Catholic University Journal of Law and Technology

Volume 29
Issue 2 *Spring 2021*

Article 8

2021

To Innovate or Regulate: How to Regulate Cloud Service Providers Within Financial Institutions

Morgan Willard
Catholic University of America (Student)

TO INNOVATE OR REGULATE: HOW TO REGULATE CLOUD SERVICE PROVIDERS WITHIN FINANCIAL INSTITUTIONS

Morgan Willard[*]

If a person had to use one word to describe the past hundred years, even the last fifty years, one word trumps all others: technology. From watches that track our every movement to robots in factories, technology is impacting both individuals and industries. Financial services is one of the industries that has been revolutionized by technological advances. Computers entered the world of banking in the 1950s, and by the 1960s began to soar.[1] Between 1963 and 1968, the use of on-premises or off-premises computers "rose from less than one-in-ten to almost half" and quickly became paramount to day-to-day business.[2] In the 1990s, more workers used computers in the financial industry than any other, which increased "the number and quality of remote services that banks could offer customers[.]"[3] From credit cards to online banking,

[*] Morgan Willard is a graduate from the Catholic University of America, Columbus School of Law. She is originally from Fairfax, Virginia and graduated from the University of St. Andrews with a degree in International Relations. Her heartfelt thanks go out to both her parents for their support and for always agreeing to read another draft and to J.C. Boggs without whom she would not have known about this topic. Her final thanks go to all the friends and colleagues who reviewed and worked on this article to make it the final product it is today.

1 *See Bank of America Revolutionizes Banking Industry*, BANK OF AM., https://about.bankofamerica.com/en-us/our-story/bank-of-america-revolutionizes-industry.html#fbid=XEcoEWAMMZ7 (last visited Mar. 19, 2021) (explaining how the first computer helped Bank of America in the banking industry by introducing Electronic Recording Method of Accounting, which could process upwards of 12,000 letters or numbers per second).

2 HAL S. SCOTT ET AL., PROGRAM ON INT'L FIN. SYS., CLOUD COMPUTING IN THE FIN. SECTOR: A GLOBAL PERSPECTIVE 3 (July 2019), https://www.pifsinternational.org/wp-content/uploads/2019/07/Cloud-Computing-in-the-Financial-Sector_Global-Perspective-Final_July-2019.pdf.

3 *Id*.

technology has improved customer access to financial services and increased efficiency in the process overall.[4] Technology has been considered to be an asset to the financial industry as it provides superior service to as many customers as possible. Consumer advocates have appreciated the expansion of banking products to underserved groups through increased information on potential customers.[5] Yet, as with most good things, there is more to the story than just positive innovation.

As financial institutions continue to rely more on technology, new risks threaten our financial markets and its financial stability.[6] Financial institutions are implementing new technology to keep up with the ongoing changes throughout the world. To stay competitive, they have begun looking for ways to increase speed and ease as new financial entities begin to emerge.[7] At the forefront of efficiency technology is cloud computing.[8] Cloud computing is a computing resource that is accessed via the internet and provides storage, networking, data management, and other services.[9] Cloud computing benefits not only basic secondary functions, but it may be utilized for its core functions within financial services.[10]

Various agencies that regulate the financial industry, however, still have

---

4 *See* James McArthur, *How Technology Has Changed Banking Industry Today?*, ENGADGET (Oct. 19, 2016), https://www.engadget.com/2016-10-19-how-technology-has-changed-banking-industry-today.html (showing how banking has changed in six different ways due to technology).

5 *See generally* Lucy Gorham & Jess Dorrance, *Catalyzing Inclusion: Financial Technology & The Underserved*, CTR. FOR CMTY. CAP., UNIV. N.C. (Aug. 2017), https://communitycapital.unc.edu/files/2017/10/CCC-FinTech-Report-2017-1.pdf.

6 Memorandum from the U.S. House of Representatives' Majority Staff of the Fin. Servs. Comm. to the Members of the Comm. on Fin. Servs. 2 (Oct. 15, 2019), https://docs.house.gov/meetings/BA/BA00/20191018/110094/HHRG-116-BA00-20191018-SD002-U1.pdf [hereinafter "Memorandum to Comm. on Fin. Servs."] (detailing how the financial services was slower to adopt cloud computing and why); *see also* Edward Appert, *Information Technology Risks in Financial Service*, DELOITTE, https://www2.deloitte.com/us/en/pages/center-for-board-effectiveness/articles/information-technology-risks-financial-services.html (last visited Mar. 19, 2021) (highlighting some of the largest technological risks in the financial services).

7 Darryn Pollock, *The Future of Banking: Is It All Bitcoin and Blockchain?*, FORBES (July 25, 2019), https://www.forbes.com/sites/darrynpollock/2019/07/25/the-future-of-banking-is-it-all-bitcoin-and-blockchain/#475077231eb9 (outlining the changing market forces, which traditional banks will need to compete with near and long term).

8 BRAD CARR ET AL., INST. OF INT'L FIN., CLOUD COMPUTING IN THE FINANCIAL SECTOR PART 1: AN ESSENTIAL ENABLER (Aug. 2018), https://www.iif.com/portals/0/Files/private/32370132_cloud_computing_in_the_financial_sector_20180803_0.pdf.

9 *Cloud Computing Basics*, UNIV. OF WASH. INFO. TECH., https://itconnect.uw.edu/research/cloud-computing-for-research/cloud-computing-basics/ (last visited Apr. 17, 2021).

10 CARR ET AL., *supra* note 8, at 1–3 (noting that cloud computing technology could "help firms expedite processes, reduce risks, and increase efficiency, as well as enhancing the ability to identify business opportunities and revenue streams").

concerns about cloud computing technology despite its ability to improve consumer experience.[11] Financial technology is quickly evolving, with minimal regulations to constraining it.[12] Unlike past technological revolutions, society is more conscientious of changes within the financial industry.[13] With its major institutions, such as Bank of America and Merrill Lynch, being deemed "too big to fail," incorporating new technology within this industry with little regulation is troubling.[14] Banks' potential failures to successfully integrate technology puts the economy of the entire country at risk and could have a destructive impact on the acceptance of financial technology in the future. As a nation, we are risk averse to structural harm to our financial system, and financial technology ("FinTech") has the potential to expose banks to such systemic risks.[15]

This paper will focus on one aspect of financial technology: cloud service providers. It will explore the best way to manage this emerging technology as it relates to financial services and bank-related functions. To achieve this goal, it is imperative to define and understand: who cloud service provides are, what cloud computing is, and the potential regulations to be applied when used by financial institutions. Lastly, this comment will discuss the Financial Services Committee's recent call to regulate cloud service providers as a systemically important financial market utility ("SIFMU"), potential alternative regulatory measures, and how they will either act as a benefit or detriment to the innovation of the technology.[16]

---

11 Alan W. Avery et al., *The Systemic Importance of Cloud-Based Service Providers to Banks*, LATHAM & WATKINS L.L.P. (Sept. 5, 2019), https://www.fintechandpayments.com/2019/09/the-systemic-importance-of-cloud-based-service-providers-to-banks/.

12 CARR ET AL., *supra* note 8, at 3 ("The biggest challenge for migrating financial institutions' data and applications to public cloud in a highly regulated environment is demonstrating to regulators that FIs are sufficiently competent to partner with CSPs. . .").

13 Jesse McWaters, *5 Ways Technology is Transforming Finance*, WORLD ECON. FORUM (June 30, 2015), https://www.weforum.org/agenda/2015/06/5-ways-technology-transforming-finance/ (discussing technology's impact on the financial industry).

14 Memorandum to Comm. on Fin. Servs., *supra* note 6, at 5; *see also Too Big to Fail? Merging Bank of America and Merrill Lynch's Cultures Risky, Analysts Say*, WINSTON-SALEM J. (Sept. 16, 2008), https://journalnow.com/business/too-big-to-fail-merging-bank-of-america-and-merrill/article_091d04bb-b2a1-5b12-b988-9fa46515bb60.html (explaining how the two financial powerhouses merging could make "the nation's largest financial-services company – one that some believe is too big to fail.").

15 Memorandum to Comm. on Fin. Servs., *supra* note 6, at 5 ("As financial institutions migrate to cloud computing . . . . the operational risks increase, especially without the in-depth regulator examination or guidelines. Operational risk refers to internal controls, people, systems, and external events, including cyber risks [e.g., data breaches, insufficient customer data backups, and operating system hijacking.]").

16 *Id.* at 3–5.

I. BACKGROUND

A. What is the Cloud?

The "cloud" is broadly defined by the National Institute of Standards and Technology as "a system for enabling efficient and on-demand access, regardless of location, to shared configurable resources that can be rapidly delivered to consumers with little management or oversight by a cloud provider."[17] Cloud computing is "the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale."[18] There are four major types of cloud deployments: public clouds, private clouds, community clouds, and hybrid clouds.[19] Public clouds are defined as "a digital environment where the computing resources are available in a shared environment and accessed by multiple customers of the [cloud service providers]."[20] Conversely, "private clouds provide computing resources dedicated to a single entity," which can be more costly than a public cloud.[21] Community clouds "are available for use by a specific community of users that have shared needs or concerns," such as security and compliance.[22] Lastly, "[h]ybrid [c]louds arrange a mix of deployments that enables quick data movability among different deployments."[23] Based on the financial institution's cloud choice, the "nature and degree of control and risk" faced will vary.[24]

Within each of these deployments are three main service implementations:

---

17 *Id*. at 1.

18 *What is Cloud Computing?*, MICROSOFT AZURE, https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/ (last visited Apr. 18, 2021).

19 Memorandum to Comm. on Fin. Servs., *supra* note 6, at 2.

20 *Id*.; *see also What Is Public Cloud? 4 Basic Features of Public Cloud*, CLOUDWAYS (Nov. 28, 2011), https://www.cloudways.com/blog/what-is-public (giving examples of a public cloud such as: "Amazon Elastic Cloud Compute, Google App Engine, Blue Cloud by IBM and Azure services Platform by Windows.").

21 Memorandum to Comm. on Fin. Servs., *supra* note 6, at 2; *see also Types of Cloud Computing: Private, Public, and Hybrid Clouds*, U. OF ILL. TECH. SERVS., https://cloud.illinois.edu/types-of-cloud-computing-private-public-and-hybrid-clouds/ (last visited Apr. 18, 2021).

22 Memorandum to Comm. on Fin. Servs., *supra* note 6, at 2; *see also* Dejan Tucakov, *What is Community Cloud? Benefits & Examples with Use Cases*, PHOENIXNAP (Jun. 18, 2020), https://phoenixnap.com/blog/community-cloud.https://phoenixnap.com/blog/community-cloud.

23 Memorandum to Comm. on Fin. Servs., *supra* note 6, at 2; *see also Types of Cloud Computing: Private, Public, and Hybrid Clouds*, *supra* note 21.

24 SCOTT ET AL., *supra* note 2, at 4.

software as a service, platform as a service, and infrastructure as a service.[25] Software as a service ("SaaS") "provides one or more software applications designed for specific purposes, typically vendor-managed and customizable by users."[26] Platform as a service ("PaaS"), also known as middleware, "is an application platform software (commonly referred to as middleware because it sits between the CSP and the customer) that provides customers flexibility to build and deploy custom applications using tools supported by [cloud service providers]."[27] It is considered to be more flexible than SaaS but more structured than infrastructure as a service ("IaaS") by enabling "the development and use of software by the customer on app[lication] hosting and development infrastructure offered by a cloud service provider."[28] Lastly, IaaS implementation, which is "known as the complete package for competing functionality, includes hardware, software, servers, and networking competing."[29]

B. Who are the Providers and What Benefits Do They Offer?

Three of the largest IaaS providers are Azure, Google Cloud, and Amazon Web Services ("AWS").[30] When utilizing this form of a cloud service, the customer "does not manage or control the underlying cloud but has control over the operating systems."[31] This allows the customer to control "everything from the operating systems to the applications that run on that infrastructure."[32]

From start-ups to major financial institutions, firms are beginning to transition to the cloud due to their "expedite[d] processes, reduce[d] risks, and increase[d] efficiency[.]"[33] Banking operations have become exceedingly complex and "proprietary data centers have become more expensive."[34] Cloud service providers allow their customers to utilize their services on an as-needed basis by permitting them to "automatically scale up when additional resources

---

25 Memorandum to Comm. on Fin. Servs., *supra* note 6, at 2–3.

26 *Id* at 2; *see also* Tony Hou, *IaaS vs PaaS vs SaaS Enter the Ecommerce Vernacular: What You Need to Know, Examples & More*, BIGCOMMERCE, https://www.bigcommerce.com/blog/saas-vs-paas-vs-iaas/#executive-summary-summing-up-saas-vs-paas-vs-iaas (last visited Apr. 18, 2021).

27 Memorandum to Comm. on Fin. Servs., *supra* note 6, at 2–3; *see also* Hou, *supra* note 26.

28 SCOTT ET AL., *supra* note 2, at 4.

29 Memorandum to Comm. on Fin. Servs., *supra* note 6, at 2–3; *see also* Hou, *supra* note 26.

30 Memorandum to Comm. on Fin. Servs., *supra* note 6, at 3.

31 *Id*.

32 SCOTT ET AL., *supra* note 2, at 4.

33 CARR ET AL., *supra* note 8, at 1.

34 SCOTT ET AL., *supra* note 2, at 6.

are needed and scale down when demand subsides."[35] This scaling process eliminates the need for "costly over-provisioning," saving the institution money while increasing its efficiency.[36] According to its chief technology officer, Microsoft Azure "continues to see strong Cloud adoption from the financial services industry, with more than 80 percent of the world's largest banks and more than 75 percent of the global systemically important financial institutions using Azure."[37] As of 2018, "[80] percent of large financial institutions [have] adopt[ed] Azure."[38] Currently, "[AWS] have almost 50 percent market share, followed by Azure, Google, IBM or Alibaba."[39] The overwhelming consensus is that clouds can increase efficiency in the industry unlike any other product, which has helped to sharpen the increase of financial institutions employing the technology.[40]

II. THE IMPLEMENTATION AND IMPACT ON FINANCIAL INSTITUTIONS AND FINANCIAL SERVICES

A. Cloud Service Implementation within the Financial Services Industry

While the cloud is being utilized by large financial institutions, it currently provides periphery rather than core functions.[41] The industry is slowly moving toward incorporating cloud services within its core functions, but it will likely continue its slow march to full incorporation because the technology used by financial institutions is complex.[42] At present, "transactional core banking is highly integrated with legacy technologies, and regulation and internal governance are stricter around outsourcing and data privacy," making financial institutions weary to adopt new IT programs.[43]

---

35 *Id*.

36 *Id*.

37 Letter from Congresswoman Nydia M. Velazquez and Congresswoman Katie Porter to The Honorable Steven M. Mnuchin, Sec'y of the U.S. Dep't of the Treasury (Aug. 22, 2019), https://velazquez.house.gov/sites/velazquez.house.gov/files/FSOC%20cloud%20.pdf [hereinafter "Letter to Sec'y Treasury"].

38 Chad Morris, *It's Time for Financial Institutions to Adopt the Cloud – These Technologies Can Help*, BIZTECH (Oct. 19, 2018), https://biztechmagazine.com/article/2018/10/its-time-financial-institutions-adopt-cloud-these-technologies-can-help.

39 CARR ET AL., *supra* note 8, at 6.

40 *Id*. at 1, 3–4.

41 *Id*. at 1; SCOTT ET AL., *supra* note 2, at 1 (explaining and listing the kinds of functions currently utilized by financial institutions: internal data information, human resources capabilities, email management, and app development).

42 CARR ET AL., *supra* note 8, at 2.

43 *Id*.

Yet, financial institutions are hard-pressed to adopt cloud technology because "financial institutions must (and are in the process to) adapt to a new reality, characterized by the customers' expectations of immediacy and personalization."[44] Although cloud services are not currently integrated into the core services of financial institutions, the data that is maintained in the cloud is still critical to the operations of the financial institutions.[45] Therefore, although governmental regulation is appropriate as financial institutions move to implement cloud services within their core functions, the urgency of the call may come too soon or too drastically, given institutions are not fast-tracking implementation.

B. The Potential Impact on the Cloud and Congress' Response

The potential impact that these providers could have on financial institutions, and the market, have sparked a debate as how best to handle the emerging technology. Most recently, on August 22, 2019, Congresswomen Velazquez and Porter of the House Financial Services Committee (the "Congresswomen") wrote a letter to the Secretary of the US Treasury Department to request that the Financial Services Oversight Committee ("FSOC") consider designating the three leading providers of cloud service provider systems as systemically important financial market utilities ("SIFMUs").[46] Financial market utilities are defined by the Federal Reserve as "multilateral systems that provide the infrastructure for transferring, clearing, and settling payments, securities, and other financial transactions among financial institutions or between financial institutions and the system."[47] When determining whether a SIFMU designation is appropriate, the FSOC considers four factors:

> the aggregate monetary value of transactions processed by the financial market utility ("FMU"); the aggregate exposure of the [FMUs] to its counterparties; the relationship interdependencies, or other interactions of the [FMUs] with other [FMUs] or payment, clearing, or settlement activities; and the effect that the failure of or

---

44 *Id.* at 3.

45 SCOTT ET AL., *supra* note 2, at 1.

46 Letter to Sec'y Treasury, *supra* note 37, at 1; *see also* Press Release, The Office of Congresswoman Nydia M. Velazquez, Velázquez, Porter Urge FSOC to Oversee Tech Giants 1 (Aug. 23, 2019), https://velazquez.house.gov/media-center/press-releases/velazquez-porter-urge-fsoc-oversee-tech-giants ("The letter follows last month's data breach at Capital One Financial Corporation, which exposed the personal information of approximately 106 million Capital One credit card customers and applicants.").

47 *Designated Financial Market Utilities*, BD. OF GOVERNORS OF FED. RES. SYS., https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm (last updated Jan. 29, 2015).

> a disruption of the [FMUs] would have on critical markets, financial institutions, or the broader financial system.[48]

Once a financial market utility is determined to be systemically important, the FSOC puts the organization or company on notice, holds hearings, allows for written submissions, and provides for consultations between the company or organization and the Federal Reserve.[49]

Currently, there are eight institutions that have been designated as SIFMUs by the Federal Reserve.[50] All of these have, even if not in their entirety, clearing house functions. A clearing house acts as an "intermediary between a buyer and seller" and seeks to ensure that the process from trade inception to settlement is smooth; its main role is to make certain that "the buyer and seller honor their contractual obligations."[51] Clearing houses are directly involved with the transaction or flow of currency, and their failure would be detrimental to the integrity of our financial markets.[52] Their functions fall squarely within the four determining factors, and this implicitly necessitates the need for heightened regulation.

However, designation as a SIFMU does not turn solely on whether or not the system falls squarely within the four factors. Authority over designation of financial market utilities further provides the FSOC with the authority to "place greater importance on whether the failure or disruption of the [financial market utility] would create or increase the risk of credit and liquidity issues among financial institutions and markets, and whether such credit and liquidity issues would threaten the stability of the US financial system."[53] This allows for a broad conception of what a SIFMU is and arguably opens the door to emerging market disrupters that have not traditionally been used in the financial sector. With this in mind, the members of the Committee on Financial Services have begun to explore the impact that cloud services could have on the US financial system, and if the threat posed is so great that it should be designated as a SIFMU.[54]

---

48 Avery et al., *supra* note 11.

49 *Id.*

50 *Designated Financial Market Utilities*, *supra* note 47 (naming the eight institutions as: Clearing House Payments Company, L.L.C, CLS Bank International, Chicago Mercantile Exchange, Inc., The Depository Trust Company, Fixed Income Clearing Corporation, ICE Clear Credit L.L.C, National Securities Clearing Corporation, and the Options Clearing Corporation).

51 Akhilesh Ganti, *Clearinghouse*, INVESTOPEDIA, https://www.investopedia.com/terms/c/clearinghouse.asp (last updated Apr. 1, 2019).

52 *Id.*

53 Avery et al., *supra* note 11.

54 Memorandum to Comm. on Fin. Servs., *supra* note 6, at 2, 5.

III. WILL THE CLOUD END DATA BREACHES OR CREATE MORE CATASTROPHIC ONES? THE CASES OF *EQUIFAX* AND *CAPITAL ONE*

A. The Tale of Equifax

The internet and technology, as discussed above, have provided endless benefits for large companies to access consumers and their information; however, they have also created new risks for institutions and service providers that store information, as these large firms become enticing targets for cyber criminals.[55] One example of an unlucky institution is Equifax. Equifax is a credit-reporting company that tracks and rates "the financial history of U.S. consumers."[56] In 2017, from May to July, Equifax suffered a data breach that compromised as many as 143 million US customers' information (names, social security numbers, birth dates, addresses, and some driver's licenses). Further, about 209,000 US customers' credit card numbers were exposed; "personal identifying information" of roughly 182,000 US customers involved in credit report disputes was also released.[57] This data breach was particularly unique, because not all customers were aware they were customers; instead, Equifax received its data from credit card companies, banks, retailers, and lenders who report the activity, "as well as by purchasing public records."[58] In the end, the company settled with affected customers for $700 million.[59] This was one of the first big data breaches that demonstrated the potential harm that can be caused by a technological breach of an institution or corporation holding sensitive personal data.

In response to this breach, Equifax is undergoing a technological and security makeover with cloud computing services at its center.[60] It has chosen to partner with the Google Cloud Platform, which will enable Equifax to create a hierarchy of control.[61] It has transitioned to this form of security based on the promise that "[i]f anything happens within any of those projects, each one is

---

55 *See What Makes Businesses a Target for Cybercrime?*, NIC, https://www.nicitpartner.com/makes-businesses-target-cybercrime/ (last visited Apr. 18, 2021) (noting that smaller firms are currently the primary targets of choice for most cyberattacks, but that firms of larger sizes are now being targeted more frequently).

56 Sarah Ashley O'Brien, *Giant Equifax Data Breach: 143 Million People Could be Affected*, CNN BUS. (Sept. 8, 2017), https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html.

57 *Id.*

58 *Id.*

59 Bridget Botelho, *Equifax Shares 'Risk Averse' Cloud Security Model Post-Breach*, TECHTARGET (Oct. 22, 2019), https://searchcloudcomputing.techtarget.com/news/252472694/Equifax-shares-risk-averse-cloud-security-model-post-breach.

60 *Id.*

61 *Id.*

essentially self-contained, so the scope [of a system compromise] is only extensive to that application[.]"[62] By 2020, Equifax hopes to move its legacy mainframe and service technology to the public cloud.[63] The senior officers of the corporation believe that transitioning Equifax's data from traditional systems to a dual-cloud and physical security team program will rebuild the trust broken with consumers and ensure security.[64] Although many regulators and consumers fear the use of the cloud will lead to more breaches, firms trying to guarantee security and information privacy are looking to the cloud as the solution to these problems.

B. The Story of Capital One

As the data breach of Equifax faded into the background, another data breach occurred at Capital One Financial Corporation in July 2019, which sparked a debate surrounding the potential harm that could be caused as other financial institutions implement cloud services.[65] The hack of Capital One's data "affected about 100 million U.S. customers, and 6 million Canadian clients . . . [a]bout 140,000 Social Security numbers and 80,000 linked bank account numbers were obtained through the breach[;] [b]ut Canadians were more heavily impacted, without about one million Social Insurance numbers compromised."[66] The majority of the information compromised included a "wide array of personal data, such as names, addresses, phone numbers, dates of birth, self-reported income, credit scores and fragments of transaction history."[67]

Fees and expenses to correct information system breaches can be significant, it is currently estimated that this breach will cost Capital One between $100 million to $150 million in 2019.[68] The breach occurred when information was

---

62 *Id.*

63 Alex Hickey, *Equifax Undergoing Major Tech Overhaul as Dust Settles from Breach Fallout*, CIODIVE (Feb. 26, 2019), https://www.ciodive.com/news/equifax-undergoing-major-tech-overhaul-as-dust-settles-from-breach-fallout/549154/.

64 *Id.*

65 Letter to Sec'y Treasury, *supra* note 37, at 1; *see also* Memorandum to Comm. on Fin. Servs., *supra* note 6, at 5 (both the letter and the memorandum for the October 18, 2019, meeting discuss the potential harm that could occur if another institution's data is compromised as it was with Capital One).

66 Lucinda Shen, *Capital One's Data Breach Could Cost the Company up to $500 Million*, FORTUNE (July 31, 2019), https://fortune.com/2019/07/31/capital-one-data-breach-2019-paige-thompson-settlement/.

67 Christian Berthelsen et al., *Capital One Says Breach Hit 100 Million Individuals in U.S.*, BLOOMBERG (July 29, 2019), https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says.

68 Shen, *supra* note 66.

illegally accessed by one of Amazon's former cloud-service employees.[69] However, it has been confirmed, and accepted, that the breach was not due to any vulnerability on the part of the Amazon Web Services systems, but rather an additional firewall that was protecting one of its applications.[70] Initially, Capital One was one of the leading advocates for the use of cloud services within banks, with a plan to completely migrate its data centers by the end of 2020.[71] Because of the disastrous breach and the potential for others in the future, it begs the question of whether other firms should reconsider moving to the cloud, or if it is unfair to place such a burden or pressure on the system that was ruled not to have caused the breach. Although the result of this breach had a wide impact, especially on retail consumers and small businesses, it has been instructive in identifying and understanding the pitfalls of cloud services.[72] The regulators and larger financial institutions can learn from this incident how best to mitigate and remediate potential incidents like this so that they do not happen in the future.

IV. DESIGNATION OF CLOUD SERVICE PROVIDERS AS SYSTEMICALLY IMPORTANT FINANCIAL MARKET UTILITIES

A. Where Does FSOC's Authority Derive From?

If cloud service providers fall under the SIFMU, they become subject to Title VIII of the Dodd-Frank Act ("Dodd-Frank Act").[73] On July 21, 2010, the Dodd-Frank Act was implemented "to mitigate systemic risk in the financial system and to promote financial stability, in part, through enhanced supervision of financial market utilities."[74] More commonly, it has been referred to as the body of law that regulates institutions that are "too big to fail."[75] Too-big-to-fail institutions are financial firms "that would crash the

---

69 Emily Flitter & Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, N.Y. TIMES (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.

70 *Id*.

71 Berthelsen et al., *supra* note 67.

72 Andrew Larkin, *Disadvantages of Cloud Computing*, CLOUD ACAD. (Aug. 7, 2019), https://cloudacademy.com/blog/disadvantages-of-cloud-computing/.

73 Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, 12 U.S.C. § 5464(f) (2010).

74 *See Title VIII of the Dodd-Frank Act*, BD. OF GOVERNORS OF FED. RES., https://www.https://www.federalreserve.gov/paymentsystems/title-viii-dfa.htm (last updated Jan. 29, 2015).

75 Dennis Kelleher, *BankThink 'Too Big to Fail' is Alive and Kicking*, AM. BANKER (Aug. 1, 2018), https://www.americanbanker.com/opinion/too-big-to-fail-is-alive-and-kicking.

entire financial system and global economy if they failed."[76] In 2008, in order to avoid another economic meltdown like the Great Depression, the government bailed out financial institutions such as JP Morgan Chase, Citigroup, Bank of America, and Morgan Stanley.[77] In a similar process to the designation of SIFMUs, regulatory bodies execute their oversight authority by designating firms as Systemically Important Financial Institutions ("SIFIs").[78] The policy aim behind designating these institutions is to recognize the influence over the market and the financial sector.[79] The FSOC is tasked with analyzing which institutions and organizations pose such a threat.[80] Once an institution is recognized as such an entity, a specific regulatory body is assigned to oversee it, usually the Federal Reserve or the Treasury.[81] Oversight of these institutions is conducted in order to ensure the stability of the market and its institutions, but also on a more fundamental level, the policy ensures consumer trust in the institution itself.[82] Dodd-Frank arose from a time of uncertainty where consumers and investors did not trust the financial industry.[83] The regulations and designations work to rebuild and foster trust between financial institutions and consumers. As will be discussed next, the Congresswomen of the Financial Oversight Committee believe cloud service providers' products have the potential to disrupt this policy and could lead to distrust, or worse a financial disaster.[84]

V. APPLICATION OF THE SIFMU FACTORS

As mentioned above, a financial market utility is considered a SIFMU when it satisfies the four factors relating to transactions and its relationship to the market, institutions, and the system overall; however, these factors are not met by the services provided by cloud service systems.[85]

As to the first factor, which considers the aggregate monetary value of transactions processed by the FMU in the financial service context of cloud computing and service providers, the systems do not provide services for

---

76 *Id.*
77 *Id.*
78 *Id.*
79 *Id.*
80 *Id.*
81 *About FSOC*, U.S. DEP'T. OF TREASURY, https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/about-fsoc (last visited Apr. 18, 2021); *see also Designated Financial Market Utilities*, *supra* note 47.
82 *Designated Financial Market Utilities*, *supra* note 47.
83 *Id.*
84 Letter to Sec'y Treasury, *supra* note 37, at 1, 4–5.
85 Avery et al., *supra* note 11; Letter to Sec'y Treasury, *supra* note 37, at 2.

processing transactions.[86] Even in the Congresswomen's memorandum, they note that "cloud service providers do not directly process monetary transactions," yet they maintain that, "their operational stability still underpins a large portion of banks' central functions."[87] They further argue that due to the fact that "[b]anks and other financial institutions use cloud-based service providers to connect to one another and to other market participants, [this] enables monetary and commercial transactions while also maintaining sensitive information regarding their clients."[88] The Congresswomen's argument tries to stretch the functions of the cloud services to fit within this first factor, but it is grounded in their view of the future.[89] They fear that while "cloud service providers may not process monetary transactions like SIFMUs, these firms provide the world's biggest banks with the technological foundation necessary to link to one another and other financial and commercial market participants, thereby helping to enable monetary and commercial transactions while simultaneously maintaining their clientele's most sensitive information and associated assets."[90] The Congresswomen fully recognize that the categorization is tenuous, but they provide a preemptive warning to the Secretary of the Treasury that within the next several years, institutions will begin to transition their platforms to the technology.[91] However, general congressional oversight does not always inform regulation but can serve to deter innovation.

The current participation of cloud service systems in the transaction process cannot be generalized to equate to a system where the aggregate monetary value of transactions is processed.[92] It is too far of a stretch. Although it is concerning that financial institutions are storing large volumes of data on the cloud and relying on their servers for data storage, this does not cause them to fall within this first factor.[93] For example, The Clearing House Payments Company ("CHIPS") was designated as an SIFMU on May 22, 2012.[94] It qualified under the first factor based on "the degree to which the U.S. banking system relies on CHIPS to facilitate significant financial flows, particularly those involving transfers between U.S. money center banks and foreign banks

---

86 Avery et al., *supra* note 11.
87 *Id.*; *see also* Letter to Sec'y Treasury, *supra* note 37, at 2.
88 Avery et al., *supra* note 11; *see also* Letter to Sec'y Treasury, *supra* note 37, at 3.
89 Letter to Sec'y Treasury, *supra* note 37, at 2.
90 *Id.* at 3.
91 *Id.* at 3–5.
92 Avery et al., *supra* note 11.
93 *Id.*; *see also* Letter to Sec'y Treasury, *supra* note 37, at 2–3.
94 U.S. DEP'T OF TREASURY, FIN. STABILITY OVERSIGHT ANN. REP. 145 (2012) https://www.treasury.gov/initiatives/fsoc/Documents/2012%20Appendix%20A%20Designation%20of%20Systemically%20Important%20Market%20Utilities.pdf.

operating in the United States."[95] The transfers are not only high profile, but every two weeks, "the value of payments settling through CHIPS . . . [is the] equivalent to the gross domestic product of the United States."[96]

Likewise, another SIFMU designee, CLS Bank International, was found to fulfill the first factor based on its settlement volumes and values, which had "an average aggregate daily value of $4.77 trillion in 2011."[97] Both firms deal with a significant volume of U.S. transactions on a daily basis.[98] The failure of one of these firms would not only pose a risk to market stability, but such a failure could also foster distrust between consumers, the market, and its institutions, which are the kind of firms SIFMU designations are meant to regulate.[99] Cloud services are not intended to provide the valuable functions CHIPS and CLS Bank provide. This does not mean they never will, but until financial institutions move in that direction, it is hard to align the functions of cloud services with the vital functions of other SIFMUs. Therefore, cloud service providers do not meet the requirements for the first factor.

As to the second factor, the aggregate exposure to counterparties, the Congresswomen recognize the lack of financial exposure in the event of a cloud failure but argue that "the operational losses stemming from such a cloud failure could be significant."[100] Their phrasing of these concerns appears dire, but their argument fails to provide the factual support to meet the requirements for the second factor. This is due to the fact that such exposure is unlikely to occur.[101] One of the core reasons for institutions to switch to the cloud is the system's redundancy measures.[102] The redundancy capabilities used by the cloud are the most cost effective and get businesses back up and running faster than current legacy systems.[103] As a result, the cloud has been championed as a more secure alternative to other similar programs.[104] Moreover, as many have argued, with multiple layers and firewalls, the most problematic scenario is significantly less likely to occur.[105]

---

95 *Id*. at 147.
96 *Id*. at 152.
97 *Id*.
98 *Id*.
99 *Designated Financial Market Utilities*, *supra* note 47.
100 Avery et al., *supra* note 11; Letter to Sec'y Treasury, *supra* note 37.
101 Avery et al., *supra* note 11.
102 CARR ET AL., *supra* note 8, at 7.
103 *Id*. at 3, 7.
104 *Id*. at 1–8.
105 Trey Herr, *Better to Be Realistic About the Security Opportunities of Cloud Computing*, LAWFARE (Mar. 17, 2020), https://www.lawfareblog.com/better-be-realistic-about-security-opportunities-cloud-computing (explaining the additional security systems that Microsoft, Google, and Amazon have in place to detect and handle security risks).

Although the Congresswomen do not reference the Capital One breach, it is worth mentioning for risk purposes. As stated above, the breach was not due to its use of cloud services per se, but rather, it resulted from a firewall created by Capital One and not AWS; however, it is arguable that due to the consolidation by the cloud, it allowed the hacker greater access than would have been possible on servers that do not keep everything under one umbrella.[106] For arguments sake, a technology that allows its clients to build on top of the cloud creates complications that the provider can neither plan for, nor detect or predict to happen.[107] This could lead hackers to steal more than just information by gaining access to the institution's core functions. Although this is a stretch, the Congresswomen would likely argue that a coordinated attack could capitalize on a resulting data breach and generate the significant damage necessary to be considered an institutional risk event. However, this is again a hypothetical and must be weighed against the potentially stifling effects a SIFMU designation will have on innovation.

The characteristics of firms currently designated as SIFMU's differ from the actual working profile of the cloud service providers with respect to the second factor. For example, the National Securities Clearing House ("NSCC") "manages or operates a multilateral system for the purpose of clearing and settling securities transactions among financial institutions and between financial institutions and NSCC."[108] The NSCC steps in if a seller is unable to procure a security, and the clearing house acts as a way of bailing it out. In 2011, "NSCC's peak daily liquidity exposure to a single counterparty [was] $13 billion."[109] Further, the NSCC is "required to contribute up to 25 percent of its retained earnings in the event the clearing fund and other collateral is not sufficient to cover a loss."[110]

Unlike cloud service systems, a disruption caused to the NSCC, and other institutions like it, has the potential to disrupt the market and cause market participants to lose faith in the system if the NSCC is unable to meet its obligations.[111] The failure of organizations like NSCC would not be an operational loss but could create untold market instability; therefore, FSOC was correct in designating the NSCC as a SIFMU because of the potential

---

106 Berthelsen et al., *supra* note 67.

107 *See generally* Brian Wheeler, *Cloud Security Tips: How to Prevent Hackers from Breaching Your Cloud*, DEVOPS.COM (Aug. 19, 2016), https://devops.com/cloud-security-tips-prevent-hackers-breaching-cloud/ (outlining a scenario similar to the above hypothetical).

108 U.S. DEP'T OF TREASURY, *supra* note 94, at 179.

109 *Id.* at 180.

110 *Id.* at 181.

111 DTCC, BEYOND THE HORIZON: A WHITE PAPER TO THE INDUSTRY ON SYSTEMIC RISK 6, 7 (Aug. 2013).

ramifications the disruption of this organization would have to its counterparts and the stability of the markets overall.[112] Conversely, cloud service providers do not inherently share NSCC's risk profile, and therefore the second factor is not met.

As to the third factor—the relationship, interdependencies, or other interactions of the financial market utility with other financial market utilities or payment, clearing, or settlement activities[113]—the Congresswomen urged the Secretary of the Treasury to recognize the importance of developing and enforcing "appropriate safeguards to protect against the possibility of a bank run in the event that a data breach were to negatively impact the public's confidence in cloud-based services and subsequently deter use of cloud-reliant banks."[114] The Congresswomen emphasized that "[s]hould any cloud service provider fail, public mistrust of the service would not be limited to that one company."[115] However, they concluded their analysis by reiterating that it is the speed of the technological development that requires enforcing safeguards in order to maintain continued acceptance of the cloud.[116] Again, this is to assume that a data breach is likely to be caused by a lack of security measures within the cloud, which has not been demonstrated to be true; and even in Capital One's case, Amazon Web Services ("AWS") was not determined to be at fault.[117]

Although their analysis demonstrates the potential fallout from a breach of the cloud,[118] the FSOC has traditionally found institutions to satisfy this third factor based on the extent of interdependence between the institutions and other "payment, clearing, or settlement activities."[119] For example, the Options Clearing Corporation's ("OCC") operations "involve significant interdependence between OCC, other [financial market utilities], settlement banks, clearing members, credit facility lenders, custodians, exchanges, cross-margining entities and pricing vendors."[120] The clearing houses rely on one another if, for instance, a member of the multilateral cross-guaranty agreement

---

112 *Id.* at 7.
113 Letter to Sec'y Treasury, *supra* note 37.
114 Avery et al., *supra* note 11; Letter to Sec'y Treasury, *supra* note 37.
115 Letter to Sec'y Treasury, *supra* note 37.
116 *Id.*
117 Matt Weinberger, *Amazon's Cloud Was at the Heart of the Big Capital One Hack, Even Though it Doesn't Seem to be at Fault*, INSIDER (July 29, 2019), https://www.businessinsider.com/capital-one-hack-amazon-web-services-2019-7.
118 Letter to Sec'y Treasury, *supra* note 37.
119 U.S. DEP'T OF TREASURY, *supra* note 94.
120 *Id.* (OCC is the sole clearing agency for U.S.-listed options in terms of providing clearance and settlement services).

defaults.[121] If this occurs, the members will share in the residual proceeds to restore balance between clearing houses with excess profit and those in a "shortfall position."[122] This kind of relationship illustrates how the current financial market utilities work together and how an impact on one of them would have a domino effect upon the others.

Instead of demonstrating the similarity between the interdependence of the cloud with other financial market utilities, the Congresswomen relied on the argument that the use of the technology in financial institutions alone could create problems for other financial market utilities.[123] However, although a potential breach could cause consumers to mistrust the system, the use of the same technology and its failure by one is unlikely to deter consumers from using all financial institutions. Society has already witnessed a cloud information breach, and it has not caused a "bank run" even from the offending financial institution.[124] Still, this is hypothetical where the designation of institutions such as OCC clearly demonstrates the intricate relationships between it and other financial market utilities, where the relationship is so closely knit that there is a unique reliance and a need for maintaining each of the other like institutions. This interlinked relationship is not present with cloud services, and therefore, it explains why they do not fit within the third category.

Lastly, with respect to the fourth factor, "the Congresswomen highlighted the potentially catastrophic effects of disruption to the cloud . . . [considering] the dependence on cloud-based services not only by all financial institutions in some capacity but also by various government agencies," thereby not only threatening "the financial industry but also government functions and national security."[125] In their letter, they cited a 2016 report by McKinsey, stating that "100 percent of financial institutions use cloud services in some capacity[,] [and] our government has come to rely on Amazon Web Services for a massive share of its data storage needs[.]"[126] Currently, "the Department of Defense holds a $10 billion cloud computing contract with Amazon Web Services, and NASA and the state of Arizona are also clients of [Amazon Web Services.]"[127] As financial institutions and government agencies begin to incorporate the cloud into their technologies, disruption to a cloud service provider could potentially debilitate not only the financial industry but also government

---

121 *Id.*
122 *Id.*
123 Letter to Sec'y Treasury, *supra* note 37.
124 Shen, *supra* note 66; Letter to Sec'y Treasury, *supra* note 37.
125 Avery et al., *supra* note 11.
126 Letter to Sec'y Treasury, *supra* note 37.
127 *Id.*

functions and our national security.[128]

This argument is analogous to the reasons for designating other SIFMUs.[129] As mentioned above, CLS Bank satisfied the fourth factor because a failure or disruption to it "may reduce FX market activity and the flow of funds in US and foreign financial markets and to the broader economy."[130] To disrupt the flow of funds in the US or foreign financial markets would have clear ramifications on financial institutions and the economy as a whole.[131] Similarly, the Depository Trust Company ("DTC") was found to meet the criteria for the fourth factor because of the devastating impact that would occur if it were to fail.[132] The ramifications of such an event could potentially lead to "spillover effects on the rest of the U.S. economy, [a reduced] amount of credit available generally, [a reduced] value of household savings and corporate reserves, affecting the financing activities of corporations, destabilizing U.S. money market funds, and reducing the availability of secured credit."[133] Such events would lead to financial instability and potentially raise concerns for the country's national security. These potential domino fallouts are similar to the concerns the Congresswomen addressed in their letter.[134] The overall potential disruption to our financial markets, coupled with the effect on basic government functions, is similar to the potential financial market and institutional disruption that the FSOC evaluates when designating an institution or third-party as a SIFMU.[135] Like the case of CLS Bank, if as a result of its own use of the cloud there is a disruption that leads to government concern that its data information is at risk based on a breach within the financial services industry, then such an event could lead the agency or institution to quickly transfer its platform for fear of a breach itself.[136] Therefore, this single factor regarding the effects of potential cloud disruption provides one of the strongest arguments in favor of the Congresswomen's position that cloud service providers should be designated as SIFMUs.[137]

Finally, the FSOC may, instead of considering all of the factors equally,

---

128 *Id*.

129 U.S. DEP'T OF TREASURY, *supra* note 94.

130 *Id*. (the FX or currency market is an over-the-counter global marketplace that determines the exchange rate for currencies around the world. Participants are able to buy, sell, exchange, and speculate on currencies on this market.).

131 *Id*.

132 *Id*.

133 *Id*.

134 Letter to Sec'y Treasury, *supra* note 37.

135 *Id*.

136 *See* Avery et al., *supra* note 11 (acknowledging generally that a data breach will negatively impact confidence in, and use of, cloud-based systems).

137 Letter to Sec'y Treasury, *supra* note 37.

determine "whether the failure or disruption of the [financial market utility] would create or increase the risk of credit and liquidity issues among financial institutions and markets, and whether such credit and liquidity issues would threaten the stability of the US financial system."[138] At this moment, there are three cloud service providers dominating the industry: Azure, Google Cloud, and AWS, which creates a lack of substitutability.[139] This, coupled with the inability to quickly transfer from one service provider to another if one should fail, creates a systemic risk.[140]

This is the Congresswomen's overall strongest argument because it speaks to the future ramifications. Rather than the actual function of the technology, this last factor is more concerned with its potential disruptive nature.[141] This characteristic of the cloud is likely what pushed the Congresswomen to bring the issue forward. And they're not alone in their plight for some form of regulation; "[w]orld financial market regulators share the concerns regarding the ramifications of cloud-based disruption or failure on financial institutions and markets."[142] As these cloud-based technologies have improved and become prevalent in a wide-range of industries, governments around the world are struggling with how to manage them and the unknown consequences of their use.[143] It should be noted that data collected by Morpheus Data found "that the total time lost from cloud outages of the 3 top [cloud service providers] in 2017 was an aggregate of just 16 hours across all industries, not just financial institutions."[144] This fact should give significant comfort to governments and market participants alike that the largest cloud service providers are carefully monitoring the greatest risks of market disruption and creating multiple levels of controls to ensure their systems work as designed.

In February 2019, the Financial Stability Board "noted that technology could upend the stability of the financial markets."[145] In further support of the Congresswomen's position, the Joint Committee of the European Supervisory Authorities issued a report to the European Commission in April 2019, which stated that cloud "computing services are central to financial institutions and highlight the vulnerabilities of the financial industry's reliance on cloud

---

138 Avery et al., *supra* note 11; Letter to Sec'y Treasury, *supra* note 37.

139 Letter to Sec'y Treasury, *supra* note 37.

140 *Id.*

141 Avery et al., *supra* note 11.

142 *Id.*; Letter to Sec'y Treasury, *supra* note 37.

143 Hedaia-t-Allah Nabil Abd Al Ghaffar, *Government Cloud Computing and National Security*, REV. OF ECON. & POL. SCI., (Mar. 23, 2020), https://www.emerald.com/insight/content/doi/10.1108/REPS-09-2019-0125/full/pdf?title=government-cloud-computing-and-national-security.

144 CARR ET AL., *supra* note 8, at 5.

145 Avery et al., *supra* note 11.

services."[146] Although regulatory bodies around the world are aware of the potential implications of cloud services, they are still unable to determine the best regulation without stifling potentially beneficial innovation.[147]

While there is international and domestic consensus that there is reason to be concerned by unregulated cloud service providers, the FSOC would need to determine that emergency conditions exist before designation should occur.[148] Currently, no emergency conditions apply.[149] The functions that the Congresswomen fear most have not been transitioned to the cloud.[150] It is inevitable that they will be, but the industry is being as cautious as possible, because likewise, it does not want to do anything that would disrupt the market. As noted above, it will be a slow and strategic process transitioning transaction functions to the cloud. Therefore, it is not necessary to jump the gun by regulating them under a designation that does not fit.

If these emergency conditions do not apply, institutions argue that there are other regulatory practices that are and have always been in place to deal with the unknown risks that come with cloud services.[151] The least intrusive way to evaluate the cloud service provider risk is to expand guidance on it, while developing and learning from the providers and other countries grappling with the same dilemma; however, the answer cannot be found in applying an ill-fitting designation for lack of an obvious alternative.

VI. IF THE SHOE DOES NOT FIT, WHAT ARE THE OTHER OPTIONS?

If this technology is going to become common place in a wide variety of industries, it is unrealistic to leave it unregulated. "[E]ven though the use of the cloud by financial institutions is currently limited, it can expand very fast and become critical infrastructure in the near future," making it imperative for the

---

146 *Id.*

147 *See* Mark O'Conor et al., *How to Regulate Cloud Computing?*, GUARDIAN (Mar. 28, 2013), https://www.theguardian.com/media-network/media-network-blog/2013/mar/28/regulation-cloud-computing-data-protection (detailing a series of potential steps for regulating the cloud but concluding that it seems that businesses will remain at the heart of contracting for technology in the way that best suits them).

148 Avery et al., *supra* note 11.

149 *See* Lee Rubin, *Cloud Computing and Regulation: Following the Eye of the Storm*, DATA CTR. DYNAMICS (May 29, 2019), https://www.datacenterdynamics.com/en/opinions/cloud-computing-and-regulation-following-eye-storm/ (highlighting the lack of standardized guidance for the rapidly growing cloud computing sector: there is no overarching "cloud law" and this is problematic).

150 CARR ET AL., *supra* note 8.

151 *See id.* (stating that some argue "there is no fundamental reason why firms cannot use cloud services in a regulatory compliant manner").

government and providers to get on the same page.[152] Rather than shoehorn the cloud into a regulatory framework that does not fit its unique qualities, the government should consider other alternatives, such as: pursuing a multi-vendor strategy, allowing banks to apply their current regulatory and compliance requirements, or following the European Bank Authority by creating new regulatory measures to fit this evolving technology.[153]

One of the fundamental risks faced by institutions using cloud service providers is the potential for cloud failure or other "operational risks."[154] Although clouds have not faced lengthy fail or down periods in the past, this does not mean that it is impossible.[155] The process of using the cloud creates a single point of failure, which could pose substantial risks to financial and governmental stability; therefore, implementing a multi-vendor strategy would ensure that there is "no one key cloud provider for any given [financial institution]."[156] If the government or institutions can work with cloud providers to draw from one another and ensure an immediate back-up if one service fails, then it would guarantee that disruption to one provider would not be detrimental to the stability of the entire system.[157] Instead, the institution could rely on the other cloud service while the failed provider works to bring the servers back online.[158]

This system would promote stability and competition, but it requires an increase in cloud firms.[159] Presently, there are a limited number of major cloud service providers with Amazon Web Services making up almost 50 percent of the market share, followed by Azure, Google, IBM, and Alibaba.[160] To properly implement a multi-vendor system, more firms must enter the existing market. Hopefully, as more institutions relocate their data to these servers, new providers will enter the market and can act as complements, or back-ups, to the leading firms.[161] However, given this solution is premised on more firms entering the market, it is not necessarily the safest route for institutional stability.[162] It may be more realistic to consider this as an option in the future, depending on how quickly financial institutions transition their functions to the

---

152 CARR ET AL., *supra* note 8, at 6.

153 *Id*. at 6–8.

154 FIN. STABILITY BD., THIRD-PARTY DEPENDENCIES IN CLOUD SERVICES CONSIDERATIONS ON FINANCIAL STABILITY IMPLICATIONS 2 (Dec. 9, 2019), https://www.fsb.org/wp-content/uploads/P091219-2.pdf.

155 CARR ET AL., *supra* note 8, at 5.

156 *Id*. at 6.

157 *Id*. at 6–7.

158 *Id*.

159 *Id*. at 7.

160 *Id*. at 7.

161 *Id*. at 6–7.

162 *Id*.

cloud. It should be recognized as an option if firms are unwilling to deal with strict government regulations.

The second alternative is to allow banks and financial institutions to negotiate regulatory and risk applications with cloud service providers. Banks and financial institutions are already governed by regulatory and compliance obligations.[163] These obligations have historically, and currently, apply to any third-party vendor or contractor that the institutions employ.[164] This is the largest challenge firms must face: to demonstrate to regulators "that financial institutions are sufficiently competent to partner with [cloud service providers] in the understanding and management of the risks and migration to (and operation in) the cloud."[165] When a financial institution enters into an agreement with a third-party for an important, new, or existing function or service, it must "undergo a strict risk assessment and due diligence of the provider[.]"[166] For instance, some banks "have adopted the policy of not moving any material workload to a public cloud provider that increases their risk profile, meaning that their use of cloud is net neutral in terms of risk."[167]

Furthermore, financial regulators require financial institutions to audit a service they have outsourced, which requires access to the provider's premises, devices, systems, networks, and data involved for providing the service.[168] Financial institutions are not only required to perform some form of audit, but they are also further required to establish the right of their governing regulators to audit the cloud service provider.[169]

The two governing laws of cloud service providers are the Bank Service Company Act ("BSCA") and the Gramm-Leach-Bliley Act ("GLBA").[170] The BSCA provides federal banking agencies with "the authority to examine and regulate the activities, functions, and operations performed by third-party service providers to the same extent as if they were performed by the bank itself."[171] Under the Dodd Frank Act, the Consumer Financial Protection

---

163 *See generally Banking Regulation 2021 | USA*, GLOBAL LEGAL INSIGHTS, https://www.globallegalinsights.com/practice-areas/banking-and-finance-laws-and-regulations/usa (last visited Mar. 19, 2021).

164 BRAD CARR ET AL., INST. OF INT'L FIN., CLOUD COMPUTING IN THE FINANCIAL SECTOR PART 3: CLOUD SERVICE PROVIDERS 5 (Aug. 2018), https://www.iif.com/Portals/0/Files/32370132_iif_cloud_part_3_-_final.pdf.

165 *Id.* at 3.

166 *Id.* at 4.

167 *Id.*

168 *Id.* at 4, 6.

169 *Id.*

170 Bank Service Company Act, 12 U.S.C. §§ 1861–1867(c); Gramm-Leach-Bliley Act, PUB. L. NO. 106-102, § 502, 113 Stat. 1138, 1437 (1999); Memorandum to Comm. On Fin. Servs., *supra* note 6.

171 Lawrence D. Kaplan & Kevin L. Petrasic, *Bank Vendor Management – An Aspirin to*

Bureau ("CFPB") has the authority "to review service providers' operations and initiate enforcement actions against both a bank and its service provider for violations of any law[.]"[172] Although the CFPB's job is primarily to oversee the financial institutions, guidance released by the agency warns third-party vendors that "they have an independent obligation to comply with all laws, regulations, and guidance that their counterparty banks are subject to, with no allowance or concessions provided for failing to fully understand these requirements, even where the bank customer fails to."[173] This regulation provides the CFPB with the authority to oversee cloud service providers when they act as third-party vendors to banks.[174] Although it is not a direct allocation of oversight power, it still requires some accountability from service providers to meet the same regulatory standards as the financial institutions.[175]

Furthermore, Section 503 of the GLBA requires a financial institution to describe its "policies and practices with respect to collecting and disclosing nonpublic personal information about a consumer to both affiliated and nonaffiliated third parties."[176] The Act further requires the institution to allow its consumers to "opt-out" of their information being shared with third-party vendors.[177] Indirectly, this would require cloud service providers to provide information on its security and information-sharing policies so that the institution could fulfill its obligation under the GLBA.[178] Like the BSCA, this would generate some accountability from the cloud service provider just by entering into a contract with a financial institution as a third-party vendor.

As such, although the government prefers stricter regulation for cloud service providers, there already is some in place.[179] By allowing financial institutions and cloud service providers the ability to govern the audit and oversight of their service contract, they can apply the already existing regulations as they fit with their special relationship.[180] There are many functions of the cloud, and given much of the technology is still evolving or

---

Prevent a Headache or Just a Headache?, PAUL HASTINGS (April 2014), https://www.paulhastings.com/docs/default-source/PDFs/third-party-vendor-management6fb8e06923346428811cff00004cbded.pdf.

172 *Id.*

173 *Id.*

174 *Id.*

175 *Id.*

176 Gramm-Leach-Bliley Act, PUB. L. NO. 106-102, § 503, 113 Stat. 1138, 1437 (1999); FED. DEPOSIT INS. CORP., FDIC CONSUMER COMPLIANCE EXAMINATION MANUAL 1 (2016), https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf.

177 Gramm-Leach-Bliley Act, PUB. L. NO. 106-102, § 502, 113 Stat. 1138, 1437 (1999); FED. DEPOSIT INS. CORP., *supra* note 176.

178 Gramm-Leach-Bliley Act, PUB. L. NO. 106-102, § 502, 113 Stat. 1138, 1437 (1999).

179 *See generally* Kaplan & Petrasic, *supra* note 171; FED. DEPOSIT INS. CORP., *supra* note 176.

180 CARR ET AL., *supra* note 164, at 9.

being integrated to financial institutions' core functions, it is hard to say now which exactly apply for the specific software or cloud being used by that institution. If the government continues to hold financial institutions accountable for auditing and oversight of their third-party contractors, then this should constitute sufficient regulation until core functions or new functions become integrated.

However, it has been asserted that "the relationship between financial institutions and public cloud providers is fundamentally different from traditional outsourcing relationship[s] – financial institutions that use the public cloud share computing resources with thousands, if not millions of other customers located across multiple jurisdictions."[181] This may mean that it will be impossible to treat cloud service providers like other third-party vendors by applying the existing regulations.[182] If this is truly the case, the government may need to reassess its playbook entirely.

If the two aforementioned solutions are too weak, or rely too heavily on potential future developments, it is instead possible to look to other countries around the world that are dealing with this conundrum and that are applying new techniques to address cloud regulation.[183] The European Bank Authority has introduced "the possibility of exercising those audits and access rights by using any of the following means: pooled audits organized jointly with other clients of the same cloud service provider and performed by these clients or by a third-party appointment by them, third-party certifications, and third-party or internal audit reports made available by the cloud service provider."[184] This approach has been regarded as more flexible compared to others and "has the benefit of increasing the efficiency of this process, likely raising the average quality of auditing while also reducing the burden of both the [financial institutions] and the [cloud service providers]."[185]

If a more flexible approach is still too lenient a measure, and the government finds it is in their best interest to apply stricter regulations, it should still take note of its allies' actions.[186] For example, the European Commission has initiated a joint approach to work with groups on cloud switching, porting data, and on cloud-security certification.[187] These groups are "co-chaired by representatives from the cloud service industry and from business users of cloud services to ensure a necessary balanced approach to

---

181 SCOTT ET AL., *supra* note 2, at 5.
182 *Id.* at 27–33.
183 *Id.* at 18.
184 CARR ET AL., *supra* note 164, at 4.
185 *Id.* at 5.
186 *Id.* at 9–10.
187 *Id.* at 9.

this work."[188] It may seem trivial, but conversations between regulators, financial institutions, and cloud service providers would provide the most holistic approach to determining the best frameworks, programs, and processes to increase the use of cloud services and address the associated risks.[189] It could also alleviate some of the animosity between the aforementioned parties, so that each feels like they are walking away with a fair deal.

VII. CONCLUSION

The SIFMU designation is the not the correct designation for cloud service providers. Although there is room for potential disruption from these providers, they do not fit within any of the current taxonomical factors for SIFMU designation. At present, such designation would only be fitting given an emergency situation. Currently, there are regulatory and oversight measures in place or moderate regulatory practices that could be put in place. The superior system of oversight would be a process of regulatory engagement and supervision with new financial technology firms. Specifically, a real-time engagement of government examiners as the systems are being built is a preferred approach to integrating financial technology firms with the more heavily regulated financial institutions. Through open channels of communication between institutions, financial technology firms, and regulators, parties can share best practices throughout the industry. This would create an environment that would hopefully demonstrate to regulators that the best security and privacy measures are being implemented throughout this new critical industry.

There is not a government in the world that does not recognize that financial institutions are moving swiftly to integrate cloud systems and the potential risks that come with it. Rather than forcing a designation that does not clearly fit, the government should create a separate regulatory body for cloud service providers. Providers' services are unique in themselves and in what they provide to their clients. Providers do not fall naturally into any existing US regulatory designations. If the government does not feel that financial institutions can perform suitable oversight, then it will need to create a specialized body that can.

---

188 *Id.*

189 *Id.* at 9–10