Fintech: Overview of Innovative Financial Technology and Selected Policy Issues

April 28, 2020

Congressional Research Service
https://crsreports.congress.gov
R46332

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46332

April 28, 2020

David W. Perkins, Coordinator
Specialist in Macroeconomic Policy

Fintech: Overview of Innovative Financial Technology and Selected Policy Issues

Advances in technology allow for innovation in the ways businesses and individuals perform financial activities. The development of financial technology—commonly referred to as *fintech*—is the subject of great interest for the public and policymakers. Fintech innovations could potentially improve the efficiency of the financial system and financial outcomes for businesses and consumers. However, the new technology could pose certain risks, potentially leading to unanticipated financial losses or other harmful outcomes. Policymakers designed many of the financial laws and regulations intended to foster innovation and mitigate risks before the most recent technological changes. This raises questions concerning whether the existing legal and regulatory frameworks, when applied to fintech, effectively protect against harm without unduly hindering beneficial technologies' development.

The underlying, cross-cutting technologies that enable much of fintech are subject to such policy trade-offs. The increased availability and use of the internet and mobile devices could offer greater convenience and access to financial services, but raises questions over how geography-based regulations and disclosure requirements can and should be applied. Rapid growth in the generation, storage, and analysis of data—and the subsequent use of Big Data and alternative data—could allow for more accurate risk assessment, but raises concerns over privacy and whether individuals' data will be used fairly. Automated decisionmaking (and the related technologies of machine learning and artificial intelligence) could result in faster and more accurate assessments, but could behave in unintended or unanticipated ways that cause market instability or discriminatory outcomes. Increased adoption of cloud computing allows specialized companies to handle technology-related functions for financial institutions, including providing cybersecurity measures, but this may concentrate financial cyber risks at a relatively small number of nonfinancial companies who may not be entirely comfortable with their regulatory obligations as financial institution service providers. Concerns over cyber risks and whether adherence to cybersecurity regulations ensure appropriate safeguards against those risks permeate all fintech developments.

Fintech deployment in specific financial industries also raises policy questions. The growth of nonbank, internet lenders could expand access to credit, but industry observers debate the degree to which the existing state-by-state regulatory regime is overly burdensome or provides important consumer protections. As banks have increasingly come to rely on third-party service providers to meet their technological needs, observers have debated the degree to which the regulations applicable to those relationships are unnecessarily onerous or ensure important safeguards and cybersecurity. New consumer point-of-sale systems and real-time-payments systems are being developed and increasingly used, and while these systems are potentially more convenient and efficient, there are concerns about the market power of the companies providing the services and the effects on people with limited access to these systems. Meanwhile, cryptocurrencies allow individuals to make payments entirely outside traditional financial systems, which may increase privacy and efficiency but creates concerns over money laundering and consumer protection. Fintech is providing new avenues to raise capital—including through crowdfunding and initial coin offerings—and changing the way companies trade securities and manage investments and may increase the ability to raise funds but present investor protection challenges. Under statute passed by Congress, insurance is primarily regulated at the state level where agencies are considering the implications to efficiency and risk that fintech poses in that industry, including peer-to-peer insurance and insurance on demand. Finally, firms across industries are using fintech to help them comply with regulations and manage risk, which raises questions about what role finetch should play in these systems.

Regulators and policymakers have undertaken a number of initiatives to integrate fintech in existing frameworks more smoothly. They have made efforts to increase communication between fintech firms and regulators to help firms better understand how regulators view a developing technology, and certain regulators have established offices within their organizations to conduct outreach. In another approach, some regulators have announced research collaborations with fintech firms to improve their understanding of new products and technologies. If policymakers determine that particular regulations are unnecessarily burdensome or otherwise ill-suited to a particular technology, they might tailor the regulations, or exempt companies or products that meet certain criteria from such regulations. In some cases, regulators can do so under existing authority, but others might require congressional action.

Contents

Figures

Appendixes

Contacts

Finance, Technology, and Recent Innovation

Finance and technological development have been inextricably linked throughout history. (Possibly, quite literally. The technology of writing in early civilization may have developed to record payments and debts.[1]) As a result, the term *fintech* is used to refer to a broad set of technologies being deployed across a variety of financial industries and activities. Although there is no consensus on which technologies qualify as new or innovative enough to be fintech, it is generally understood to mean recent innovations to the way a financial activity is performed that are made possible by rapid advances in digital information technology.[2] Underlying, cross-cutting technological advancements that enable fintech include increasingly widespread, easy access to the internet and mobile technology; increased data generation and availability and use of Big Data and alternative data; increased use of cloud computing services; the development of algorithmic decisionmaking (and the related technological evolutions toward machine learning and artificial intelligence); and the coevolution of cyber threats and cybersecurity.

The complementary use of these technologies to deliver financial services could potentially create benefits.[3] Many technologies aim to create efficiencies in financing, which reduce costs for financial service providers. Certain cost savings may be passed along to consumers through reduced prices. With lower prices, some customers that previously found services too expensive could enter the market. In addition, some individuals and businesses that previously could not access financial services because of price or lack of available financial information could gain access at lower prices or through increased data availability and improved data analysis. Fintech also may allow businesses to reach new customers that were previously restricted by geographic remoteness or unfamiliarity with products and services. Increased accessibility may be especially beneficial to traditionally underserved groups, such as low-income, minority, and rural populations.

However, fintech may also generate risks and result in undesirable outcomes. Predicting how an innovation with only a brief history of use will perform involves uncertainty, particularly without the experience of having gone through a recession. Thus, technologies may not ultimately allocate funds, assess risks, or otherwise function as efficiently and accurately as intended; they may instead generate unexpected losses. Some technologies aim to eliminate or replace a middle man, but in certain cases the middle man may in fact be useful or even necessary. For example, an experienced financial institution or professional may be able to explain and advise consumers on financial products and their risks. In addition, new fintech startups may be inexperienced in complying with consumer-protection laws. These characteristics may increase the likelihood that consumers using financial technology engage in a financial activity and take on risks that they do not fully understand and which unduly expose them to losses. Furthermore, some studies suggest that fintech's use can result in disparate impact on protected groups,[4] and that the increasing use

[1] Denise Schmandt-Besserat, *How Writing Came About* (Austin, TX: University of Texas Press, 1996), pp. 7-8.

[2] Patrick Schueffel, "Taming the Beast: A Scientific Definition of Fintech," *Journal of Innovation Management*, vol. 4, no. 4 (2016), pp. 32-33.

[3] Thomas Philippon, *The Fintech Opportunity*, National Bureau of Economic Research, Working Paper no. 22476, August 2016, pp. 2-9, at https://www.nber.org/papers/w22476.

[4] For example, see Robert Bartlett et al., *Consumer-Lending Discrimination in the FinTech Era*, National Bureau of Economic Research, Working Paper no. 25943, June 2019, at https://www.nber.org/papers/w25943.

of high-speed internet and mobile devices in finance may be leaving behind groups that cannot afford those services and devices.[5]

As financial activity increasingly uses digital technology, sensitive data are generated. On the one hand, data can be used to assess risks and ensure customers receive the best products and services. On the other hand, data can be stolen and used inappropriately, and there are concerns over privacy. This raises questions over data ownership and control—including consumers' rights and companies' responsibilities in accessing and using data—and whether companies that use and collect data face appropriate cybersecurity requirements.

Given that fintech may produce both positive and negative outcomes, Congress and other policymakers may consider whether existing laws and regulations appropriately foster the development and implementation of potentially beneficial technologies while adequately mitigating the risks those technologies may present. This report examines (1) underlying technological developments that are being used in financial services, (2) selected examples of financial activities affected by innovative technology, and (3) some approaches regulators have used to integrate new technologies or technology companies into the existing regulatory framework. Policy issues that may be of interest to Congress are examined throughout the report. Additional CRS products and resources also are identified throughout the report and in the **Appendix**. For a detailed examination of how fintech is regulated, see CRS Report R46333, *Fintech: Overview of Financial Regulators and Recent Policy Approaches*, by Andrew P. Scott.

Selected Underlying Technological Developments

Fintech is generally enabled by advances in general-use technologies that are used to perform financial activities. This section examines certain of these underlying technologies, including their potential benefits and risks, and identifies policy issues related to their use in finance that Congress is considering or may choose to consider.

Proliferation of Internet Access and Mobile Technology[6]

The proliferation of online financial services has a number of broad implications. One consideration is that online companies can often quickly grow to significant size shortly after entering a financial market.[7] This could enable the rapid growth of small fintech startups, possibly through capturing market share from incumbent financial firms. Adopting information technology, however, may require significant investment, which could advantage existing firms if they have increased access to capital. Larger technology firms—including Amazon, Apple, Facebook, and Google—have started financial services operations, and thus may become competitors to or partners with traditional financial institutions. Some industry experts predict that platforms offering the ability to engage with different financial institutions from a single channel will likely become the dominant model for delivering financial services.[8] These

[5] Terri Friedline, *Unequal Fintech Landscapes*, New America, March 2018, at https://newamerica.org/documents/2110/Unequal_Fintech_landscapes_FINAL.pdf.

[6] For questions regarding the use of the internet and mobile devices in financial services, congressional clients may contact David Perkins or Chris Jaikaran.

[7] Itay Goldstein and Andrew Karolyi, "Fintech: What's Real, and What's Hype," Knowledge@Wharton, March 12, 2019, at https://knowledge.wharton.upenn.edu/article/fintech.

[8] For example, see World Economic Forum, *Beyond Fintech: A Pragmatic Assessment Of Disruptive Potential In Financial Services*, August 2017, at http://www3.weforum.org/docs/Beyond_Fintech_-_A_Pragmatic_Assessment_of_Disruptive_Potential_in_Financial_Services.pdf.

developments may raise concerns that offering finance through digital channels could drive industry concentration.

Another consideration in this area involves consumer disclosures for financial products. In the past, voluntary or mandatory disclosures were designed to be delivered through paper. As firms move more of their processes online, they have begun to update these disclosures with electronic formats in mind. Consumers may interact differently with mobile or online disclosures than paper disclosures. Accordingly, firms may need to design online disclosures differently than paper disclosures to communicate the same level of information to consumers.

Possible Issues for Congress

The internet raises questions over what role geography-based financial regulations should play in the future. Many financial regulations are applied to companies and activities based on geographic considerations, as most areas of finance are subject to a dual federal-state regulatory system. For example, nonbank lenders and money transmitters are primarily regulated at the state level in each state in which they operate and are subject to those states' consumer-protection laws.[9] Fintech proponents argue the internet facilitates the provision of products and services on a national scale, and 50 separate state regulatory regimes are inefficient when applied to internet-based businesses that are not constrained by geography.[10] However, state regulators and consumer advocates assert state regulators' experience and local connection are best situated to regulate nonbank fintech companies.[11] An Office of the Comptroller of the Currency (OCC) initiative to accept applications for special-purpose bank charters that would allow certain fintechs to enter the national bank regulator regime, and subsequent lawsuits filed by state regulators to block such charters, exemplify this policy debate.[12] Another example is the debate over how a bank's geographic assessment area should be defined for the purposes of the Community Reinvestment Act (P.L. 95-128)—a law designed to encourage banks to meet the credit needs of the communities in which they operate—when so many services are delivered over the internet instead of at a physical branch location.[13]

Another area in which the internet raises concerns is how effective disclosure requirements are if they are sent electronically and read on a screen, when many disclosure forms may have been designed to be delivered and read on paper. Thus, although electronic disclosures can eliminate costs of printing and physically delivering disclosures, they may hinder customers' ability to read and understand them. Currently, financial regulatory agencies are responsible for implementing consumer-disclosure laws. Often, these agencies create either mandatory or *safe harbor*[14] form

[9] Conference of State Bank Supervisors, "Chapter 2: Overview of Nonbank Supervision," in *Reengineering Nonbank Supervision*, August 2019, pp. 3-9, at https://www.csbs.org/csbs-white-paper-reengineering-nonbank-supervision.

[10] Brian Knight, *Modernizing Financial Technology Regulations to Facilitate a National Market*, Mercatus Center at George Mason University, Mercatus on Policy, July 2017, at https://www.mercatus.org/publications/financial-markets/modernizing-financial-technology-regulations-facilitate-national.

[11] Testimony of Charles Clark, Director of Washington Department of Financial Institutions, before U.S. Congress, House Committee on Financial Services, Taskforce on Financial Technology, *Overseeing the Fintech Revolution: Domestic and International Perspectives on Fintech Regulation*, 116th Cong., 1st sess., June 25, 2019, at https://democrats-financialservices.house.gov/UploadedFiles/HHRG-116-BA00-Wstate-ClarkC-20190625.pdf.

[12] For more information on the Office of the Comptroller of the Currency (OCC) charter and legal challenges, see CRS Report R44614, *Marketplace Lending: Fintech in Consumer and Small-Business Lending*, by David W. Perkins.

[13] Mark Willis, *Updating CRA Geography: It's Not Just About Assessment Areas*, University of Pennsylvania Institute for Urban Research, Penn IUR Working Paper, September 2019, at https://penniur.upenn.edu/uploads/media/Mark_Willis_10-1.pdf.

[14] Safe harbor provisions provide that if the financial company uses the form they are presumed to be in compliance

designs that firms use to comply with these laws. Some financial regulatory agencies are either required or choose to test new consumer disclosures themselves before implementing a new disclosure requirement on the entities they regulate.[15] In the past, when most consumer credit origination occurred in person, this testing generally focused on paper delivery. As firms move more of their origination processes online, financial regulatory agencies might consider updating their consumer testing research with this format in mind.

Big Data[16]

Today, companies can easily collect, cheaply store, and quickly process data, regardless of its size, frequency, type, or location. *Big Data* commonly refers to the vast amounts and types of data an information technology (IT) system may handle. Big Data data sets share characteristics that require different hardware and software in IT systems to store, manage, and analyze those data. The four characteristics of Big Data are volume, velocity, variety, and variability.[17] *Volume* refers to a data set's extensive size. *Velocity* refers to the rate of flow for the data coming into, being processed by, and exiting the IT system. *Variety* refers to the differing types of data in a data set, such as information entered by a company analyst, images, data from a partner database, and data scraped from a website. Variety can also refer to different types of devices and subsystems in an IT system handling the data. *Variability* refers to the recognition that Big Data data sets can change with regard to the first three attributes. A data set may grow or shrink in volume, data may flow at different velocities, and a data set may include a different variety of data from one point in time to another. Changes in data variability drive IT systems to have a scalable architecture in order to manage the data sets.

Big Data is used to generate insights, support decisionmaking, and enable automation.[18] Big Data allows extensive and complex information to be analyzed with new methods (e.g., cloud computing resources, which are discussed in more detail below), leading users to understand and use the data in novel ways. Loan underwriting (evaluating the likelihood that a loan applicant will make timely repayment) is an example from the financial services industry. Loan underwriting has relied on an in-person process, using only a few data sources that might have been months or years old. Big Data enables underwriting to be performed online using a greater variety of more current data sources, potentially allowing for greater speed, accuracy, and confidence in loan decisions, but raises concerns over privacy and questions over what information is appropriate to collect and use.[19]

In recent years, new technologies have led to the development of new products in the financial services sector.[20] For example, as account information has become electronic, some products

with applicable disclosure laws.

[15] For example, the Consumer Financial Protection Bureau (CFPB) is required to test new disclosure forms with consumers before it requires the entities it regulates to provide the disclosures to its customers (P.L. 111-203, §1032).

[16] For questions regarding Big Data, congressional clients may contact Chris Jaikaran. For questions regarding the use of Big Data in financial services, congressional clients may contact Cheryl Cooper or Andrew Scott.

[17] National Institute of Standards and Technology (NIST), *NIST Big Data Interoperability Framework: Volume 1, Definitions*, Special Publication 1500-1r1, June 2018, at https://doi.org/10.6028/NIST.SP.1500-1r1.

[18] Gartner, "Gartner Glossary," at https://www.gartner.com/en/information-technology/glossary/big-data.

[19] U.S. Government Accountability Office (GAO), *Data and Analytics Innovation: Emerging Opportunities and Challenges*, GAO-16-659SP, September 2016, at https://www.gao.gov/assets/680/679903.pdf.

[20] For a more detailed discussion of financial services technology developments, see U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, July 2018, pp. 22-39, at https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-

allow consumers to combine accounts with several financial services providers on a single software platform, sometimes in combination with financial advisory services.[21] The underlying technology providers for these platforms are sometimes known as *data aggregators,* which refers to companies that compile information from multiple sources into a standardized, summarized form. One technology commonly used to collect account data is *web scraping,* a technique that scans websites and extracts data from them, and in general can be performed without a direct relationship with the website or financial firm maintaining the data.[22] As an alternative to web scraping, the financial institution managing the account may provide customer account information through a structured data feed or application program interface (API). Advantages and disadvantages exist when accessing alternative data by API rather than web scraping. For example, in certain circumstances web scraping may be an easier way for companies to gather data because it does not rely on bilateral company agreements, but some industry observers assert that APIs are more secure in terms of cybersecurity and fraud risks.[23] Using API banking standards to facilitate data sharing between financial firms is sometimes called *open banking*. New financial products that take advantage of data aggregation and open banking could provide benefits to consumers by enabling them to manage personal finances, automate or set goals for saving, receive personalized product recommendations, apply for loans, and perform other tasks. However, increasing access to these data may pose data security and privacy risks to consumers.

Possible Issues for Congress

Questions exist about how current laws and regulations should apply to Big Data. Typically, these questions relate to concerns about privacy and cybersecurity. One area of debate is whether data security standards should be prescriptive and government defined or flexible and outcome based. Some argue that a prescriptive approach can be inflexible and harm innovation, but others argue that an outcome-based approach might lead to institutions having to comply with a wide range of data standards.[24] In addition, questions exist about whether relevant data security laws continue to cover all sensitive individual financial information, or whether the scope of these laws should be expanded.[25]

Opportunities---Nonbank-Financi....pdf.

[21] For a more detailed discussion of data aggregation, consumer benefits, and consumer risks, see CFPB, "Request for Information Regarding Consumer Access to Financial Records," 81 *Federal Register* 83808, November 22, 2016, at https://www.consumerfinance.gov/policy-compliance/notice-opportunities-comment/archive-closed/request-information-regarding-consumer-access-financial-records/. For a summary of the feedback from this Request for Information, see CFPB, *Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights That Inform The Consumer Protection Principles*, October 18, 2017, at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

[22] Web scraping is used in many industries. See Timothy B. Lee, "Web Scraping Doesn't Violate Anti-Hacking Law, Appeals Court Rules," Ars Technica, September 9, 2019, at https://arstechnica.com/tech-policy/2019/09/web-scraping-doesnt-violate-anti-hacking-law-appeals-court-rules/.

[23] For more information on web scraping vs. application program interfaces (API), see U.S. Department of Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, July 2018, pp. 25-39, at https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf.

[24] For a longer discussion of this debate, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh.

[25] GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663, September 2013, p. 19, at https://www.gao.gov/assets/660/658151.pdf.

Alternative Data[26]

Alternative data generally refers to types of data that are not traditionally used by the national consumer reporting agencies to calculate a credit score.[27] It can include both financial and nonfinancial data. New technology makes it more feasible for financial institutions to gather alternative data from a variety of sources.

For example, the Consumer Financial Protection Bureau (CFPB) included the following list of alternative data in a 2017 Request for Information:

> Data showing trends or patterns in traditional loan repayment data.
>
> Payment data relating to non-loan products requiring regular (typically monthly) payments, such as telecommunications, rent, insurance, or utilities.
>
> Checking account transaction and cashflow data and information about a consumer's assets, which could include the regularity of a consumer's cash inflows and outflows, or information about prior income or expense shocks.
>
> Data that some consider to be related to a consumer's stability, which might include information about the frequency of changes in residences, employment, phone numbers or email addresses.
>
> Data about a consumer's educational or occupational attainment, including information about schools attended, degrees obtained, and job positions held.
>
> Behavioral data about consumers, such as how consumers interact with a web interface or answer specific questions, or data about how they shop, browse, use devices, or move about their daily lives.
>
> Data about consumers' friends and associates, including data about connections on social media.[28]

Alternative data could potentially be used to expand access to credit for consumers, such as currently credit invisible or unscorable consumers,[29] but also could create risks related to data security or consumer-protection violations.[30] Financial institutions can mitigate some of these

---

[26] For questions regarding alternative data, congressional clients may contact Chris Jaikaran. For questions regarding the use of alternative data in financial services, congressional clients may contact Cheryl Cooper.

[27] The consumer reporting agencies typically use past repayments on mainstream financial institution credit, among other data points, to calculate credit scores. For more information on the credit reporting industry, see CRS Report R44125, *Consumer Credit Reporting, Credit Bureaus, Credit Scoring, and Related Policy Issues*, by Cheryl R. Cooper and Darryl E. Getter.

[28] CFPB, "Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process," 82 *Federal Register* 11185, February 21, 2017, at https://www.consumerfinance.gov/policy-compliance/notice-opportunities-comment/archive-closed/request-information-regarding-use-alternative-data-and-modeling-techniques-credit-process/.

[29] The CFPB distinguishes between different types of consumers with limited credit histories. One category of consumers, referred to as *credit invisibles*, have no credit record at the three nationwide credit reporting agencies and, thus, do not exist for the purposes of credit reporting. According to the CFPB, this group represents 11.0% of the U.S. adult population, or 26 million consumers. Another category of consumers do exist (have a credit record), but they still cannot be scored or are considered *nonscorable*. Nonscorable consumers either have insufficient (short) histories or outdated (stale) histories. The insufficient and stale unscored groups, each containing more than 9 million individuals, collectively represent 8.3% of the U.S. adult population, or approximately 19 million consumers, according to the CFPB. See Kenneth P. Brevoort, Philipp Grimm, and Michelle Kambara, *Data Point: Credit Invisibles*, CFPB, May 2015, at http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf. For more information, see CRS Report R45979, *Financial Inclusion and Credit Access Policy Issues*, by Cheryl R. Cooper.

[30] For a longer discussion on the benefits and risks of alternative data to consumers, see CFPB, "Request for

risks through data encryption and other robust data governance practices.[31] Moreover, some prospective borrowers may be unaware that alternative data has been used in credit decisions, raising privacy and consumer-protection concerns.[32] Additionally, alternative data may pose fair lending risks if alternative data elements are correlated with prohibited classes, such as race or ethnicity.[33]

Alternative data could potentially increase accuracy, visibility, and scorability in credit reporting by including additional information beyond that which is traditionally used. The ability to calculate scores for previously credit invisible or nonscoreable consumers could allow lenders to better determine their creditworthiness. Arguably, using alternative data would potentially increase access to—and lower the cost of—credit for some credit invisible or unscorable individuals by enabling lenders to find new creditworthy consumers.[34] However, alternative data could potentially harm some consumers' existing credit scores if it includes negative or derogatory information.[35]

Possible Issues for Congress

The main statute regulating the credit reporting industry is the Fair Credit Reporting Act (FCRA; P.L. 91-508), enacted in 1970. The FCRA requires "that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit ... in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."[36] Using alternative data for credit reporting raises FCRA compliance questions. For example, alternative data providers outside of the traditional consumer credit industry may find FCRA data-furnishing requirements burdensome.

Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process," 82 *Federal Register* 11185-11188, February 21, 2017, at https://www.consumerfinance.gov/policy-compliance/notice-opportunities-comment/archive-closed/request-information-regarding-use-alternative-data-and-modeling-techniques-credit-process/.

[31] Encryption is a process that secures information from unwanted access or use by changing information which can be read (plaintext) and making it so that it cannot be read (ciphertext). For more information on encryption, see CRS Report R44642, *Encryption: Frequently Asked Questions*, by Chris Jaikaran; and CRS Report R44407, *Encryption: Selected Legal Issues*, by Richard M. Thompson II and Chris Jaikaran.

[32] For more information on data privacy and data protection law, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh.

[33] For example, a Charles River Associates report suggests that "geographic location, use of banking services, educational attainment, college or university attended and use of nonprime credit tend to be correlated with race and ethnicity." Bank regulatory agencies have not made it clear whether using this information is or is not a *legitimate business justification* (like, for example, using credit bureau information). For more information, see Marsha J. Courchane and David M. Skanderson, *Fair Lending in the Brave New World of Big Data*, Charles River Associates, May 2017, p. 5, at https://www.crai.com/sites/default/files/publications/FE-Fair-Lending-whitepaper-050317.pdf.

[34] Experian, "New Study Shows How Alternative Payment Data Helps U.S. Consumers' Credit Profiles," press release, February 25, 2015, at https://www.experianplc.com/media/news/2015/alternative-data-to-credit-reports-utilities-and-rent-2015/; and FinRegLab, *The Use of Cash Flow Data in Underwriting Credit: Empirical Research Findings*, July 2019, https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

[35] In its testimony to the House Financial Services Committee, the National Consumer Law Center suggested that gas and electric utility data and alternative financial product data may harm some consumers' credit scores, and that rental data with consumer protections would generally increase consumers' credit scores. The written testimony also mentioned telecommunication payment data and bank transaction or cashflow data as additional alternative data sources to study. See Testimony of Chi Chi Wu, in U.S. Congress, House Committee on Financial Services, *Who's Keeping Score? Holding Credit Bureaus Accountable and Repairing a Broken System*, hearings, 116th Cong., 1st sess., February 26, 2019, pp. 9-11, at https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-wstate-wuc-20190226.pdf.

[36] 15 U.S.C. §1681.

Some alternative data may have accuracy issues, and managing consumer disputes requires time and resources. These regulations may discourage some organizations from furnishing alternative data, even if the data could potentially help some consumers become scorable or increase their credit scores. In addition, consumers may not know what specific information alternative credit scoring systems use and how to improve the credit scores produced by these models.[37]

The CFPB and federal banking regulators have been monitoring alternative data developments in recent years, and in December 2019 they released a policy statement on the appropriate use of alternative data in the underwriting process.[38] The release followed a February 2017 CFPB request for information from the public about the use of alternative data and modeling techniques in the credit process.[39] Information from this request led the CFPB to outline principles for consumer-authorized financial data sharing and aggregation in October 2017.[40] These nine principles include, among other things, consumer access and usability, consumer control and informed consent, and data security and accuracy.[41] In addition, the CFPB issued its first (and, to date, only) *no-action letter* in 2017 to the Upstart Network, a company that uses alternative data, such as education and employment history, to make credit and pricing decisions.[42] In 2018, the Treasury Department released a report about regulatory recommendations, with a chapter on consumer financial data, including data sharing, aggregation, and other technology issues.[43]

Regulating Fintech: Consumer Protection Agencies

The mandate for the consumer protection agencies—CFPB and the Federal Trade Commission (FTC)—is largely to ensure that consumers are not unfairly or deceptively harmed by the practices of businesses under their jurisdiction while maintaining a competitive marketplace. Within the context of fintech, there are trade-offs between these objectives. For instance, encouraging firms to offer new kinds of consumer-friendly financial services can help create a competitive market, but the new products also can create the potential for unforeseen risks to consumers.

[37] Federal Reserve Governor Lael Brainard, "The Opportunities and Challenges of Fintech," remarks at the Conference on Financial Innovation at the Board of Governors of the Federal Reserve System, Washington, DC, December 2, 2016, at https://www.federalreserve.gov/newsevents/speech/brainard20161202a.htm.

[38] The Federal Reserve, CFPB, Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), and OCC, *Interagency Statement on the Use of Alternative Data in Credit Underwriting*, December 3, 2019, at https://files.consumerfinance.gov/f/documents/cfpb_interagency-statement_alternative-data.pdf.

[39] CFPB, "Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process," 82 *Federal Register* 11185, February 21, 2017.

[40] CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, October 18, 2017, at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

For a summary of the feedback that informed these principals, see CFPB, *Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights That Inform The Consumer Protection Principles*, October 18, 2017, at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

[41] CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, October 18, 2017, pp. 3-5, at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[42] A *no-action letter* is an official communication stating a regulator does not expect to take enforcement actions against particular companies in certain situations. For more information, see CFPB, "CFPB Announces First No-Action Letter to Upstart Network," press release, September 14, 2017, at https://www.consumerfinance.gov/about-us/newsroom/cfpb-announces-first-no-action-letter-upstart-network/.

[43] U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, July 2018, pp. 23-59, at https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf.

Similar to other financial regulators, the CFPB and FTC issue and promulgate regulations on issues pertinent to fintech,[44] such as payments and data security. In addition, both agencies have created outreach offices. The consumer protection agencies also use enforcement actions as tools to manage the effects of fintech on the financial system.

For a detailed examination of the consumer protection agencies' regulatory approaches and initiatives related to fintech, see CRS Report R46333, *Fintech: Overview of Financial Regulators and Recent Policy Approaches*, by Andrew P. Scott.

Automated Decisionmaking and Artificial Intelligence[45]

Performing financial activities often involves making decisions about how to allocate resources (e.g., whether a particular borrower should be given a loan or whether shares of a particular stock should be purchased at the current price) based upon analysis of information (e.g., whether the borrower has successfully paid back loans in the past or how much profit the stock-issuing company made last year). Historically, these complex tasks could only be performed by a human. More recently, technological advances have enabled computers to perform these tasks. This development creates potential benefits and risks, and has a number of financial regulatory implications.

Financial firms have used algorithms—precoded sets of instructions and calculations executed automatically—to enable computers to make decisions for a number of years, notably in the lending and investment management industries. Such automation may produce benefits if algorithmic analysis—perhaps using Big Data and alternative data, discussed previously—is better able to assess risks, predict outcomes, and allocate capital across the financial system than traditional human assessments. Eliminating inefficiencies through such automation could reduce the prices and increase the availability of and access to financial services, including for consumers, small businesses, and the underserved.[46]

Automation can also create certain concerns, particularly if automated programs may not perform as intended, possibly resulting in market instability or discrimination against protected groups. Algorithms can fail to perform as expected for reasons such as programmer error or unforeseen conditions, potentially producing unexpected losses. Because algorithms can execute actions so quickly and at large scale, those losses can be quite large. An illustrative event is the Flash Crash of May 6, 2010, in which the Dow Jones Industrial Average fell by roughly 1,000 points (and then rebounded) in intraday trading. The event was caused in part by an automated futures selling program that made sales more quickly than anticipated, resulting in tremendous market volatility.[47]

[44] Section 18 of the Federal Trade Commission Act (15 U.S.C. §57) authorizes the FTC to prescribe "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce." In addition, various other statutes authorize FTC rulemaking; such rulemaking is typically promulgated in accordance with 5 U.S.C. §553. One of the more significant rules the FTC promulgates with respect to financial institutions is the Safeguards Rule, which implements the data security provisions of the Gramm-Leach-Bliley Act (GLBA; P.L. 106-102). For more on GLBA and the Safeguards Rule, see CRS Insight IN11199, *Big Data in Financial Services: Privacy and Security Regulation*, by Andrew P. Scott.

[45] For questions regarding automated decisionmaking and artificial intelligence, congressional clients may contact Laurie Harris. For questions regarding the use of automated decisionmaking and artificial intelligence in financial services, congressional clients may contact David Perkins.

[46] Financial Stability Board, *FinTech and Market Structure In Financial Services: Market Developments and Potential Financial Stability Implications*, February 14, 2019, pp. 1-5, at https://www.fsb.org/wp-content/uploads/P140219.pdf.

[47] Commodity Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC), *Findings*

In addition, automated decisions may result in adverse impacts on certain protected groups in a discriminatory way.[48] In lending, for example, these discriminatory outcomes may include higher rates of denial for minority loan applicants than for white applicants with similar incomes and financial histories. Such discrimination can occur for a number of reasons, even if algorithm developers did not intend to discriminate. For example, the data set used to train the lending program is likely historical data of past loan recipients, and minorities may be underrepresented in that sample. By using these data to learn, the algorithm may similarly make fewer loans to underrepresented groups.[49]

Possible Issues for Congress

Programs enabled with artificial intelligence or machine-learning capabilities (i.e., automated programs that are able to change themselves with little or no human input) raise a number of policy concerns. The programs' complexity and the lack of human input needed to change their decisionmaking processes can make it exceedingly difficult for human programmers to predict what these programs will do and explain why they did it. Under these circumstances, the ability of regulators or other outside parties to understand what a program did, and why, may be limited or nonexistent. This poses a significant challenge for companies using AI programs to ensure they will produce outcomes that comply with applicable laws and regulations, and for regulators to effectively carry out their oversight duties.[50] In order to address this *black box* problem, some observers assert that regulators should set standards for how AI programs are developed, tested, and monitored.[51] If Congress decided such standards were necessary, it could encourage or direct financial regulatory agencies to develop them. In addition, it could direct the agencies to implement rules regarding the development and use of AI programs.

Cloud Computing[52]

Some have jokingly referred to cloud computing as "someone else's computer."[53] Although this is a facetious characterization, it succinctly describes the technology's core tenet. Cloud computing users transfer their information from a resource (e.g., hard drives, servers, and networks) that they own to one that they lease. Cloud computing alleviates users from having to buy, develop, and maintain technical resources and recruit and retain the staff to manage those resources. Instead,

Regarding The Market Events of May 6, 2010, Report of the Staffers of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues, September 30, 2010, pp. 1-8, at https://www.sec.gov/news/studies/2010/marketevents-report.pdf.

[48] Robert Bartlett et al., *Consumer-Lending Discrimination in the FinTech Era*, National Bureau of Economic Research, Working Paper no. 25943, June 2019, at https://www.nber.org/papers/w25943.

[49] Ernest Hamilton, "AI Perpetuating Human Bias in the Lending Space," Tech Times, April 2, 2019, at https://www.techtimes.com/articles/240769/20190402/ai-perpetuating-human-bias-in-the-lending-space.htm.

[50] Penny Crosman, "Can AI's 'black box' problem be solved?" *American Banker*, January 1, 2019, at https://www.americanbanker.com/news/can-ais-black-box-problem-be-solved.

[51] NIST, *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*, prepared in response to Executive Order 13859, August 9, 2019, pp. 3-6, at https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

[52] For questions regarding cloud computing, congressional clients may contact Chris Jaikaran. For questions regarding the use of cloud computing in financial services, congressional clients may contact David Perkins.

[53] David C. Brock, "Someone Else's Computer: The Prehistory of Cloud Computing," IEEE Spectrum, August 31, 2017, at https://spectrum.ieee.org/tech-history/silicon-revolution/someone-elses-computer-the-prehistory-of-cloud-computing.

cloud computing users pay providers who specialize in building and managing such resource infrastructures.

Cloud and high-performance computing architectures are better suited to processing Big Data than desktop computing. For many, this makes Big Data and cloud computing inextricably linked, and many commenters may refer to them interchangeably. Although this may be common practice, it is not technically accurate. Cloud computing refers to the computing resource (e.g., servers, applications, and service), whereas Big Data refers to the data a computing resource may use.

Cloud computing is used extensively by financial institutions, including banks,[54] insurers, and securities firms. Most financial firms store and process large amounts of data related to customer accounts and transactions. Typically, they also provide internet-based access to accounts and services through websites and mobile device apps and attract customers with these services. Meeting these business needs requires significant IT infrastructures and capabilities. For some financial companies, it may be less costly to pay a cloud service provider than to do everything in-house.[55]

Cloud computing introduces certain information security considerations and risks. Because data are not physically under the user's direct control (i.e., the data are no longer on a local, owned or controlled data server), the risk that access to those data may spread beyond intended users may be higher. Cloud providers counter that although they have *physical access* to the data, they do not necessarily have *logical access* to the data, nor do they own the data. In other words, they argue that although the data are hosted on their servers, they are encrypted or otherwise segmented from the provider's ability to access them.

Another related potential risk is commonly referred to as the *insider threat*—the risk that a trusted insider may purposely harm an employer or clients. Although users may limit unauthorized access to their data through encryption, an insider may be able to manipulate the encrypted files in such a manner that the information is kept confidential, but is no longer available. Users would then depend on the provider to restore a functioning backup of the data to resume data access. Or, the provider may offer encryption and key-management services to the user. In doing so, providers keep the data in their servers confidential between clients, but in a way that continues to afford that provider access to the user's data through encryption and decryption protocol maintenance.[56]

It should be noted that financial institutions that keep IT operations in-house also face the insider threat. However, migrating to cloud computing adds the cloud service provider's employees to the set of people that could pose an insider threat. In addition, a portion of the risk shifts from being internally managed by the financial institution to being externally managed by the cloud service provider. How well a financial institution manages these changing risk exposures depends on the quality of its policies, programs, and relationship with its cloud provider.

[54] This report will use the term *banks* to refer collectively to bank- and thrift-holding companies and their insured depository subsidiaries. This report does not refer to credit unions, though many of the issues related to banks examined in the report may also relate to credit unions.

[55] For more information on cloud computing characteristics, see Institute of International Finance, *Cloud Computing in the Financial Sector, Part 1: An Essential Enabler*, August 2018, pp. 1-4, at https://www.iif.com/Publications/ID/780/IIF-Cloud-Computing-paper-Part-1.

[56] For more information on encryption, see CRS Report R44642, *Encryption: Frequently Asked Questions*, by Chris Jaikaran, *Encryption: Frequently Asked Questions*, by Chris Jaikaran.

Possible Issues for Congress

Policymakers may examine whether the existing regulatory framework and rules appropriately balance the goals of guarding against the risks cloud computing presents to individual financial institutions and systemic stability, while not hindering beneficial innovations. Firms face operational risk (including legal and compliance risks) whether they operate and maintain IT in-house or outsource to a cloud provider.[57] Arguably, the risk of system disruptions and failures can be reduced by using a cloud provider with technical specialization in operating, maintaining, and protecting IT systems. Nevertheless, the nature of operational risk exposure changes when an institution adopts cloud computing.

This dynamic potentially raises friction between banks, cloud providers, and regulators regarding how banks' relationships with cloud providers should be regulated. The Bank Services Company Act (BSCA; P.L. 87-856) requires regulators to subject activities performed by bank service providers to the same regulatory requirements as if they were performed by the bank itself.[58] This could place substantial regulatory burden on banks and cloud services providers that see potential benefit to working together.[59]

The BSCA gives bank regulators supervisory authority over service providers.[60] Exercising this authority over cloud service providers, however, may raise challenges. At least initially, bank regulators may be unfamiliar with the cloud service industry, and cloud service providers may not be familiar with what is expected during bank-like examinations. The Federal Reserve's April 2019 examination of Amazon Websites Services (AWS; a cloud provider with bank clients) anecdotally illustrates the frictions in this area. Reportedly, AWS was wary of the process, and when examiners asked for additional documents and information, "the company balked, demanding to first see details about how its [AWS's] data would be stored and used, and who would have access and for how long."[61]

The cloud computing industry could pose risk to broader financial system stability in addition to risk at individual financial firms. Cloud computing resources are pooled, meaning cloud service providers build their resources to service many users simultaneously. This means many financial institutions could be using the same cloud provider, and are likely doing so because the cloud computing industry is highly concentrated at a small number of large providers (as discussed in more detail in the next section). Before cloud computing was available, successful cyberattacks or other technological disruptions would occur in individual institutions' systems. With cloud computing, an incident at one of the main cloud service providers could affect several firms

---

[57] Operational risk refers to the risk of loss due to failed internal controls, people, or systems, or from external events, and includes cyber risks (e.g., data breaches, insufficient customer data backups, and operating system hijackings). See Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk*, June 2011, at https://www.bis.org/publ/bcbs195.pdf, and European Banking Authority, *EBA Report on the Prudential Risks and Opportunities Arising From Fintech*, July 3, 2018, pp. 50-53, at https://eba.europa.eu/sites/default/documents/files/documents/10180/2270909/02c7859f-576e-421e-b243-a145c0eaa131/Report%20on%20prudential%20risks%20and%20opportunities%20arising%20for%20institutions%20from%20FinTech.pdf.

[58] 12 U.S.C. §1867(c).

[59] The broader issue of regulating bank relations with third-party technology service providers is also discussed in the "Banks and Third-Party Vendor Relationships" section later in this report.

[60] 12 U.S.C. §1867(c).

[61] Liz Hoffman, Dana Mattioli, and Ryan Tracy, "Fed Examined Amazon's Cloud in New Scrutiny for Tech," *Wall Street Journal*, August 1, 2019, at https://www.wsj.com/articles/fed-examined-amazons-cloud-in-new-scrutiny-for-tech-11564693812.

simultaneously, thus affecting large portions of the entire financial system. Large, systemically important banks are reportedly moving significant portions of their operations onto cloud services, which could exacerbate the effects of a disruption at a cloud service provider.[62] Certain financial regulators have mandates to ensure financial stability, so policymakers may choose to consider whether their authorities to regulate cloud service providers are appropriately calibrated.

Data Security[63]

Cybersecurity is a major concern of financial institutions and federal regulators.[64] In many ways, it is an important extension of physical security. For example, banks are concerned about both physical and electronic theft of money and other assets, and they do not want their businesses shut down by weather events or denial-of-service attacks.[65] Maintaining the confidentiality, security, and integrity of physical records and electronic data held by banks is critical to sustaining the level of trust that allows businesses and consumers to rely on the banking industry to supply services on which they depend.

Enormous amounts of data about individuals' personal and financial information are now generated and stored across numerous financial institutions. This could create additional opportunities for criminals to commit fraud and theft at a scale not previously possible. Instead of stealing credit cards one wallet at a time, someone hacking into a payment system can steal thousands of credit cards at once, and the internet allows stolen credit cards to be sold and used many times. For example, the 2013 Target data breach compromised approximately 70 million credit cards.[66] Whereas a traditional criminal method might involve stealing tax refund checks from individual mail boxes, the IRS announced in May 2015 that its computer system was hacked, allowing unknown persons to file up to 15,000 fraudulent tax returns worth up to $50 million total.[67] The Equifax breach that occurred between May and July 2017 potentially jeopardized almost 148 million U.S. consumers' identifying information.[68]

Possible Issues for Congress

To mitigate cybersecurity risks, financial institutions are subject to an array of laws and regulations. The basic authority that federal regulators use to establish cybersecurity standards emanates from the organic legislation that established the agencies and delineated the scope of

[62] Ibid.

[63] For questions regarding cybersecurity, congressional clients may contact Chris Jaikaran. For questions regarding cybersecurity in financial services, congressional clients may contact Andrew Scott.

[64] This report focuses only on cybersecurity in financial services. For more information on cybersecurity generally, see CRS In Focus IF10559, *Cybersecurity: An Introduction*, by Chris Jaikaran. For information on data protection law, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh.

[65] A denial-of-service attack is a cyberattack whereby an adversary delays authorized users from accessing system resources. They may delay such access by overwhelming the system, for example, by sending an excessive amount of internet traffic to a website, degrading its ability to operate.

[66] Rachel Adams, "Target to Pay $18.5 Million to 47 States in Security Breach Settlement," *New York Times*, May 23, 2017, at https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.

[67] John D. McKinnon and Laura Saunders, "Breach at IRS Exposes Tax Returns," *Wall Street Journal*, May 26, 2015, at https://www.wsj.com/articles/criminals-steal-taxpayer-data-via-irs-web-service-1432672691.

[68] Anna Maria Andriotis, "Equifax Identifies Additional 2.4 Million Affected by 2017 Breach," *Wall Street Journal*, March 18, 2018, at https://www.wsj.com/articles/equifax-identifies-additional-2-4-million-affected-by-2017-breach-1519918282.

their authority and functions. In addition, certain state and federal laws—including the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank; P.L. 111-203), the Gramm-Leach-Bliley Act of 1999 (GLBA; P.L. 106-102), and the Sarbanes-Oxley Act of 2002 (P.L. 107-204)—have provisions related to the cybersecurity of financial services that are often performed by banks. In addition, regulators issue guidance in a variety of forms designed to help banks evaluate their risks and comply with cybersecurity regulations.[69]

The existing framework was implemented before certain developments in financial technology, and risks related to cybersecurity arguably have increased with digitization's proliferation in finance. Successful hacks of financial institutions, such as those mentioned above, highlight the importance of financial services cybersecurity oversight. The framework governing financial services cybersecurity reflects a complex and sometimes overlapping array of state and federal laws, regulators, regulations, and guidance. However, whether this framework is effective and efficient, resulting in adequate protection against cyberattacks without imposing undue cost burdens on banks, is an open question.[70]

Concerns about data security aside, generating and analyzing data also raises privacy concerns. Individuals' transactions are increasingly recorded and analyzed by financial institutions. Debates over how financial institutions should be allowed to use or share consumer data between institutions remain unresolved.

For more information on these issues, see CRS Report R44429, *Financial Services and Cybersecurity: The Federal Role*, by N. Eric Weiss and M. Maureen Murphy; CRS In Focus IF10559, *Cybersecurity: An Introduction*, by Chris Jaikaran; and CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh.

Selected Technological Innovations in Finance

When innovative financial technology is developed for a specific financial market, activity, or product, it might raise questions over the degree to which existing applicable laws and regulations foster the potential benefits and protects against potential risks. This section examines certain fintech innovations, including their potential benefits and risks, and identifies related policy issues that Congress is considering or may choose to consider.

Lending[71]

Traditionally, consumer and small business lenders worked in person with prospective borrowers applying for a new loan. These lenders employed human underwriters to assess prospective borrowers' creditworthiness, determining whether the lender would extend credit to an applicant and under what terms. The underwriting process can be relatively laborious, time consuming, and costly. Dating back to at least 1989, with the debut of a general-purpose credit score called

[69] For example, the bank regulators, through the Federal Financial Institution Examination Council, issue a Cybersecurity Assessment Tool to help an institution identify its cybersecurity risks and its ability to address them.

[70] For example, see Greg Baer and Rob Hunter, *A Tower of Babel: Cyber Regulation for Financial Services*, Bank Policy Institute, Banking Perspectives, second quarter 2017, at https://www.theclearinghouse.org/banking-perspectives/2017/2017-q2-banking-perspectives/articles/cyber-regulation-for-financial-services.

[71] For questions regarding lending, congressional clients may contact David Perkins or Cheryl Cooper.

FICO,[72] automation has increasingly become a part of the underwriting process.[73] In general, automation in underwriting relies on algorithms—precoded sets of instructions and calculations executed by a computer—to determine whether to extend credit to an applicant and under what terms. In contrast, human underwriting relies on a person to use knowledge, experience, and judgement (perhaps informed by a numerical credit score) to make assessments.

More recently, with the proliferation of internet access and data availability, some new lenders—often referred to as *marketplace lenders* or *fintech lenders*—rely entirely or almost entirely on online platforms and algorithmic underwriting.[74] In addition, the abundance of alternative data about prospective borrowers now available to lenders—either publicly accessible or accessed with the borrower's permission—means lenders can incorporate additional information beyond traditional data provided in credit reports and credit scores into assessments of whether a particular borrower is a credit risk.[75] Potentially, more data about a borrower could allow a lender to accurately assess—and thus extend credit to—prospective borrowers for whom traditional information is lacking (e.g., people with thin credit histories)[76] or insufficient to make a determination about creditworthiness (e.g., small businesses).[77] However, such practices raise questions about what kind of data should be accessible and used in credit decisions and whether its use could result in disparate impacts or other consumer-protection violations. Although fintech lending remains a small part of the consumer lending market,[78] it has been growing quickly in recent years. According to the GAO, "in 2017, personal loans provided by these lenders totaled about $17.7 billion, up from about $2.5 billion in 2013."[79]

[72] FICO is a trademarked term that was originally an acronym that stood for Fair, Issac, and Company—the company that developed the score.

[73] Matthew Adam Bruckner, "The Promise and Perils of Algorithmic Lenders' Use of Big Data," *Chicago-Kent Law Review*, vol. 93, no. 1 (March 16, 2018), pp. 11-15, at https://scholarship.kentlaw.iit.edu/cklawreview/vol93/iss1/1/.

[74] U.S. Treasury Department, *Opportunities and Challenges in Online Marketplace Lending*, May 10, 2016, p. 5, at https://www.treasury.gov/connect/blog/Documents/Opportunities_and_Challenges_in_Online_Marketplace_Lending_white_paper.pdf.

[75] GAO, *Financial Technology: Agencies Should Provide Clarification on Lenders' Use of Alternative Data*, GAO-19-111, December 2018, p. 33, at https://www.gao.gov/assets/700/696149.pdf.

[76] A recent academic study from the Federal Reserve Bank of Philadelphia suggests that alternative data may expand credit access and improve credit terms for some consumers. See Julapa Jagtiani and Catharine Lemieux, *The Roles of Alternative Data and Machine Learning in Fintech Lending: Evidence from the LendingClub Consumer Platform*, Federal Reserve Bank of Philadelphia, Consumer Finance Institute, Working Paper 18-15, at https://www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2018/wp18-15r.pdf.

[77] Julapa Jagtiani and Catharine Lemieux, *The Roles of Alternative Data and Machine Learning in Fintech Lending: Evidence from the LendingClub Consumer Platform*, pp. 19-23.

[78] Making a comparison of the relative size of these lenders to the consumer credit industry as a whole is difficult. Borrowers often take out marketplace loans to pay down credit card debt and student loans, and thus arguably the entire unsecured consumer loan market is the appropriate comparison. If the comparison group is set inclusively with all consumer credit included, the $17.7 billion is a relatively small segment of an industry of about $3.8 trillion as of the end of 2017. See Federal Reserve, *Financial Accounts of the United States*, Consumer Credit Outstanding – G.19, historical data, at https://www.federalreserve.gov/releases/g19/HIST/cc_hist_sa_levels.html. In addition, marketplace lenders also make loans to small businesses and small business owners, and thus arguably small commercial and industrial loans also should be included in the comparison. However, marketplace loans are unlike credit card loans, in that they are *nonrevolving* (i.e., the amount loaned and term to pay back in full are specified), and they are unlike student loans in that the can be more easily discharged in bankruptcy. If one characterizes marketplace loans strictly as personal, nonrevolving, and unsecured loans that are not student loans, they would account for an estimated 8.7% of a $203.5 billion market at the end of 2017. See Federal Reserve, *Financial Accounts of the United States*, Data Download Program, at https://www.federalreserve.gov/datadownload/Choose.aspx?rel=z1. Upon congressional request, CRS will provide data.

[79] For a more detailed discussion of relevant laws fintech lenders must comply with and the lack of detailed guidance

Possible Issues for Congress

A general issue underlying many of the policy questions involving fintech in lending is whether the current regulatory framework appropriately fosters these technologies' potential benefits while mitigating the risks they may present. Some commentators argue that current regulation is unnecessarily burdensome or inefficient. Often these criticisms are based largely or in part on the argument that the state-by-state regulatory framework facing nonbank lenders is ill-suited to an internet-based (and hence borderless) industry.[80] Opponents of this view assert that state-level licensing and consumer-protection laws, including usury laws (laws that target lending at unreasonably high interest rates), are important safeguards that should not be circumvented.[81]

Additional policy questions arise in cases where banks and nonbanks have partnered with each other to issue loans, such as in an arrangement depicted in **Figure 1**. Fintech companies and banks enter into a variety of such arrangements in which one or the other may build the online, algorithmic platform; do the underwriting on the loan; secure the funding to make the loan; originate it; and hold it on its own balance sheet or sell it to investors.[82] These arrangements generally require a bank to closely examine its compliance obligations related to vendor relationship requirements, discussed in more detail in this report's "Banks and Third-Party Vendor Relationships" section. In addition, certain arrangements have raised legal questions concerning federal preemption of state usury laws—specifically, whether federal laws that allow *banks* to export their home states' maximum interest rates apply to loans that are originated by banks but later purchased by *nonbank* entities.[83] Whether applicable laws and regulations governing these arrangements are appropriately calibrated to ensure availability of needed and beneficial credit or expose consumers to potential harm through the preemption of important consumer protections is a matter of debate.

from regulators, see GAO, *Financial Technology: Agencies Should Provide Clarification on Lenders' Use of Alternative Data*, GAO-19-111, December 2018, pp. 9-10, at https://www.gao.gov/assets/700/696149.pdf.

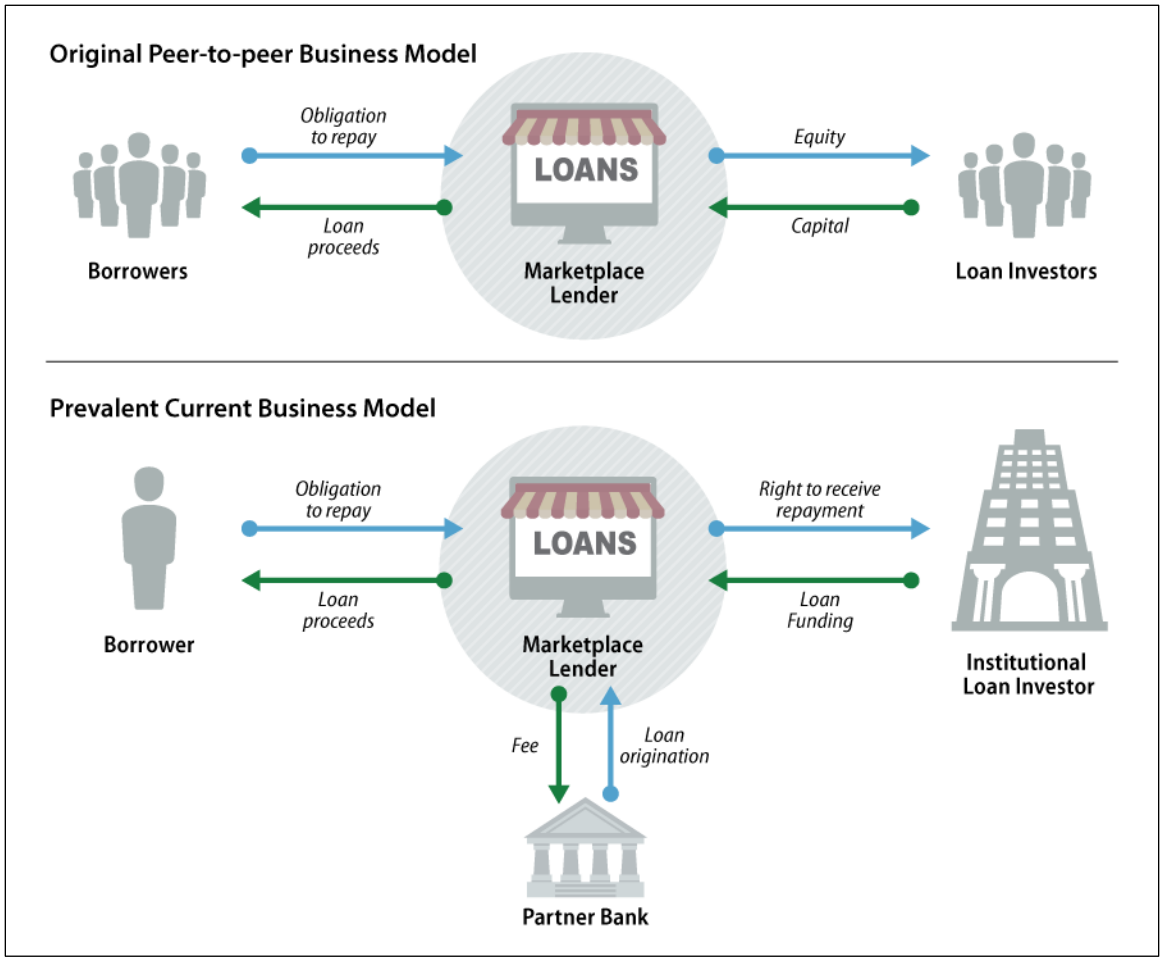
[80] Brian Knight, *Modernizing Financial Technology Regulations to Facilitate a National Market*, Mercatus Center at George Mason University, Mercatus on Policy, July 2017, at https://www.mercatus.org/publications/financial-markets/modernizing-financial-technology-regulations-facilitate-national.

[81] For example, see letter from Cynthia H. Coffman, Colorado Attorney General, Maura Healey, Massachusetts Attorney General, et al. to Sen. Mitch McConnell, Sen. Charles E. Schumer, Sen. Mike Crapo, and Sen. Sherrod Brown, June 27, 2018, at https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2018/07/AG-Madden-letter.pdf.

[82] GAO, *Financial Technology: Agencies Should Provide Clarification on Lenders' Use of Alternative Data*, GAO-19-111, December 2018, pp. 9-10, 15-18.

[83] For more information, see CRS Report R45726, *Federal Preemption in the Dual Banking System: An Overview and Issues for the 116th Congress*, by Jay B. Sykes.

Figure 1. Depiction of Common Marketplace Lending Models



Source: Congressional Research Service.

Another area of debate is how consumers will be affected by fintech in lending. Fintech lending proponents argue that, because financial technologies increasingly use quantitative analysis of new data sources, the technologies may expand credit availability to individuals and small businesses in a fair, safe, and less costly way. Thus, these proponents argue that overly burdensome regulation of these technologies could cut off a beneficial credit source to individuals who may have previously lacked sufficient credit access. However, some consumer advocates argue that inexperienced fintech lenders with a relative lack of federal regulatory supervision could inadvertently violate consumer-protection regulations. For example, these lenders may make loan decisions that unintentionally have a disparate impact on protected groups,[84] violating fair lending laws.[85] Also, when lenders deny a loan application they generally must send a notice

[84] For a hypothetical example, imagine a lender determines that which high school a person went to is correlated to how likely he or she is to default on a loan, and so writes an algorithm that favors certain high schools relative to others in terms of probability of application acceptance and interest rate charges. If the high school a person attends is also correlated to race, that algorithm could result in a disparate impact on a certain race.

[85] For example, the Equal Credit Opportunity Act (ECOA; 15 U.S.C. §§1691-1691f) generally prohibits discrimination in credit transactions based upon certain protected classes, including an applicant's sex, race, color, national origin, religion, marital status, age, and "because all or part of the applicant's income derives from any public assistance program." ECOA historically has been interpreted to prohibit both intentional discrimination and *disparate impact*

to the applicant explaining the reason for the denial, called an *adverse action notice*.[86] Some commentators question how well lenders will understand and thus be able to explain the reasons for an adverse action resulting from a decision made by algorithm.

For more detailed examination of these topics, see CRS Report R44614, *Marketplace Lending: Fintech in Consumer and Small-Business Lending*, by David W. Perkins; and CRS Report R45726, *Federal Preemption in the Dual Banking System: An Overview and Issues for the 116th Congress*, by Jay B. Sykes.

Banks and Third-Party Vendor Relationships[87]

As more banking transactions are delivered through digital channels, insured depository institutions (i.e., banks and credit unions) that lack the in-house expertise to set up and maintain these technologies are increasingly relying on third-party vendors, specifically technology service providers (TSPs), to provide software and technical support. In light of banks' growing reliance on TSPs, regulators are scrutinizing how banks manage their *operational risks*, the risks of loss related to failed internal controls, people, and systems, or from external events.[88] Rising operational risks—specifically cyber risks (e.g., data breaches, insufficient customer data backups, and operating system hijackings)—have compelled regulators to scrutinize banks' security programs aimed at mitigating operational risk. Regulators require an institution that chooses to use a TSP to ensure that the TSP performs in a safe and sound manner, and activities performed by a TSP for a bank must meet the same regulatory requirements as if they were performed by the bank itself.

The Bank Service Company Act (BSCA; P.L. 87-856) and the Gramm-Leach-Bliley Act (GLBA; P.L. 106-102) give insured depository institution regulators a broad set of authorities to supervise TSPs that have contractual relationships with banks. The BSCA directs the federal depository institution regulators to treat all activities performed by contract as if they were performed by the bank and grants them the authority to examine and regulate third-party vendors that provide services to banks, including check and deposit sorting and posting, statement preparation, notices, bookkeeping, and accounting. Section 501 of GLBA requires federal agencies to establish appropriate standards for financial institutions to ensure the security and confidentiality of customer information. Hence, the prudential depository regulators issued interagency guidelines in 2001 that require banks to establish information security programs. Among other things, banks must regularly assess the risks to consumer information (in paper, electronic, or other form) and implement appropriate policies, procedures, testing, and training to mitigate risks that could cause substantial harm and inconvenience to customers. The guidance requires banks to provide continuous oversight of third-party vendors such as TSPs to ensure that they maintain appropriate

discrimination, in which a facially neutral business decision has a discriminatory effect on a protected class. However, the Supreme Court's reasoning in a June 2015 decision involving the Fair Housing Act, another federal antidiscrimination law, has sparked debate about whether disparate impact claims are permissible under ECOA. For background on disparate impact claims, see CRS Report R44203, *Disparate Impact Claims Under the Fair Housing Act*, by David H. Carpenter, *Disparate Impact Claims Under the Fair Housing Act*, by David H. Carpenter.

[86] 12 C.F.R. §1002.9(a)(2).

[87] For questions regarding bank third-party vendors, congressional clients may contact Darryl Getter.

[88] See Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk*, June 2011, at https://www.bis.org/publ/bcbs195.pdf.

security measures. The regulators periodically update and have since released additional guidance pertaining to third-party vendors.[89]

Possible Issues for Congress

Regulation aimed at banks' relationships with third-party vendors such as TSPs has benefits in mitigating operational risks but imposes costs on banks that want to utilize available technologies. Banks, particularly community banks and small credit unions, may find it difficult to comply with regulator standards applicable to third-party vendors. For example, certain institutions may lack sufficient expertise to conduct appropriate diligence when selecting TSPs or to structure contracts that adequately protect against the risks TSPs may present. Some banks may also lack the resources to monitor whether the TSPs are adhering to GLBA and other regulatory or contract requirements. In addition, regulatory compliance costs are sometimes cited as a factor in banking industry consolidation, because compliance costs may be subject to economies of scale that incentivize small banks to merge with larger banks or other small banks to combine their resources to meet their compliance obligations.[90]

For more detailed examination of this issue, see CRS In Focus IF10935, *Technology Service Providers for Banks*, by Darryl E. Getter.

Regulating Fintech: Depository Regulators

The depository regulators—the Federal Reserve, FDIC, OCC, and National Credit Union Administration (NCUA)—face particular fintech-related challenges regarding how to ensure banks and credit unions can efficiently and safely interact with nonbank fintech companies.[91] Sometimes fintech companies partner with and offer services to banks or credit unions. Other times, they seek to compete with banks by offering bank or bank-like services directly to customers. In some circumstances, banks themselves can develop their own fintech.

Given their broad responsibilities, banking regulators can engage with and respond to fintech in numerous ways, including by amending rules and issuing guidance to clarify how rules apply to new products; supervising the relationships banks form with fintech companies; granting banking licenses to fintech companies: and conducting outreach with new types of firms to facilitate communication between industry and regulators.

For a detailed examination of the depository regulators' approaches and initiatives related to fintech, see CRS Report R46333, *Fintech: Overview of Financial Regulators and Recent Policy Approaches*, by Andrew P. Scott.

[89] For example, see the following releases: NCUA, *Evaluating Third Party Relationships*, Letter No.: 07-CU-13, December 2007; FDIC, *Guidance for Managing Third-Party Risk*, FIL-44-2008, June 6, 2008; Federal Financial Institutions Examination Council, "Financial Regulators Release Guidance for the Supervision of Technology Service Providers," press release, October 31, 2012, at https://www.ffiec.gov/press/pr103112.htm; FDIC, *Technology Outsourcing: Informational Tools for Community Bankers*, FIL-13-2014, April 7, 2014; FDIC Office of Inspector General, *Technology Service Provider Contracts with FDIC-Supervised Institutions*, Office of Audits and Evaluations, Report No. EVAL-17-004, February 2017; and NCUA Office of Inspector General, *Audit of the NCUA Information Technology Examination Program's Oversight of Credit Union Cybersecurity Programs*, Report No OIG-17-08, September 28, 2017.

[90] For more information on banking industry consolidation, see CRS Report R45518, *Banking Policy Issues in the 116th Congress*, coordinated by David W. Perkins; and CRS Insight IN11062, *BB&T and SunTrust: The Latest Proposed Merger in a Long-Term Trend of Banking Industry Consolidation*, by David W. Perkins.

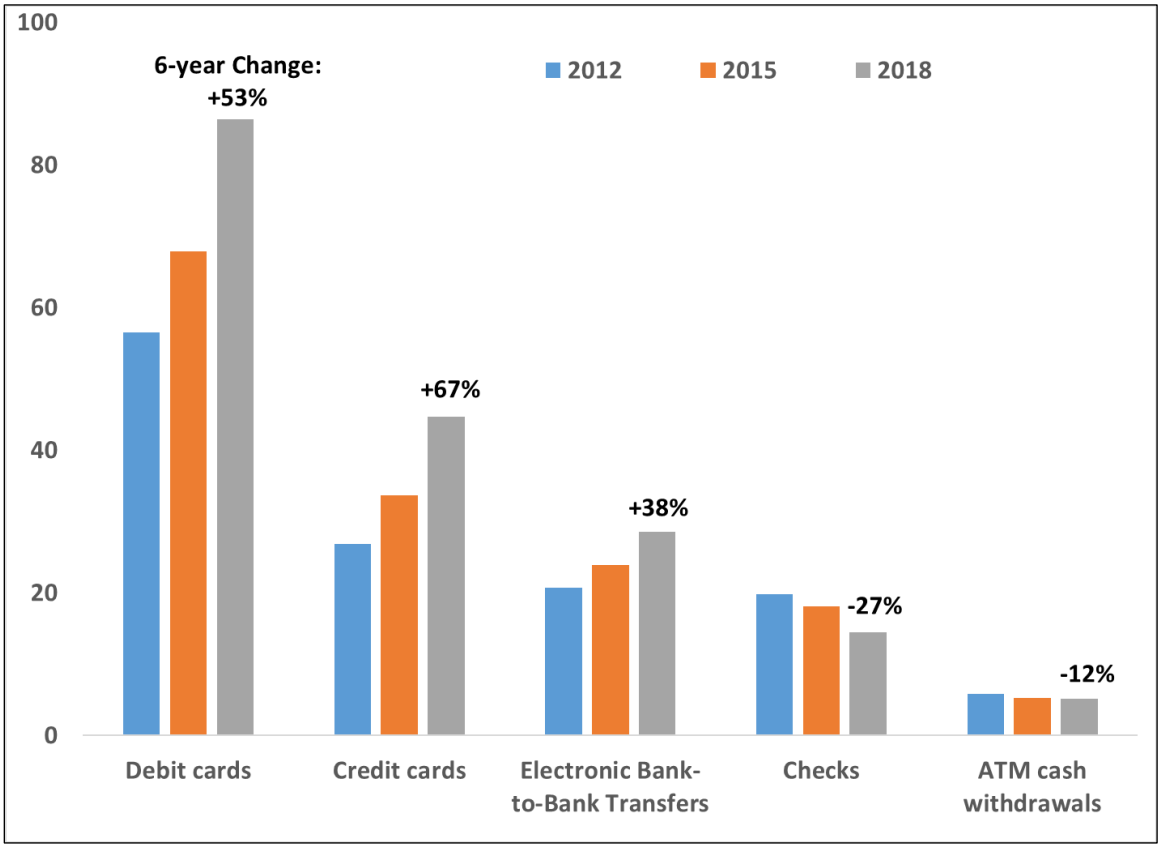
[91] The Federal Reserve, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency comprise the federal banking regulators. The National Credit Union Administration regulates federal credit unions. These four agencies are collectively the federal depository regulators.

Consumer Electronic Payments[92]

Consumers have several options to make electronic, noncash transactions, as shown in **Figure 2**. For instance, consumers can make purchases by swiping, inserting, or tapping a card to a payment terminal; they can store their preferred payment information in a digital wallet; or they can use an app to scan a barcode on a mobile phone that links to a payment of their choice. Merchants also enjoy electronic payments innovations that allow them to accept a range of payment types while limiting the need to manage cash.[93]

Figure 2. Consumers Payment Transactions, Selected Years

Number of U.S. Transactions, In Billions



Source: *The 2019 Federal Reserve Payments Study: Initial Data Release,* at https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm.

Despite the technology surrounding noncash payments, electronic payment networks eventually run through the banking system. Accessing these systems typically involves paying fees, which

[92] For questions regarding payment systems, congressional clients may contact Andrew Scott.

[93] For example, PayPal enables users to send and receive money via credit or debit card, directly through their bank, or by using funds stored in their account. Square offers a mobile payment terminal that enables consumers to swipe or insert a payment card. Further, cash can take longer to process at the point of sale (making change, counting coins, etc.), presents a security risk (carrying cash in a register), and takes time to store (depositing cash reserves in a bank account)—some of these issues are elucidated in Andy Newman, "Cash Might Be King, but They Don't Care," *New York Times*, December 25, 2017, at https://www.nytimes.com/2017/12/25/nyregion/no-cash-money-cashless-credit-debit-card.html.

may be burdensome on certain groups. For instance, while most Americans have a bank account, a 2017 survey found that almost a third of those who left the banking system did so because of fees associated with their account.[94] While some services, such as prepaid cards, allow individuals to make electronic payments without bank accounts, these options also often involve fees. As a result, cash payments may be the most affordable payment option for certain groups.

Possible Issues for Congress

If electronic payment methods significantly displace cash as a commonly accepted form of payment, that evolution could have both positive and negative outcomes. Proponents of reducing cash use argue that doing so will generate important benefits, such as reducing the costs associated with producing, transporting, and protecting cash. Conversely, opponents of reducing cash usage and acceptance argue that doing so would further marginalize people with limited access to the financial system. Although consumers tend to prefer using debit cards and credit cards, cash maintains an important role in retail payments and person-to-person (P2P) transfers, especially for smaller transactions and lower-income households.[95]

Electronic payments and cash displacement have various implications for the security and privacy of consumers and merchants. For example, not having cash on store premises can reduce the risk of theft while increasing fees paid to payment card processors.[96] Similarly, consumers may be denied services if they only use cash, but if they transition to electronic payments, the privacy offered by cash transactions' anonymous nature is eroded. Further, as more transactions occur over electronic payment systems, the data processed in these transactions are exposed to cybersecurity attacks. Policymakers may examine whether they should encourage or discourage an evolution away from cash based on their assessments of such a change's benefits and costs.

For more information on this topic, see CRS Report R45716, *The Potential Decline of Cash Usage and Related Implications*, by David W. Perkins.

Real-Time Payments[97]

There are several steps in the process of completing a payment, involving multiple systems run by various actors. *End user* payment services accessed by consumers and retailers are only run by the private sector. On the other hand, bank-to-bank payment messaging, clearing, and settlement can currently be executed through systems run privately or by the Federal Reserve.[98] The

[94] FDIC, *2017 FDIC National Survey of Unbanked and Underbanked Households*, October 2018, p. 4, at https://www.fdic.gov/householdsurvey/2017/2017report.pdf.

[95] A 2018 nationally representative survey from the Federal Reserve shows that 42% of consumers prefer to use debit cards, compared to 29% for credit cards and 22% for cash. The survey also shows that half of consumer transactions are less than $25, and 40% of those transactions are completed with cash; further, almost three-quarters of P2P transfers were cash transactions. Finally, although cash has generally trended down both in preference and usage over the past few years, households with annual incomes under $50,000 have increased their daily cash holdings. For more, see Raynil Kumar and Shaun O'Brien, *2019 Findings from the Diary of Consumer Payment Choice*, Federal Reserve System, Cash Product Office, June 2019, p. 7, at https://www.frbsf.org/cash/publications/fed-notes/2019/june/2019-findings-from-the-diary-of-consumer-payment-choice/.

[96] Claire Wang, *Cash Me If You Can: The Impacts of Cashless Businesses on Retailers, Consumers, and Cash Use*, Federal Reserve System, Cash Product Office, August 2019, at https://www.frbsf.org/cash/files/Cash-Me-If-You-Can-August2019.pdf.

[97] For questions regarding real-time payment systems, congressional clients may contact Marc Labonte.

[98] Federal Financial Institutions Examinations Council, *Wholesale Payment Systems*, IT Examination Handbook, July 2004, pp. 1-8, 12-17, at https://ithandbook.ffiec.gov/it-booklets/wholesale-payment-systems.aspx.

processing of these bank-to-bank electronic payments currently results in payment settlement occurring hours later or on the next business day after a payment is initiated.[99] However, advances in technology have made systems featuring real-time payments (RTP)—payments that settle almost instantaneously—possible.

The Federal Reserve plans to introduce an RTP system called FedNow in 2023 or 2024.[100] FedNow would be "a new interbank 24x7x365 real-time gross settlement service with integrated clearing functionality to support faster payments in the United States" that "would process individual payments within seconds ... (and) would incorporate clearing functionality with messages containing information required to complete end-to-end payments, such as account information for the sender and receiver, in addition to interbank settlement information."[101] FedNow is to be available to all financial institutions with a reserve account at the Federal Reserve.[102] It will require banks using FedNow to make funds transferred over it available to their customers immediately after being notified of settlement.[103]

Several private-sector initiatives are also underway to implement faster payments, some of which would make funds available to the recipient in real time (with deferred settlement) and some of which would provide real-time settlement.[104] Notably, the Clearing House introduced its RTP network (with real-time settlement), which is jointly owned by its members (a consortium of large banks), in November 2017; according to the Clearing House, it currently "reaches 50% of U.S. transaction accounts, and is on track to reach nearly all U.S. accounts in the next several years."[105]

Possible Issues for Congress

According to Federal Reserve Chair Jerome Powell, "the United States is far behind other countries in terms of having real-time payments available to the general public."[106]

---

[99] Federal Reserve, "Potential Modifications to the Federal Reserve Banks' National Settlement Service and Fedwire® Funds Service To Support Enhancements to the Same-Day ACH Service," 84 *Federal Register* 221223, May 16, 2019, at https://www.federalregister.gov/documents/2019/05/16/2019-09949/potential-modifications-to-the-federal-reserve-banks-national-settlement-service-and-fedwire-funds. The Federal Reserve sought comments on this proposal in November 2018. See Federal Reserve, "Potential Federal Reserve Actions to Support Interbank Settlement of Faster Payments," 83 *Federal Register* 221, November 15, 2018, p. 57351, at https://www.govinfo.gov/content/pkg/FR-2018-11-15/pdf/2018-24667.pdf.

[100] The Federal Reserve stated, "it will likely take longer for any service, whether the FedNow Service or a private-sector service, to achieve nationwide reach regardless of when the service is initially available." Federal Reserve, *Federal Reserve Actions to Support Interbank Settlement of Faster Payments*, Docket No. OP-1670, August 5, 2019, at https://www.federalreserve.gov/newsevents/pressreleases/files/other20190805a1.pdf.

[101] Federal Reserve, *Federal Reserve Actions to Support Interbank Settlement of Faster Payments*, Docket No. OP-1670, August 5, 2019, pp. 72-73, at https://www.federalreserve.gov/newsevents/pressreleases/files/other20190805a1.pdf.

[102] By statute, all depository institutions, including commercial banks and credit unions, and a select number of nonbank financial institutions may hold reserve accounts at the Fed.

[103] Federal Reserve, *Federal Reserve Actions to Support Interbank Settlement of Faster Payments*, Docket No. OP-1670, August 5, 2019, at https://www.federalreserve.gov/newsevents/pressreleases/files/other20190805a1.pdf.

[104] For an overview, see National Automated Clearing House Association, "Faster Payments 101," May 3, 2019, at https://www.nacha.org/system/files/2019-10/FasterPayments101_2019.pdf.

[105] The Clearing House, "The RTP Network: For All Financial Institutions," at https://www.theclearinghouse.org/payment-systems/rtp/institution.

[106] Federal Reserve, *Transcript of Chair Powell's Press Conference*, July 31, 2019, at https://www.federalreserve.gov/mediacenter/files/FOMCpresconf20190731.pdf.

Businesses and consumers would benefit from the ability to receive funds more quickly, particularly as a greater share of payments are made online or using mobile technology. A faster payment system may provide certain other benefits for low-income or liquidity-constrained consumers (colloquially, those living "paycheck to paycheck") who may more often need access to their funds quickly. In particular, many lower-income consumers say that they use alternative financial services, such as check cashing services and payday loans, because they need immediate access to funds.[107] Faster payments may also help some consumers avoid checking account overdraft fees.[108] Note, however, that some payments that households make would also be cleared faster—debiting their accounts more quickly—than they are in the current system, which could be harmful to some households.

The main policy issue regarding the Federal Reserve and RTP is whether Federal Reserve entry in this market is desirable. Some stakeholders question whether the Federal Reserve can justify creating a RTP system in the presence of competing private systems.[109] They fear that FedNow will hold back or crowd out private-sector initiatives already underway and could be a duplicative use of resources.[110] The Treasury Department supports Federal Reserve involvement on the grounds that it will help private-sector initiatives at the retail level.[111] Others, including many small banks, fear that aspects of payment and settlement systems exhibit some features of a natural monopoly (because of network effects), and, in the absence of FedNow, private-sector solutions could result in monopoly profits or anticompetitive behavior, to the detriment of financial institutions accessing RTPs and their customers (merchants and consumers).[112] From a societal perspective, it is unclear whether it is optimal to have a single provider or multiple providers in the case of a natural monopoly, particularly when one of those competitors is governmental. Multiple providers could spur competition that might drive down user costs, but more resources are likely to be spent on duplicative infrastructure.

RTP competition between the Federal Reserve and the private sector also has mixed implications for other policy goals, including innovation, ubiquity, interoperability, equity, and security.[113]

For more information on this topic, see CRS Report R45927, *U.S. Payment System Policy Issues: Faster Payments and Innovation*, by Cheryl R. Cooper, Marc Labonte, and David W. Perkins.

---

[107] Aaron Klein, "Real-Time Payments Can Help Combat Inequality," Brookings Institution, March 5, 2019, at https://spotlightonpoverty.org/spotlight-exclusives/real-time-payments-can-help-combat-inequality/.

[108] CFPB, *Consumer Voices on Overdraft Programs*, November 2017, pp. 16-19, at https://files.consumerfinance.gov/f/documents/cfpb_consumer-voices-on-overdraft-programs_report_112017.pdf.

[109] Thomas Wade, *Primer: What Is A Real-Time Payments System, And Who Should Operate It?* American Action Forum Insight, June 11, 2019, at https://www.americanactionforum.org/insight/primer-what-is-a-real-time-payments-system-and-who-should-operate-it/.

[110] The Clearing House, comment letter, Docket No. OP-1625, December 14, 2018, at https://www.federalreserve.gov/SECRS/2019/February/20190207/OP-1625/OP-1625_121418_133156_423844567989_1.pdf.

[111] U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities*, July 2018, p. 156, at https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf.

[112] Independent Community Bankers of America, comment letter, Docket No. OP-1625, December 14, 2018, at https://www.federalreserve.gov/SECRS/2019/March/20190315/OP-1625/OP-1625_121418_133342_402680988614_1.pdf; Open Payment Network, comment letter, Docket No. OP-1625, December 14, 2018, at https://www.federalreserve.gov/SECRS/2019/April/20190408/OP-1625/OP-1625_121418_133340_452781016249_1.pdf.

[113] See Aaron Rosenbaum et al., *Faster Payments: Market Structure and Policy Considerations*, Federal Reserve, Working Paper no. 2017-100, September 2017, at https://www.federalreserve.gov/econres/feds/files/2017100pap.pdf.

Cryptocurrency[114]

Cryptocurrencies are digital money in electronic payment systems that generally do not require government backing or the involvement of an intermediary, such as a bank. Instead, system users validate payments using public ledgers that are protected from invalid changes by certain cryptographic protocols. In these systems, individuals establish an account identified by a string of numbers and characters (often called an *address* or *public key*) that is paired with a password or *private key* known only to the account holder.[115] A transaction occurs when two parties agree to transfer digital currency (perhaps in payment for a good or service) from one account to another. The buying party will unlock the currency used as payment with her private key, allowing some amount to be transferred from her account to the seller's. The seller then locks the currency in her account using her own private key.[116] From the perspective of the individuals using the system, the mechanics are similar to authorizing payment on any website that requires an individual to enter a username and password. In addition, companies offer applications or interfaces that users can download onto a device to make transacting in cryptocurrencies more user-friendly. Individuals can purchase cryptocurrencies on exchanges for traditional government-issued money like the U.S. dollar (see **Figure 3**) or other cryptocurrencies, or they can earn them by doing work for the cryptocurrency platform.

Many digital currency platforms use blockchain technology to validate changes to the ledgers.[117] In a blockchain-enabled system, payments are validated on a public or distributed ledger by a decentralized network of system users and cryptographic protocols.[118] In these systems, parties that otherwise do not know each other can exchange something of value (i.e., a digital currency) because they trust the platform and its protocols to prevent invalid changes to the ledger.

[114] For questions regarding cryptocurrency and blockchain payment systems, congressional clients may contact David Perkins, Eva Su, or Chris Jaikaran.

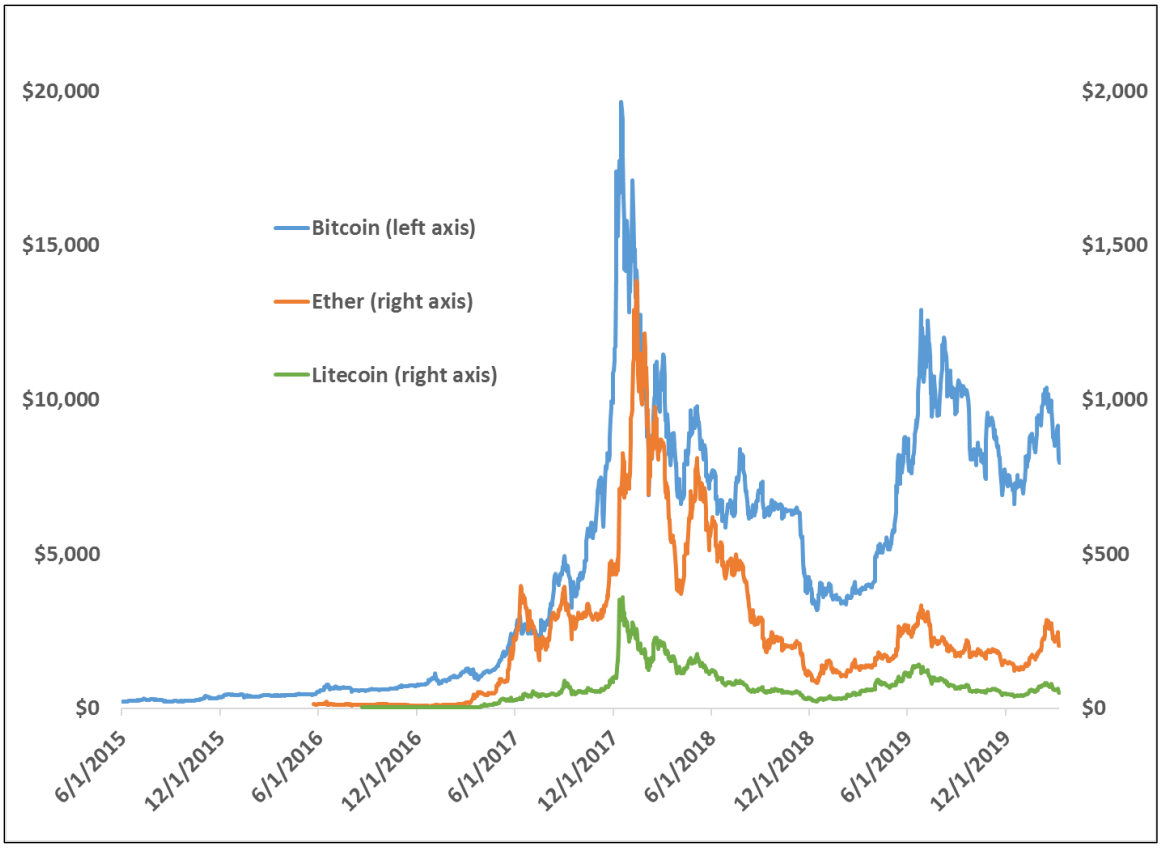
[115] In cryptography, a *key* is a value (e.g., a string of numbers) used for the operations of encryption, decryption, signature generation, or signature verification.

[116] David Mills et al., *Distributed Ledger Technology in Payments, Clearing, and Settlement*, Board of Governors of the Federal Reserve System, Financial and Economics Discussion Series 2016-095, Washington, DC, 2016, pp. 10-14, at https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf.

[117] For more information on blockchain technology, see CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran, *Blockchain: Background and Policy Issues*, by Chris Jaikaran.

[118] Dylan Yaga et al., *Blockchain Technology Overview*, NIST, NIST Interagency Report 8202, January 2018, pp. 12-25, at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

Figure 3. Cryptocurrency Prices, June 2015-March 2020



Source: Coinbase data, accessed through the Federal Reserve Bank of St. Louis Economic Data website at https://fred.stlouisfed.org/categories/33913.

Cryptocurrency advocates assert that a decentralized payment system operated through the internet could be faster and less costly than traditional payment systems and existing infrastructures.[119] Whether such efficiencies can or will be achieved remains an open question. However, the potential for increased payment efficiency from these systems is promising enough that certain central banks have investigated the possibility of issuing government-backed, electronic-only currencies—called central bank digital currencies (CBDCs)—in such a way that the benefits of certain alternative payment systems could be realized with appropriately mitigated risk. How CBDCs would be created and function are still matters of speculation at this time, and the possibility of their introduction raises questions about central banks' appropriate role in the financial system and the economy.[120]

Possible Issues for Congress

Whether cryptocurrencies are appropriately regulated is an open question. Cryptocurrency proponents argue that regulation should not stifle the development of a potentially beneficial payment system, while opponents argue that regulation should protect against criminals using

[119] Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers*, Mercatus Center at George Mason University, 2016, pp. 13-18, at https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf.

[120] For more information on this issue, see CRS Report R45427, *Cryptocurrency: The Economics of Money and Selected Policy Issues*, by David W. Perkins; and CRS Report R45716, *The Potential Decline of Cash Usage and Related Implications*, by David W. Perkins.

cryptocurrency to evade or hide their activities from authorities, or consumers potentially suffering losses from an untested technology. For anti-money laundering purposes, cryptocurrency regulation occurs at the exchanges that allow people to buy and sell cryptocurrencies either for government-backed fiat currencies or other cryptocurrencies. Generally, these exchanges must register as money transmitters at the state level and must report to the U.S. Treasury's Financial Crimes Enforcement Network as money services businesses at the federal level, and are subject to the applicable anti-money laundering requirements those types of companies face. However, cryptocurrency critics warn that their pseudonymous, decentralized nature nevertheless provides a new avenue for criminals to launder money, evade taxes, or sidestep financial sanctions.[121]

Consumer groups and other commentators are also concerned that digital currency users are inadequately protected against unfair, deceptive, and abusive acts and practices. The way cryptocurrencies are sold, exchanged, or marketed can subject cryptocurrency exchanges or other cryptocurrency-related businesses to generally applicable consumer-protection laws, and certain state laws and regulations are being applied to cryptocurrency-related businesses.[122] However, other laws and regulations aimed at protecting consumers engaged in electronic financial transactions may not apply. For example, the Electronic Fund Transfer Act of 1978 (EFTA; P.L. 95-630) requires traditional financial institutions engaging in electronic fund transfers to make certain disclosures about fees, correct errors when identified by the consumer, and limit consumer liability in the event of unauthorized transfers.[123] Because no bank or other centralized financial institution is involved in digital currency transactions, EFTA generally has not been applied to these transactions.[124]

Finally, some central bankers and other experts and observers have speculated that widespread cryptocurrency adoption could affect the ability of the Federal Reserve and other central banks to implement and transmit monetary policy, if one or more additional currencies that were not subject to government supply controls were also prevalent and viable payment options.

For more information on these issues, see CRS Report R45427, *Cryptocurrency: The Economics of Money and Selected Policy Issues*, by David W. Perkins; CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran; and CRS Report R45664, *Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals*, by Jay B. Sykes and Nicole Vanatko.

Capital Formation: Crowdfunding and ICOs[125]

Financial innovation in capital markets has generated new forms of fundraising for firms, including *crowdfunding* and *initial coin offerings*. Crowdfunding involves raising funds by

[121] For example, The U.S. Attorney's Office Southern District of New York, "Ross Ulbricht, the Creator and Owner of the 'Silk Road' Website, Found Guilty in Manhattan Federal Court on All Counts," press release, February 5, 2015, at https://www.justice.gov/usao-sdny/pr/ross-ulbricht-creator-and-owner-silk-road-website-found-guilty-manhattan-federal-court.

[122] Nicholas Gess and Andrew Ray, "State Attorneys General to Fintech Companies: Eyes on Cryptocurrencies," *All Things FinReg* (blog), Lexology, July 31, 2018, at https://www.lexology.com/library/detail.aspx?g=baaab9f9-af12-49e6-99d5-b063b0e61533.

[123] 15 U.S.C §1693c, §1693f, §1693g.

[124] See CRS Report R43339, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, by Edward V. Murphy and M. Maureen Murphy.

[125] For questions regarding capital formation, congressional clients may contact Eva Su.

soliciting investment or contributions from a large number of individuals, generally through the internet.[126] Initial coin offerings (ICO) raise funds by selling digital coins or tokens—generally created and transferred using blockchain technology—to investors; the coins or tokens allow investors to access, make purchases from, or otherwise participate in the issuing company's platform, software, or other project.[127] In cases where crowdfunding and ICOs meet the legal definition of a securities offering, they are subject to securities law and regulation by the Securities and Exchange Commission (SEC).[128]

Four kinds of crowdfunding exist: (1) donation crowdfunding, where contributors give money to a fundraising campaign and receive in return, at most, an acknowledgment; (2) reward crowdfunding, where contributors give to a campaign and receive in return a product or a service; (3) peer-to-peer lending crowdfunding, where investors offer a loan to a campaign and receive in return their capital plus interest; and (4) equity crowdfunding, where investors buy stakes in a company and receive in return company stocks.[129] Donation and reward crowdfunding are relatively lightly regulated because contributors are in effect giving without expectation of gaining anything of monetary value in return or preordering a product, respectively. Equity crowdfunding may meet the criteria of a securities offering, and in such cases it is subject to SEC regulation,[130] as are certain peer-to-peer lending arrangements in which a security is issued.[131]

ICOs are a relatively new approach to raising capital.[132] A typical ICO transaction involves the issuer selling new digital coins or tokens—also referred to as *digital assets* or, in cases in which they qualify as securities, *digital asset securities*—to individual or institutional investors. Investors can often pay in traditional fiat currencies (e.g., U.S. dollars) or cryptocurrencies (e.g., Bitcoin, Ethereum) pursuant to the terms of each individual ICO.[133] ICOs are often compared with the traditional financial world's initial public offerings (IPOs) because both are methods companies use to acquire funding. The main difference is that IPO investors receive an equity stake representing company ownership, rather than a digital asset. Coin or token purchasers can generally redeem the coins for goods or services from the issuing enterprise, or hold them as investments in the hope that their value will increase if the company is successful. Although every ICO is different, issuers are generally able to make transfers without an intermediary or any geographic limitation.[134]

---

[126] SEC, "Updated Investor Bulletin: Crowdfunding for Investors," May 10, 2017, at https://www.sec.gov/oiea/investor-alerts-bulletins/ib_crowdfunding-.html (hereinafter SEC, "Updated Investor Bulletin: Crowdfunding for Investors").

[127] SEC, "Investor Bulletin: Initial Coin Offerings," July 25, 2017, at https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings (hereinafter SEC, "Investor Bulletin: Initial Coin Offerings").

[128] SEC, "Updated Investor Bulletin: Crowdfunding for Investors"; and SEC, "Investor Bulletin: Initial Coin Offerings."

[129] Garry Gabison, *Understanding Crowdfunding and its Regulations*, European Commission, 2015, at http://publications.jrc.ec.europa.eu/repository/bitstream/JRC92482/lbna26992enn.pdf.

[130] SEC, "Crowdfunding," 80 *Federal Register* 71388-71390, November 16, 2015.

[131] Marc Franson and Peter Manbeck, *The Regulation of Marketplace Lending: A Summary of the Principal Issues*, Chapman and Cutler LLP, April 2019, pp. 89-129, at https://www.chapman.com/media/publication/926_Chapman_Regulation_of_Marketplace_Lending_2019.pdf.

[132] For more information on securities regulation and initial coin offerings, see CRS Report R45301, *Securities Regulation and Initial Coin Offerings: A Legal Primer*, by Jay B. Sykes.

[133] SEC, "Investor Bulletin: Initial Coin Offerings."

[134] SEC Chairman Jay Clayton, "Statement on Cryptocurrencies and Initial Coin Offerings," December 11, 2017, at https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

Possible Issues for Congress

Policymakers are now considering whether these new innovations fit well within the existing regulatory framework, or whether the framework should be adapted to address the risks and benefits that they pose. In general, policymakers and regulators have attempted to provide regulatory clarity and investor protection without hindering financial innovation and technological advancements.

Currently, equity crowdfunding debates typically involve questions over how broadly crowdfunding exemptions from certain SEC registration requirements should be applied. Generally, public equity offerings, such as stock issuances, involve a number of costs, including paying an investment bank to price the stock and find investors. In addition, the offering must be registered with the SEC and the company must disclose certain information to investors.[135] Crowdfunding may be less costly than traditional public offerings in certain respects and thus might present a new avenue for small businesses without the resources or expertise to complete a traditional IPO to raise funds.

In 2012, Title III of the Jumpstart Our Business Startups Act (JOBS Act; P.L. 112-106) created an exemption from registration for internet-based securities that made offerings of up to $1 million (inflation-adjusted) over a 12-month period.[136] Certain companies that are still relatively small by some measures may nevertheless not qualify for the exemption, and certain of those companies may find the costs of raising funds through an equity issuance prohibitively high.[137] Title III includes certain investor protection provisions, including limitations on investors' investment amounts and issuer disclosure requirements. However, exempting an issuer from registration may weaken investor protections. Thus, what the appropriate criteria should be to allow an equity crowdfunding issuer to forego registration requirements is a matter of debate.

Regarding ICOs, issuers and investors face varying degrees of uncertainty when determining how or if securities laws and regulations apply to them.[138] It may not always be clear whether a digital asset is a security subject to SEC regulation. Meanwhile, ICO and digital asset investors—which may include less-sophisticated retail investors, who may not be positioned to comprehend or tolerate high risks—may be especially vulnerable to new types of fraud and manipulation, leading to questions about whether investor protections in this area are adequate. There appear to be high levels of ICO scams and business failures. For example, one 2018 study from the ICO advisory firm Satis Group found that 81% of ICOs are scams and another 11% fail for operational reasons.[139] Digital assets may be an attractive method for scammers since transactions in digital assets do not have the same protections as traditional transactions. For example, banks can delay, halt, or reverse suspicious transactions and link transactions with user identity, while many digital asset transactions are generally irreversible.[140]

---

[135] PwC Deals, *Considering an IPO to Fuel Your Company's Future? Insight into the Costs of Going Public and Being Public*, November 2017, at https://www.pwc.com/us/en/deals/publications/assets/cost-of-an-ipo.pdf.

[136] P.L. 112-106, 126 Stat. 306 (2012).

[137] SEC, "Crowdfunding," 80 *Federal Register* 71388-71389, November 16, 2015.

[138] For more information, see CRS In Focus IF11004, *Financial Innovation: Digital Assets and Initial Coin Offerings*, by Eva Su.

[139] Satis Group, *Crypto-asset Market Coverage Initiation: Network Creation*, July 11, 2018, at https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ.

[140] Financial Industry Regulatory Authority (FINRA), "Initial Coin Offerings (ICOs)—What to Know Now and Time-Tested Tips for Investors," Investor Alert, August 16, 2018, at http://www.finra.org/investors/alerts/initial-coin-offerings-what-to-know.

The SEC has taken initiatives to address some of these issues. In September 2017, the SEC established a new Cyber Unit and increased its monitoring of and enforcement actions against entities engaged in digital asset transactions.[141] Since that time, the SEC has increased the frequency of enforcement actions against issuers—the end recipients of ICO funding—as well as market intermediaries (i.e., broker-dealers and investment managers). In addition to the enforcement activities against entities for noncompliance with securities regulations, the SEC has obtained court orders to halt allegedly fraudulent ICOs.[142]

Related Issue: Digital Asset "Exchanges"[143]

Digital assets, often referred to as *crypto assets*, among other terminology, are digital representations of value made possible by cryptography and blockchain, and include the coins and tokens offered through ICOs. Within the past two years, this new asset class has experienced rapid growth, high volatility, maturing practices, and regulatory scrutiny.[144] About 300 platforms are offering digital asset trading and referring to themselves as "exchanges" as of December 2019.[145] In addition, platforms trading digital assets appear to resemble securities exchanges, as they bring together buyers and sellers, execute trades, and display prices. However, many such platforms, if they are regulated at all, are registered as money-transmission services (MTSs) instead of SEC-regulated national securities exchanges.[146] The SEC issued a statement in 2018 clarifying that online platforms for buying and selling digital assets that qualify as securities could be unlawful.[147]

The SEC-regulated exchanges are designed to protect investors against fraudulent and manipulative activities—the very activities frequently observed in digital asset trading. One widely cited academic study illustrates the scale of potential damage one digital asset market manipulation could create. The study argues that a single market manipulator likely fueled half of Bitcoin's 2017 price surge that pushed its price close to $20,000.[148] The activities were reportedly carried out through the largest digital asset "exchange" at that time—Bitfinex. A group of cryptocurrency investors has filed a class complaint against Bitfinex and Tether—a company that administers a cryptocurrency of the same name—for $1.4 trillion in damages.[149]

The SEC took its first enforcement action against an unregistered digital asset "exchange" in 2018. The SEC stated that the platform "had both the user interface and underlying functionality of an online national securities exchange and was required to register with the SEC or qualify for an exemption," but was perceived to have failed to do so.[150]

[141] SEC, "SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors," press release, September 25, 2017, at https://www.sec.gov/news/press-release/2017-176.

[142] SEC, "Cyber Enforcement Actions," at https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

[143] For questions regarding digital asset securities "exchanges," congressional clients may contact Eva Su.

[144] Financial Stability Board, *Crypto-assets Report to the G20 on Work by the FSB and Standard-setting Bodies*, July 16, 2018, at http://www.fsb.org/wp-content/uploads/P160718-1.pdf.

[145] CoinMarketCap, "Top 100 Cryptocurrency Exchanges by Trade Volume," at https://coinmarketcap.com/rankings/exchanges.

[146] MTSs are money transfer or payment operations that are mainly subject to state, rather than federal, regulations. Marco Santori, "What Is Money Transmission and Why Does It Matter?" Coin Center, April 7, 2015, at https://coincenter.org/entry/what-is-money-transmission-and-why-does-it-matter.

[147] For more details, see SEC, "Statement on Potentially Unlawful Online Platforms for Trading Digital Assets," March 7, 2018, at https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading.

[148] John Griffin and Amin Shams, *Is Bitcoin Really Un-Tethered?* SSRN, October 28, 2019, at https://ssrn.com/abstract=3195066.

[149] Phillip Rosenstein, "$1.4T Bitcoin Manipulation Case Preposterous, Tether Says," Law360, November 15, 2019, at https://www.law360.com/articles/1220333/print?section=fintech; and New York Attorney General, "Attorney General James Announces Court Order Against 'Crypto' Currency Company Under Investigation For Fraud," press release, April 25, 2019, at https://ag.ny.gov/press-release/2019/attorney-general-james-announces-court-order-against-crypto-currency-company.

[150] SEC, "SEC Charges EtherDelta Founder With Operating an Unregistered Exchange," press release, November 8, 2018.

If digital asset trading platforms are buying and selling securities and fall within the SEC's regulatory regime, securities regulation's basic objectives should arguably continue to apply.[151] However, some observers, including international authorities, believe that, although digital asset trading platforms may face issues similar to traditional exchanges, regulatory approaches may still need to be adjusted to account for particular operating models that may amplify risks differently.[152]

For more information on these issues, see CRS Report R46208, *Digital Assets and SEC Regulation*, by Eva Su; CRS Report R45221, *Capital Markets, Securities Offerings, and Related Policy Issues*, by Eva Su; and CRS Report R45301, *Securities Regulation and Initial Coin Offerings: A Legal Primer*, by Jay B. Sykes.

High-Frequency Securities and Derivatives Trading[153]

Although, there is no universal legal or regulatory definition of high-frequency trading (HFT), the term generally refers to a subset of algorithmic trading in financial instruments, such as equity securities, derivatives, and cryptocurrencies, that is conducted by supercomputers executing trades within microseconds or milliseconds. It has grown substantially over the past 15 years and currently accounts for roughly 50% to 60% of the trading volume in domestic equity markets.[154] Depending on trading strategy and market conditions, evidence suggests that HFT in some cases can have either certain positive effects on market quality (e.g., increased liquidity, smaller spreads, decreased short-term volatility, and improved price discovery) or certain negative effects (e.g., decreased liquidity, higher volatility, and higher transaction costs for certain investors).[155]

Generally, traders who employ HFT strategies are attempting to earn a small profit per trade on a huge number of trades. This is achieved through automated trading by computers programmed to execute certain kind of trades in response to specific market data and involves rapid order placement. Broadly speaking, these strategies can be categorized as passive or aggressive strategies. Passive strategies include *arbitrage trading*—attempts to profit from price differentials for the same stocks or their derivatives traded on different trading venues; and *passive market making*, in which profits are generated by spreads between the difference or the spread between the prices at which securities are bought and sold. Aggressive strategies include those known as *order anticipation* or *momentum ignition* strategies.[156]

---

[151] SEC, *Statement on Digital Asset Securities Issuance and Trading*, November 16, 2018, at https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading; and Board of the International Organization of Securities Commissions, *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms*, May 2019, at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf.

[152] G7 Working Group on Stablecoins, *Investigating The Impact of Global Stablecoins*, October 2019, at https://www.bis.org/cpmi/publ/d187.pdf.

[153] For questions regarding high-frequency trading, congressional clients may contact Gary Shorter.

[154] Molly Wood, "Too much High-Frequency Trading Can Rig the Market, IEX Founder Says," Marketplace, September 18, 2019, at https://www.marketplace.org/2018/09/18/too-much-high-frequency-trading-can-rig-market-says-iex-exchange-founder/.

[155] Staff of the Division of Trading and Markets, *Equity Market Structure Literature Review Part II: High Frequency Trading*, SEC, March 18, 2014, pp. 8-11, at https://www.sec.gov/marketstructure/research/hft_lit_review_march_2014.pdf.

[156] *Order anticipation* involves traders using computer algorithms to identify large institutional orders that sit in dark pools or other stock order trading venues. As part of it, high-frequency traders may repeatedly submit small-sized exploratory trading orders intended to detect orders from large institutional investors. In *momentum ignition* strategies an HFT firm initiates a series of orders or trades aimed at causing rapid up or down securities price movements. Such traders "may intend that the rapid submission and cancellation of many orders, along with the execution of some trades,

Regulators have been scrutinizing HFT practices for years. The SEC oversees HFT and other trading in the securities markets and the more limited securities-related derivatives markets that it regulates. The CFTC oversees any HFT, along with other types of trading, in the derivatives markets it regulates. These markets include futures, swaps, and options on commodities and most financial instruments or indices, such as interest rates.

Possible Issues for Congress

HFT's supporters argue that by quickly executing many trades, often in response to a perceived price inefficiency, HFT improves market quality in a number of ways. Surveys of empirical research suggest that in both equity and foreign exchange markets, HFT appears to have narrowed bid-ask spreads, bolstered market liquidity, reduced some measures of price volatility, and improved the price discovery process.[157] Some commentators argue that HFT is just the latest technological innovation in a financial activity that has a long history of coevolution with technology, and that market participants and regulators are well practiced at incorporating such innovations.[158]

Some studies suggest, however, that aggressive HFT strategies should be a matter of public policy concern.[159] Such strategies arguably share similarities to practices such as *front-running* (when an entity conducts a securities trade while knowing of a future transaction that will have an effect on the price of the securities being traded) and *spoofing* (offering to buy or sell securities with an intent to cancel the bid or offer before execution), both of which can be illegal.[160] In addition, regulators have expressed concerns over whether certain aggressive HFT strategies may be associated with increased market fragility and volatility, such as that demonstrated in the Flash Crash of May 6, 2010, in which the Dow Jones Industrial Average (DJIA) fell by roughly 1,000 points (and then rebounded) in intraday trading.[161]

Arguably the most ambitious market surveillance project in SEC history, the ongoing implementation of Consolidated Audit Trail (CAT) is a direct response to the perceived dearth of market data available during the regulatory analysis of the Flash Crash's causes and the role HFT

---

will "spoof" the algorithms of other traders into action and cause them to buy (or sell) more aggressively. Alternatively, the trader may intend to trigger standing stop loss orders that would help facilitate a price decline." See SEC, "Concept Release on Equity Market Structure," 75 *Federal Register* 3609, January 21, 2010.

[157] The bid-ask spread of a security is essentially the difference between the price investors are willing to pay for it and the price other investors are willing to sell it for. Theoretically, lowered bid-ask spreads should reduce the costs of trading for all investors. Liquidity describes an investor's ability to promptly purchase or sell a security while having a minimal impact on its price. Price discovery is the process by which the value of a security is established through market supply and demand dynamics.

See Terrence Hendershott, Charles M. Jones, and Albert Menkveld, "Does Algorithmic Trading Improve Liquidity?" *Journal of Finance*, vol. 66, no. 1 (2011); and Charles M. Jones, "What Do We Know About High-Frequency Trading?" *Columbia Business School*, Research Paper No. 13-11, March 20, 2013.

[158] Albert J. Menkveld, "The Economics of High-Frequency Trading: Taking Stock," *Annual Review of Financial Economics*, vol. 8, no. 1 (2016), pp. 2-3, 5-6.

[159] SEC, *Equity Market Structure Literature Review Part II: High-frequency Trading*, March, 18, 2014, pp. 8-11, 22-28.

[160] For more information, see CRS Report R44443, *High Frequency Trading: Overview of Recent Developments*, by Rena S. Miller and Gary Shorter.

[161] Subsequently, a joint SEC-CFTC analysis determined that human error was the direct cause, but that HFT may have exacerbated it. See CFTC and SEC, *Findings Regarding The Market Events of May 6, 2010*, Report of the Staffers of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues, September 30, 2010, pp. 1-8, at https://www.sec.gov/news/studies/2010/marketevents-report.pdf.

traders played during that event. First approved by the SEC in 2012,[162] CAT is planned as a single data repository that will consolidate trade orders, trade quotes (the most recent prices at which a trade on a particular stock was executed), and general trade data across domestic equities and options markets. According to then-SEC Chair Mary Jo White, by virtue of CAT "[R]egulators will have more timely access to a comprehensive set of trading data, enabling us to more efficiently and effectively conduct research, reconstruct market events, monitor market behavior, and identify and investigate misconduct."[163] The system, which has raised some cybersecurity concerns,[164] has also earned prospective praise as a tool that will make HFT more transparent, broadening what the SEC will be able to see as it surveils such trades.[165] CAT phase-in began in late 2019, and it is projected to be fully operational in 2022.

Policymakers have taken a number of other actions in recent years to address concerns related to HFT. Whether these strike the appropriate balance between fostering HFT's potential benefits while appropriately mitigating risks associated with it is an open question. For example, the SEC and CFTC have either approved or not opposed requests by several securities exchanges (including the NYSE American, the IEX, and the gold and silver futures markets at ICE Futures U.S.) to adopt trading delay mechanisms aimed at removing HFT traders' speed advantages.[166]

For more information on these issues, see CRS Report R44443, *High Frequency Trading: Overview of Recent Developments*, by Rena S. Miller and Gary Shorter; and CRS Report R43608, *High-Frequency Trading: Background, Concerns, and Regulatory Developments*, by Gary Shorter and Rena S. Miller.

Asset Management[167]

Asset management companies pool money from various individual or institutional investor clients and invest the funds on their behalf for financial returns.[168] The SEC is the asset management industry's primary regulator. The asset management industry is increasingly using fintech to conduct investment research, perform trading, and enhance its client services. A prominent example is the proliferation of *robo-advisor* services, in which automated programs give

[162] SEC, "SEC Approves New Rule Requiring Consolidated Audit Trail to Monitor and Analyze Trading Activity," press release, July 11, 2012, at https://www.sec.gov/news/press-release/2012-2012-134htm.

[163] SEC, "SEC Approves New Rule Requiring Consolidated Audit Trail to Monitor and Analyze Trading Activity."

[164] In March 2019, the SEC removed one such critical concern when it said that some personal information from individual investors will be excluded from CAT, which reportedly was a concession to broker-dealers and other traders with concerns that such data would be targeted by hackers. Gabriel T. Rubin, "SEC Addresses Cybersecurity Concerns About Stock-Investor Data," *Wall Street Journal*, March 26, 2019, at https://www.wsj.com/articles/sec-addresses-cybersecurity-concerns-about-stock-investor-data-11553625211. In addition, in the fall of 2019, various stock exchanges and the Financial Industry Regulatory Authority, which is building made CAT, made a request to SEC officials that some personal data such as social security numbers and dates of birth be excluded from CAT. SEC Chair Jay Clayton has said that he was receptive to the idea. Andrew Ramonas, "SEC on Course to Fix 'Worst Executed' Audit Trail, Clayton Says," Bloomberg Law, November 19, 2019, at https://news.bloomberglaw.com/privacy-and-data-security/sec-on-course-to-fix-worst-executed-audit-trail-clayton-says.

[165] Ivy Schmerken, "CAT is out of the Bag," *Finextra*, December 3, 2018, at https://www.finextra.com/blogposting/16372/cat-is-out-of-the-bag.

[166] For example, see Nick Baker, "'Flash Boys'-Style Speed Bump Planned for Futures Markets," Bloomberg, February 13, 2019, at https://www.bloomberg.com/news/articles/2019-02-13/a-flash-boys-style-speed-bump-planned-for-u-s-futures-markets.

[167] For questions regarding investment management, congressional clients may contact Eva Su.

[168] For more on asset management, see CRS Report R45957, *Capital Markets: Asset Management and Related Policy Issues*, by Eva Su.

investment advice to clients. There is also potential to apply artificial intelligence and machine learning within asset management, both in robo-advisory services and other functions such as risk management, regulatory compliance, and trading and portfolio management.[169] Another notable development in the industry is that some large, prominent technology companies have begun to offer asset management services and partner with incumbent asset managers.

The term robo adviser generally refers to an automated digital investment advisory program offering asset management services to clients through online algorithmic-based platforms, such as websites or mobile applications.[170] The main differences between human and robo advisers are the amount of human interaction available to investors and the reliance on algorithmic-based platforms for providing financial advice.[171] The potential benefit of this technology is that robo advisers may be able to serve more customers at lower costs than human advisors, thus potentially enabling more affordable consumer access to investment advisory services.[172] Robo advising is a fast-growing segment of the investment management industry. According to one report, direct-to-consumer robo-advisory platforms reached $257 billion in size at the end of 2018 and are projected to have $1.26 trillion in assets under management by 2023.[173]

As mentioned above, big tech firms like Amazon, Facebook, Google, and Apple have started financial services operations as potential competitors and partners to the asset management industry. These types of companies could provide investment management through their widely used platforms, potentially disrupting the asset management industry.[174] The potential of big tech asset management platforms has already been realized in certain overseas markets. For example, Ant Financial, an affiliate of Alibaba Group, now manages the world's largest money market mutual fund of $168 billion as of year-end 2018, with a third of the Chinese population, or 588 million Alipay users, already invested in the fund.[175]

Possible Issues for Congress

In general, robo advisers present similar policy issues as all asset managers do related to striking the right balance between protecting investors and mitigating risks while allowing for innovation, appropriately informed risk taking, and financial returns. However, robo advising could also

[169] See Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, November 1, 2017, at http://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service; and John Schindler, Associate Director, Federal Reserve Board, presentation slides: *Artificial Intelligence and Machine Learning in Finance*, September 29, 2017, at https://philadelphiafed.org/-/media/bank-resources/supervision-and-regulation/events/2017/fintech/resources/24_slides_schindler.pdf?la=en.

[170] SEC, *Investment Management Guidance Update: Robo-Advisers*, February 2017, at https://www.sec.gov/investment/im-guidance-2017-02.pdf.

[171] SEC, "Investor Bulletin: Robo-Advisers," February 23, 2017, at https://www.sec.gov/oiea/investor-alerts-bulletins/ib_robo-advisers.html.

[172] Facundo Abraham, Sergio L. Schmukler, and Jose Tessada, *Robo-Advisors: Investment Through Machines*, World Bank Group, February 2019, at http://documents.worldbank.org/curated/en/275041551196836758/pdf/Robo-Advisors-Investing-through-Machines.pdf.

[173] Aite Group, *U.S. Digital Investment Management Market Monitor, Q2 2019*, May 22, 2019, at https://www.aitegroup.com/report/us-digital-investment-management-market-monitor-q2-2019.

[174] Bailey Lipschultz, "Could Amazon Manage Your Money? Bernstein Analysts Think So," Bloomberg, July 24, 2018, at https://www.bloomberg.com/news/articles/2018-07-24/could-amazon-manage-your-money-bernstein-analysts-think-so.

[175] Stella Xie, "More than a Third of China is Now Invested in One Giant Mutual Fund," *Wall Street Journal*, March 27, 2019, at https://www.wsj.com/articles/more-than-a-third-of-china-is-now-invested-in-one-giant-mutual-fund-11553682785.

present additional policy considerations. Some observers have expressed concerns that robo advisers may cause risks and excess volatility if they result in *herding*, in which very large numbers of investors are all directed to the same investments at the same time.[176] AI- or machine learning-enabled robo advising could also be subject to policy concerns related to *black box* algorithm-based decisionmaking, wherein it is not entirely clear how computer programs have assessed risks or arrived at decisions, and so are effectively unexplainable and unauditable. Some observers are also concerned about the assignment of responsibilities when large losses in an AI-recommended investment occur. For example, questions surround how to assign blame if an investment loss occurred through an AI-based system—should the designer of the AI system or the investment manager incorporating its use bare the blame and penalty?[177] If asset management continues to become increasingly automated, policymakers may weigh these risks and concerns against possible benefits, such as reduced cost and increased access.

Regulating Fintech: Securities Regulators

The federal securities regulators—SEC and CFTC—are focused on any securities-related activities, including those of fintech companies. Examples would include a fintech company raising capital by issuing equity through an initial coin offering or a firm creating a new technology for derivatives contracts. Given their mandate, the securities regulators have used a range of regulatory tools, largely focused on clarifying whether and how the existing regulatory framework applies to new types of technologies, including writing rules and guidance to clarify how existing rules apply to new types of approaches to securities; issuing enforcement actions against any fintech firms that may violate the securities laws under their jurisdiction; and setting up fintech outreach offices to serve as points of contact for stakeholders.

For a detailed examination of the securities regulators' approaches and initiatives related to fintech, see CRS Report R46333, *Fintech: Overview of Financial Regulators and Recent Policy Approaches*, by Andrew P. Scott.

Insurance[178]

Fintech's application to insurance offers a similar potential transformation in the insurance industry as in other aspects of financial services. Fintech could affect insurance throughout the business, including insurance products, underwriting, claims, and marketing, and across all lines of insurance (life, health, and property and casualty [P&C]). Potential aspects of *insurtech* include peer-to-peer insurance, Big Data, artificial intelligence, blockchain, mobile technology, and insurance on demand.[179] Specific examples could include life or health insurers offering discounts for people wearing devices that track activity and fitness; auto insurers offering discounts for cars that include telematics devices tracking drivers' behavior; and insurers scanning social media as an underwriting tool or to detect fraud. In 2017, the fastest-growing P&C insurer by direct

[176] Mark Carney, Governor of the Bank of England, "The Promise of Fintech: Something New Under the Sun?" Speech at Deutsche Bundesbank G20 Conference, January 25, 2017, p. 11, at https://www.bis.org/review/r170126b.pdf.

[177] In a recent case concerning a $20 million AI-related investment loss, a Stanford University law professor commented, "people tend to assume that algorithms are faster and better decision-makers than human traders. That may often be true, but when it's not, or when they quickly go astray, investors want someone to blame." Thomas Beardsworth and Nishant Kumar, "Who to Sue When a Robot Loses Your Fortune," Bloomberg, May 5, 2019, at https://www.bloomberglaw.com/document/XA51N7GO000000?bna_news_filter=banking-law&jcsearch=BNA%25200000016a8ce4d6bfadfb9cee2ed10000#jcite.

[178] For questions regarding insurance, congressional clients may contact Baird Webel.

[179] For more information generally, see National Association of Insurance Commissioners (NAIC), "INSURTECH," at https://www.naic.org/cipr_topics/topic_insurtech.htm; and World Bank Group, *How Technology Can Make Insurance More Inclusive*, Fintech Note no. 2, at http://documents.worldbank.org/curated/en/583381531209953337/pdf/128157-9-7-2018-11-49-10-FintechNotesTechnologyInsuranceInclusiveFinalLowRes.pdf.

premiums written was an auto insurer, Metromile Insurance, offering per-mile insurance with a telematics tracker. In 2018, the fastest-growing P&C insurer was Root Insurance, also a telematics-based auto insurer, and the second-fastest growing was Lemonade Insurance, a homeowners and renters insurer using technology like chatbots and AI to sell and service policies.[180]

Unlike banks or securities firms, the primary regulators for insurers are the individual states. An insurer is required to obtain a charter or license in every state in which it operates. The states coordinate insurance regulatory policies through the National Association of Insurance Commissioners (NAIC) and have been active in addressing issues raised by technology. In 2017, NAIC created an NAIC Insurance and Technology task force[181] and adopted a model law relating to insurer data security.[182] A U.S. Department of the Treasury report specifically encouraged states to adopt the model law and, as of August 4, 2019, seven states had adopted the model with another state considering adoption.[183] All 50 state insurance regulators have identified a specific point of contact for "InsurTech, Innovation & Technology" in order to introduce the regulatory process for new entrants.[184]

Possible Issues for Congress

The state regulatory system for insurance originated following a Supreme Court decision in 1868, but since a further decision in 1944, its foundation has been statutory, not constitutional.[185] The 1945 McCarran-Ferguson Act generally provides for a state-based system,[186] but Congress can enact laws overriding the states and has done so on a number of occasions. Congress has also conducted oversight on specific aspects of the insurance regulatory system and encouraged the states to act on issues without enacting specific statutes at the federal level. Given the breadth of technology's potential impact on insurance, Congress might question numerous aspects of the states' approach to the new technology, including the impact on consumers and the potential for regulatory arbitrage between the federal regulatory approach for banks and securities firms and the state regulatory approach for insurers.

Risk Management and *Regtech*[187]

Risk-management and compliance functions in financial firms frequently rely on data analysis to assess the risk of bad outcomes, such as wrongdoing or financial losses. For example, in anti-money laundering compliance, financial firms are required to file suspicious activity reports (SARs) when transactions by a customer appear potentially to be tied to illicit crime, fraud,

[180] See Tim Zawacki, "US P&C Industry's Fastest-Growing Insurer Takes Root As Insurtech Flourishes," S&P Global Market Intelligence, May 29, 2019.

[181] See NAIC, "Innovation and Technology (EX) Task Force," at https://www.naic.org/cmte_ex_ittf.htm.

[182] See NAIC, "NAIC Passes Insurance Data Security Model Law," press release, October 24, 2017, at http://live-naic-static.pantheonsite.io/Releases/2017_docs/naic_passes_data_security_model_law.htm.

[183] U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities - Asset Management and Insurance*, October 2017, p. 117, at https://www.treasury.gov/press-center/press-releases/Documents/A-Financial-System-That-Creates-Economic-Opportunities-Asset_Management-Insurance.pdf; and NAIC, *Implementation of Model Act #668 Insurance Data Security Model Law*, May 6, 2019, at https://naic-cms.org/sites/default/files/inline-files/Model%20%23668%20Map.pdf.

[184] NAIC, "InsurTech, Innovation & Technology," at https://www.naic.org/index_innovation_technology.htm.

[185] For background on the insurance industry, see CRS Report R44958, *Insurance Regulation: Legislation in the 115th Congress*, by Baird Webel.

[186] 15 U.S.C. §§1011-1015.

[187] For questions regarding risk management and regtech, congressional clients may contact Rena Miller.

money laundering, terrorist financing, or other transgressions. In addition, banks may also be subject to requirements involving stress testing, modeling risks, forecasting, and monitoring employees and internal risk (e.g., the probability that a risky trade under consideration could imperil a bank's capital or liquidity positions). Regulators also must monitor for certain risks or unfolding events (e.g., securities markets regulators trying to detect illegal trading practices). Companies are increasingly using innovative technology in these risk management and regulatory compliance activities. Sometimes in the latter case, the technology is referred to as *regtech*.

Algorithms are especially well suited to sifting through, analyzing, and identifying patterns in large data sets, and so potentially could be used in these risk assessment and compliance functions. Algorithms' increased sophistication and the development of machine learning and artificial intelligence have fueled strong interest in the financial industry in further using these technologies to automate risk-management and compliance functions. For example, FINRA predicts that such tools will help with anti-money laundering processes; surveilling internal firm employees involved in placing trades on a firm's behalf; broker-dealer trade execution for customers; ensuring customer data privacy and preventing security risks; and centralizing supervisory control systems for additional risk management.[188]

In large part, the goal of cost savings is driving the development and adoption of automation in compliance. Some financial firms argue that because they are relatively more regulated than firms in other industries, they must deploy automation wherever possible to reduce compliance costs and remain profitable and competitive.[189] Certain industry observers predict that the cost of processes that involve prediction will drop in coming years and the accuracy of automated prediction processes will continue to increase.[190]

However, exactly how these technologies will develop and be deployed in regulatory compliance, and what outcomes they will produce if deployed, remains to be seen.

Possible Issues for Congress

The possibility that automation's ability to identify risks and suspect behaviors may surpass that of humans in certain cases raises questions over the role and power existing human compliance officials should have in deciding whether to take actions against individuals or institutions. While automation could more efficiently collect and act on information, individuals may be uncomfortable that their transactions and private information could be instantly reported to the government or their financial situation affected through a process that involved no human judgement or oversight. For example, should a human have to file a SAR about a customer to the Treasury Department, or should the filing of such reports be completely automated? To take this

[188] FINRA, *Technology Based Innovations for Regulatory Compliance ("Regtech") in the Securities Industry*, September 2018, at http://www.finra.org/sites/default/files/2018_RegTech_Report.pdf.

[189] For example, see Douglas W. Arner, Janos Barberis, and Ross P. Buckley, "Fintech, Regtech and the Reconceptualization of Financial Regulation," *Northwestern Journal of International Law and Business*, vol. 37, no. 3 (Summer 2017), pp. 371-376; see also Institute of International Finance, *Regtech in Financial Services: Technology Solutions for Compliance and Reporting 5-8*, March 2016; Bart van Liebergen et al., *Regtech in Financial Services: Technology Solutions for Compliance and Reporting*, Institute of International Finance, Report responding to the UK Financial Conduct Authority's "Call for input: supporting the development and adoption of regtech," Washington, DC, March 2016, at https://www.iif.com/Portals/0/Files/private/iif-regtech_in_financial_services_-_solutions_for_compliance_and_reporting.pdf?ver=2019-01-04-142943-690.

[190] Ajay Agrawal, "The Economics of Artificial Intelligence," *McKinsey Quarterly*, April 2018, at https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-economics-of-artificial-intelligence.

example a step further, should the decision to close a customer's account be fully automated as well?

Regtech tools also raise similar privacy and cybersecurity risks as the other technologies discussed in this report. After all, certain regtech programs involve the automated monitoring of individuals' and private companies' financial transactions, flagging some of those transactions as suspicious, and reporting those transactions to government agencies. Policymakers may consider under what circumstances certain regtech processes inappropriately impinge on people's privacy.

To the extent that certain processes or functions can be automated to achieve greater regulatory efficiency or effectiveness, questions exist concerning whether regulators need to be more active in deploying compliance technologies themselves and allowing the institutions they regulate to do so. For example, the American Bankers Association lists "regulator buy-in" as one of the challenges to such adoption.[191]

Potential Regulatory Approaches[192]

Given that most of the federal financial regulatory framework was created prior to the development and deployment of many recent technologies, fintech companies often face uncertainty over how—or whether—existing federal laws and regulations may apply to them or their products. Thus, policymakers may consider ways to reduce regulatory uncertainty and integrate fintech into the regulatory framework. This often involves balancing efforts to encourage innovation while protecting consumers and the financial system from excessive risk. Many still-evolving terms are used to describe different programs regulators have implemented or proposed to address fintech uncertainty. Such programs are often informally called *sandboxes* or *greenhouses*. Generally, such programs use at least one of a variety of approaches.

One such approach involves fostering communication between fintech firms and regulators. Communication can help these firms better understand how regulators view a developing technology and potential regulatory concerns. Communication also helps make regulators aware of new fintech innovations when developing new or interpreting existing regulations. As discussed below, certain regulators have established offices within their organizations to conduct outreach to fintechs—including maintaining outreach websites, participating in fintech conferences, and organizing office hours with fintech firms. In another approach, some regulators have announced research collaborations with fintech firms to improve their understanding of new products and technologies. Such initiatives could include jointly designing a research trial or fintech firms sharing data about their product performance with regulators.

Another potential approach policymakers may use if they determine that particular regulations are unnecessarily burdensome or otherwise ill-suited to a particular technology is to exempt companies or products that meet certain criteria from such regulations. Similarly, a regulator could issue a *no-action letter*—an official communication stating a regulator does not expect to take enforcement actions in certain situations. Regulators will often only provide such special regulatory treatment to companies that first demonstrate that consumers will not be exposed to undue harm or meet other conditions, like agreeing to share data with regulators for research purposes. Regulatory uncertainty can be resolved if regulators offer or require certain fintech

[191] American Bankers Association, *Understanding Regtech*, Fintech Playbook whitepaper, July 25, 2018, pp. 5-6, at https://www.aba.com/news-research/references-guides/understanding-regtech.

[192] For questions regarding regulatory approaches, congressional clients may contact David Perkins, Cheryl Cooper, Andrew Scott, or Eva Su.

firms to enter a regulatory regime with well-defined permissions, restrictions, and responsibilities. For example, a regulator could offer or require a specific charter or license for certain firms.

Financial regulators have begun to implement some of these approaches through a number of rulemakings and by establishing programs and offices and taskforces within agencies. For a detailed examination of these initiatives, see CRS Report R46333, *Fintech: Overview of Financial Regulators and Recent Policy Approaches*, by Andrew P. Scott.

Possible Issues for Congress

The regulatory approaches described above could be supported or opposed by various stakeholders depending on how they are designed and implemented and which firms or products are affected. For example, while fintech firms may want to reduce regulatory uncertainty and operate under one set of rules nationally (rather than different rules in each state), they may also oppose new or additional data-reporting requirements. Incumbent financial institutions may argue that regulatory tailoring and exemptions for fintech firms would put incumbents at a competitive disadvantage. State regulators and consumer advocates may oppose any federal charter that would preempt state consumer-protection laws.

Congress or financial regulators may consider various regulatory approaches. Policymakers choosing to tailor regulation for fintechs could apply a different regulatory treatment either to companies or to products. If the goal is to provide new, inexperienced firms an opportunity to learn how they and their products would be regulated, institution-based regulation for firms meeting criteria associated with start-up companies may be the better option. But if the goal is to integrate a new technology regardless of the size or sophistication of the firm offering it, the differentiated regulatory treatment could apply to the product rather than the firm. Policymakers could also choose to tailor regulation for fintechs meeting certain objective criteria. Alternatively, regulators could use discretion in determining which fintech companies or products would qualify for such tailoring, potentially based on authorities or directions enacted in legislation. Policymakers may also consider how long to apply a particular regulatory treatment to a fintech company or product. For example, a specific charter could last indefinitely, while an exemption or no-action letter might last for only a finite period.

For more information on these issues, see CRS Report R46333, *Fintech: Overview of Financial Regulators and Recent Policy Approaches*, by Andrew P. Scott; and CRS In Focus IF11195, *Financial Innovation: Reducing Fintech Regulatory Uncertainty*, by David W. Perkins, Cheryl R. Cooper, and Eva Su.

Appendix. CRS Fintech Products

Cybersecurity

CRS Report R44429, *Financial Services and Cybersecurity: The Federal Role*, by N. Eric Weiss and M. Maureen Murphy.

CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh.

CRS In Focus IF10559, *Cybersecurity: An Introduction*, by Chris Jaikaran.

Lending

CRS Report R44614, *Marketplace Lending: Fintech in Consumer and Small-Business Lending*, by David W. Perkins.

CRS Report R45726, *Federal Preemption in the Dual Banking System: An Overview and Issues for the 116th Congress*, by Jay B. Sykes.

Payments

CRS Report R45927, *U.S. Payment System Policy Issues: Faster Payments and Innovation*, by Cheryl R. Cooper, Marc Labonte, and David W. Perkins.

CRS Report R45716, *The Potential Decline of Cash Usage and Related Implications*, by David W. Perkins.

Banks and Third-Party Vendor Relationships

CRS In Focus IF10935, *Technology Service Providers for Banks*, by Darryl E. Getter.

Cryptocurrency and Blockchain-Based Payment Systems

CRS Report R45427, *Cryptocurrency: The Economics of Money and Selected Policy Issues*, by David W. Perkins.

CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran.

CRS Report R45664, *Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals*, by Jay B. Sykes and Nicole Vanatko.

CRS In Focus IF10824, *Financial Innovation: "Cryptocurrencies"*, by David W. Perkins, Financial Innovation: "Cryptocurrencies", by David W. Perkins.

Digital Assets and Capital Formation

CRS Report R46208, *Digital Assets and SEC Regulation*, by Eva Su.

CRS Report R45221, *Capital Markets, Securities Offerings, and Related Policy Issues*, by Eva Su.

CRS Report R45301, *Securities Regulation and Initial Coin Offerings: A Legal Primer*, by Jay B. Sykes.

CRS In Focus IF11004, *Financial Innovation: Digital Assets and Initial Coin Offerings*, by Eva Su.

High-Frequency Securities and Derivatives Trading

CRS Report R44443, *High Frequency Trading: Overview of Recent Developments*, by Rena S. Miller and Gary Shorter.

CRS Report R43608, *High-Frequency Trading: Background, Concerns, and Regulatory Developments*, by Gary Shorter and Rena S. Miller.

Regulatory Approaches and Issues for Congress

CRS Report R46333, *Fintech: Overview of Financial Regulators and Recent Policy Approaches*, by Andrew P. Scott.

CRS In Focus IF11195, *Financial Innovation: Reducing Fintech Regulatory Uncertainty*, by David W. Perkins, Cheryl R. Cooper, and Eva Su.

Author Information

David W. Perkins, Coordinator
Specialist in Macroeconomic Policy

Cheryl R. Cooper
Analyst in Financial Economics

Darryl E. Getter
Specialist in Financial Economics

Chris Jaikaran
Analyst in Cybersecurity Policy

Marc Labonte
Specialist in Macroeconomic Policy

Rena S. Miller
Specialist in Financial Economics

Andrew P. Scott
Analyst in Financial Economics

Gary Shorter
Specialist in Financial Economics

Eva Su
Analyst in Financial Economics

Baird Webel
Acting Section Research Manager

Acknowledgments

The authors would like to thank retired CRS specialist N. Eric Weiss for his helpful contributions to this report.

Disclaimer