risk-based approach instead of blanket enforcement will help to minimize unintended consequences for FinTechs while maximizing consumer protections.

Digital Assets

Two bills have been introduced in the House related to the treatment and deployment of digital assets. The first bill, Eliminate Barriers to Innovation Act of 2021 (H.R.1602), proposes to establish a digital asset working group comprised of representatives from FinTech firms, investors, and advocacy groups. The working group will report to the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) on its findings related to best practices for strengthening the digital asset market, safety and soundness of the industry, investor protections, and compliance. The working group will also analyze the impact our current regulatory framework has on digital assets in the primary and secondary markets. Of all the FinTech-related bills currently being tracked by the Milken Institute FinTech Program, this bill has currently received the most traction in Congress. H.R.1602 passed the House at the end of April 2021 and is now being considered in the Senate.

Subsection (c)(1)(B)(iii)(III) of the bill solicits recommendations to "assist in compliance with anti-money laundering and countering the financing of terrorism obligations under the Bank Secrecy Act." This language mirrors lawmakers' intent to mitigate terrorist financing through digital channels, as reflected in H.R.296. These bills strengthen the notion of a policy trend emerging related to heightened reporting and compliance standards for digital asset marketplaces and higher scrutiny being placed on virtual currency exchanges. To achieve this goal without hampering innovation, government engagement with the FinTech industry will be paramount.

H.R.1602 does not include a specific definition for "digital asset" in the bill text. Applying a definition to a word that is currently undefined in law is no small undertaking. The writers of H.R.1602 may need to consider the bill's stakeholders and the intended purposes of the working group as they approach their definition of a digital asset. A delicate balance must be found between being too vague and running the risk of confusing readers and being too prescriptive and potentially creating a definition that becomes outdated as technology continues to evolve. Looking at the definitions of digital asset used by other government agencies may provide a helpful framework for this.

As demonstrated by H.R.296, definitions are essential for the sake of clarity, especially when it comes to regulatory oversight. Definitions ensure that all interpretations of the bill align with the original intentions laid out by sponsors and co-sponsors. For example, some people may classify a non-fungible token (NFT) as a subset of digital assets. Still, NFTs may not fit with H.R.1602's intended scope for the digital asset working group. Definitions help regulators navigate any potential ambiguities in the law—such as whether or not the working group should spend time discussing and analyzing NFTs—especially as these emerging technologies continue to gain mainstream popularity.

The same 2020 National Strategy for Combating Terrorist and Other Illicit Financing mentioned above also highlights how the SEC or the CFTC does not regulate all digital assets. In fact, most digital asset activities in the United States meet the Financial Crimes Enforcement Network's (FinCEN's) classification of a money service business and thus fall within FinCEN's regulatory purview. These money service businesses encompass many of the secondary market participants referred to in this bill, including digital

asset intermediaries and exchanges. Digital asset participants regulated by FinCEN have reporting requirements under the Bank Secrecy Act, just like those regulated by the SEC and the CFTC. The three agencies—FinCEN, the SEC, and the CFTC—have historically coordinated in regulating digital assets, publishing a joint statement in 2019 on the topic. Accordingly, the bill's working group's reporting requirements should be expanded to include FinCEN.

The second bill directly related to digital assets has a slightly different goal than the first. The Automatic Boost to Communities Act, H.R.1030, seeks to establish a program under the Department of the Treasury providing monthly payments to consumers to aid in their COVID-19 economic recovery. On January 1, 2022, payments may be administered through a digital dollar account wallet referred to as a "FedAccount." Subsection (i)(1)(C) of the bill authorizes Federal Reserve banks to maintain these digital dollar account wallets. The bill proposes a partnership between digital dollar account wallets and post office branches. Postal banking as a concept has been around for over a century but has not been in effect since 1967.

Many members of Congress do not support postal banking or sending further stimulus payments to consumers. Regardless, several important features of this bill should not be overlooked, such as how the designation of Federal Reserve banks to maintain these wallets further codifies the Office of the Comptroller of the Currency's interpretive letter from 2020 stating that federally chartered banks could provide custody services for cryptocurrency. Additionally, the bill directs the Treasury to establish digital dollar cash wallets, "which shall be branded as 'eCash Wallets' and made available to any eligible individual to store, send, and receive digital coins or other digital currency instruments issued by the United States Treasury as legal tender." The eCash Wallets proposed in H.R.1030 could lay the strong groundwork toward deploying a CBDC or a similar government-backed digital currency.

Despite its potential to bolster the recognition and acceptance of digital assets, H.R.1030 will likely receive pushback from FinTechs. FinTechs will no longer be the primary conduit between consumers and the Treasury as they were during original stimulus checks made available to CashApp users who had their account and routing number on file with the Internal Revenue Service. A FinTech–government partnership has already been proven as a highly effective model for distributing funds as established by the success of FinTechs throughout the Paycheck Protection Program. Akin to The Clearing House versus FedNow for Real-Time Payments debate, people tend to favor incumbents, but the government still holds disproportionate power in this scenario. Consumer choice between the public and private option should be protected in both cases.

Looking Ahead

As we head into the second half of 2021, bolstering the post-COVID-19 economic recovery will remain a central concern for lawmakers as many of their constituents continue to face unprecedented rates of joblessness and economic hardships this year. Additionally, the theme of preventing illicit activity and terrorist financing through digital assets and virtual currencies will remain a top priority among lawmakers.

Legislation should take a risk-based approach rather than enacting blanket enforcement. Applying modern solutions to regulate modern financial technologies will require inter-governmental coordination and strong public-private coordination, especially as the FinTech industry may be impacted, either directly or indirectly, by several pieces of legislation introduced this year. Maintaining strong lines of communication between lawmakers and leaders in the FinTech industry will be imperative for achieving greater safety and soundness in the market without taking away from the United States' competitive edge in innovative technologies. Establishing definitional clarity for key terms such as digital assets, virtual currencies, digital currencies, etc., should be another priority for lawmakers. With no legal definition for many of these terms, it is critical to have uniformity between bill texts and regulatory agencies' definitions to facilitate industry compliance and rulemaking authority once a bill is passed.

Find out more about the Milken Institute FinTech Program