BANKING ON THE CLOUD

Colleen Baker, David Fratto, & Lee Reiners†*

Abstract

Cloud computing is fast becoming a ubiquitous part of today's economy for both businesses and individuals. Banks and financial institutions are no exception. While it has many benefits, cloud computing also has costs and introduces risks. Significant cloud providers are single points of failure and, as such, are an important new source of systemic risk in financial markets. Given this reality, this article argues that such institutions should be considered critical infrastructures and designated as systemically important financial market utilities under Dodd-Frank's Title VIII.

* Colleen Baker, Assistant Professor of Legal Studies, University of Oklahoma Price College of Business; David Fratto, Associate, Weil, Gotshal & Manges LLP, any views or opinions represented in this article belong solely to the author in his personal capacity. Nothing in this article is attributable to Weil, Gotshal & Manges LLP; and, Lee Reiners, Lecturing Fellow and Executive Director of Duke Law School's Global Financial Markets Center.

† This article extends and incorporates David Fratto & Lee Reiners, *A New Source of Systemic Risk: Cloud Service Providers*, THE FINREG BLOG (Aug. 8, 2019), https://sites.duke.edu/thefinregblog/2019/08/08/a-new-source-of-systemic-risk-cloud-service-providers/, and it also extends Colleen Baker's work on Dodd-Frank's Title VIII in articles such as *The Federal Reserve As Last Resort*, 46 U. MICH. J.L. REFORM 69 (2012).

I. INTRODUCTION

In April 2019, Federal Reserve Bank of Richmond (FRBR) examiners paid a visit to an Amazon facility in Virginia.[1] The Bank Service Company Act provided them with minimal powers for this call. However, there was no red-carpet rollout to greet the visitors. Instead, they were chaperoned by an employee and allowed only a limited, no copies taken, document review. The examiners were purportedly also unaware at that time that a hacker had compromised Capital One data – a bank supervised by the FRBR – stored on Amazon's cloud.[2] The breach exposed credit card application information of around 106 million people.[3] Multiple lawsuits related to the incident have been filed, including against Amazon.[4] "[W]hether they want to be or not," cloud service providers "such as Amazon are now . . . crucial player[s] in the U.S. banking system."[5]

Cloud computing is fast becoming ubiquitous in today's economy for businesses and individuals. As highly-regulated entities, banks have been slower to the party; but, this is changing.[6] For example, Bank of America (BoA) announced plans "to deliver 80 percent of its technological functions on virtual platforms and with public cloud infrastructure" in the near future.[7] A 2016 McKinsey Report noted that nearly 100% of financial

---

[1] Liz Hoffman, Dana Mattioli & Ryan Tracy, *Banks' Cloud Practices Face Fed's Scrutiny*, WALL ST. J. (August 2, 2019), https://www.wsj.com/articles/fed-examined-amazons-cloud-in-new-scrutiny-for-tech-11564693812, at A1.

[2] In 2018, Amazon captured about half of the public cloud market. *Id.*

[3] Nat Levy, *Amazon and Capital One Face Legal Backlash After Massive Hack Affects 106M Customers*, GEEKWIRE (Aug. 9, 2019, 12:16 PM), https://www.geekwire.com/2019/amazon-capital-one-face-lawsuits-massive-hack-affects-106m-customers/.

[4] *Id.*

[5] Hoffman, *supra* note 1, at A1. *But see* Christina Rexrode & Emily Glazer, *Global Finance: Amazon Cloud Service Is Aimed at Big Banks*, Wall ST. J. at A1 (reporting on Amazon's courtship of banks for its cloud services) (Feb 23, 2016).

[6] *See generally* U.S. DEP'T OF TREASURY, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (July 2018) [hereinafter Treasury Report]. *But see* Deutsche Bank, *Regulation Driving Banking Transformation* (Oct. 2018), https://cib.db.com/docs_new/GTB_Digital_Whitepaper.pdf [hereinafter Banking Transformation] (discussing banks history of private cloud usage).

[7] Letter from Katie Porter, Congresswoman, and Nydia M. Velazquez, Congresswoman, to Steven T. Mnuchin, Sec'y, U.S. Dep't of Treasury (Aug. 22, 2019), (https://velazquez.house.gov/sites/velazquez.house.gov/files/FSOC%20cloud%20.pdf) (citing *Bank of America Chooses the Microsoft Cloud to Support Digital Transformation*, MICROSOFT NEWS CENTER (Oct. 2, 2017)), https://news.microsoft.com/2017/10/02/bank-of-america-chooses-the-microsoft-cloud-to-support-digital-transformation/ [hereinafter Mnuchin Letter].

institutions use some form of cloud computing.[8] Consequently, multifaceted scrutiny of banks' use of cloud services is set to accelerate. Across the globe, banking regulators are increasingly focusing in on financial market innovations,[9] such as the use of cloud computing, which presents both known and unknown risks to financial market stability. Hence, as banks and financial institutions[10] continue their march to the cloud, the type of supervisory visit described above is simply not going to cut it.

This article contends that significant cloud service providers are core infrastructures in financial markets and, therefore, critical financial market utilities (FMUs). Accordingly, it argues that significant cloud service providers should be designated by the Financial Stability Oversight Council (FSOC)[11] as systemically important financial market utilities (SIFMUs) under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank). It expands upon work by the authors on financial market utilities[12] and by Professor Nizan Geslevich Packin, arguing that key digital service providers should be designated as "Critical Service Providers."[13] Indeed, Congresswomen Katie Porter and

---

[8] Nagendra Bommadevara, Andrea Del Miglio & Steven Jansen, *Cloud Adoption to Accelerate IT Modernization*, *Digital McKinsey: Insights* 12, 14 (Apr. 2018), https://mckinsey.com/business-functions/mckinsey-digital/our-insights/cloud-adoption-to-accelerate-it-modernization#.

[9] *See* Bank of England, Financial Stability Report 4944-4849 (July 2019), https://www.bankofengland.co.uk/financial-stability-report/2019/july-2019; Alan W. Avery, Nicola Higgs and Fiona M. Maclean, *FSB Concerns Over Cloud Concentration in Financial Services Continues,* GLOBAL FINTECH & PAYMENTS BLOG (Oct. 8, 2019), https://www.fintechandpayments.com/2019/10/fsb-concerns-over-cloud-concentration-in-financial-services-continues/#page=1.

[10] This article uses the phrase "banks and financial institutions," and the individual terms "bank" or "financial institution" almost interchangeably. However, readers unfamiliar with banking and financial institutions law should realize that while all banks can be considered financial institutions, not all financial institutions are, from a legal perspective, banks. Banks are among the most highly regulated institutions, but this is not necessarily the case for all non-bank financial institutions, some of which are barely regulated at all.

[11] The Financial Stability Oversight Council, established by the Dodd-Frank Wall Street Reform and Consumer Protection Act, is a government council of financial regulators chaired by the Secretary of the U.S. Treasury Department. See generally Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 111, 124 Stat. 1392, 1393 (2010) (codified at 12 U.S.C. § 5321).

[12] *Supra* note †.

[13] Nizan Geslevich Packin, *Too-Big-To-Fail 2.0? Digital Service Providers as Cyber-Social Systems*, 93 IND. L.J. 1211 (2018) (arguing that key digital service providers, like the largest financial institutions, are too big to fail and should be recognized as such).

Nydia M. Velázquez wrote to U.S. Treasury Secretary Steven T. Mnuchin requesting that the FSOC consider Title VIII designations for Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, which currently capture the greatest percentage of the cloud computing market.[14]

The FSOC refers to designated FMUs as the "plumbing of the financial system."[15] As this article demonstrates, this description aligns closely with the services cloud firms provide to banks and financial institutions, specifically, the provision of infrastructure and platform computing services. As banks accelerate their use of cloud services, the risk that these technology service providers will pose to financial market stability will escalate.[16] Similar to the eight existing SIFMUs,[17] significant cloud service providers are single points of failure and will come to represent one of the most important systemic risks to global financial market stability. In fact, SIFMUs such as the Options Clearing Corporation are themselves increasingly relying on cloud services.[18] This reality significantly bolsters the argument for designating such cloud service providers as SIFMUs.

The FRBR examiners' spring 2019 visit to an Amazon facility arguably supports this new reality. An appropriate regulatory framework for cloud service providers is beyond the scope of this article; however, it lays important groundwork towards this task. It demonstrates that significant cloud service providers could and should be SIFMUs. This article proceeds as follows: Part I provides a brief overview of cloud computing; Part II analyzes benefits, costs, and risks associated with banks and financial institutions' use of cloud services; Part III examines relevant legal and regulatory considerations; Part IV argues that cloud service providers will increasingly constitute a critical risk to financial market stability, and

---

[14] Mnuchin Letter, *supra* note 7.

[15] *See* Press Release, U.S. Dep't Treasury, Financial Stability Oversight Council Makes First Designations in Effort to Protect Against Future Financial Crises (Jul. 18, 2012) (on file with author).

[16] *See* Brendan Pedersen, *Does Amazon-Google-Microsoft Hold on the Cloud Pose a Risk to Banking?,* AMERICAN BANKER (Sept. 30, 2019), https://www.americanbanker.com/news/does-amazon-google-microsoft-hold-on-the-cloud-pose-a-risk-to-banking.

[17] *Designated Financial Market Utilities*, FEDERALRESERVE.GOV, https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm (last visited Jan. 24, 2020).

[18] *OCC Launches Renaissance Initiative to Modernize Technology Infrastructure*, THE OPTIONS CLEARING CORPORATION, https://www.theocc.com/about/newsroom/releases/2019/january-14-occ-launches-renaissance-initiative-to-modernize-technology-structure.jsp (last visited Jan. 24, 2020).

that cloud service providers should be designated as SIFMUs under Dodd-Frank's Title VIII; and the conclusion follows.

II. BRIEF OVERVIEW OF CLOUD COMPUTING

Cloud computing turns the outdated enterprise data center model on its head by creating advantages in scale, resource elasticity, organizational agility, and operational resiliency. No one definition of cloud computing exists. The National Institute of Standards and Technology defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[19] Cloud resources can be deployed as: public, in which there is a public sharing of cloud resources; private, in which specific cloud resources, owned by the user or third-party, are restricted to one user; community-based, in which resources are shared by select users and owned by one or more of these users or a third-party; or hybrid, a combination of approaches.

Three cloud service models also exist to characterize the services provided by the cloud to the user and vary in terms of the extent of customer outsourcing and customization ability. They are explained in Figure 1, and include: Software as a Service, in which customers rely on the provider for management of applications, computing resources, and infrastructure; Platform as a Service, in which customers can control applications, but providers manage computing resources and infrastructure; and Infrastructure as a Service, in which customers control "fundamental computing resources" and providers manage the underlying infrastructure.[20] Banks and financial institutions have used all of the deployment and service models.[21]

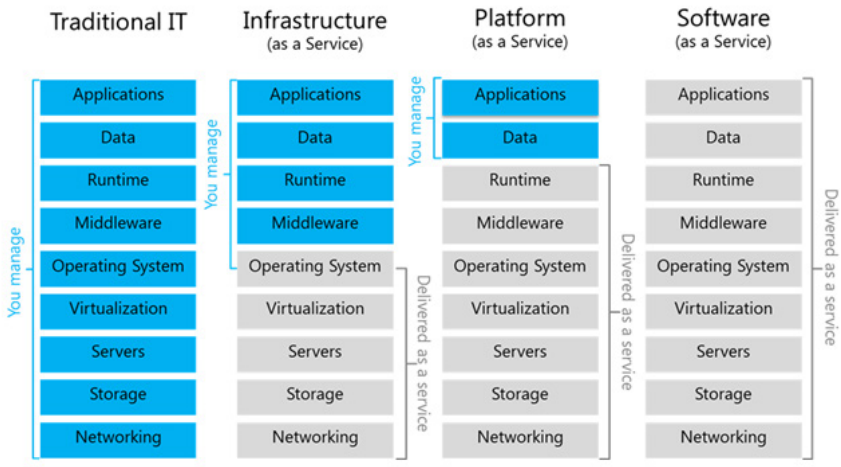
---

[19] Peter Mell & Timothy Grance, The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology, Special Publication 800-145 (2011).

[20] *Id.*

[21] Treasury Report, *supra* note 6, at 48.

Figure 1: Comparison of Cloud Computing Service Models[22]



While customers can transfer their data and operations to the cloud, banks have generally been cautious about migrating critical data and operations. Instead, banks are taking an incremental approach leading first with non-core data aspects and operations. However, banks are increasingly considering "the possibility of migrating core systems from private to public clouds, signifying a significant leap forward."[23] Indeed, some banks, such as Capital One, no longer support their own proprietary data centers and have instead migrated "much of their digital footprint to the cloud."[24] Analysts predict that almost 40% of financial service firms will process half of their transactions on the cloud by 2020.[25] Within 5-10 years, banks could rely on cloud service providers for "the vast majority of their computing needs."[26] Increased migration to the cloud will require high comfort levels about such arrangements from a regulatory perspective, particularly in regard to sensitive data and critical functions.[27]

A limited number of significant cloud service providers exist. This is typical of SIFMUs. Most SIFMUs – such as designated clearinghouses – are essentially natural monopolies.[28] AWS captured about half of the

[22] David Chou, *Cloud Service Models (IaaS, PaaS, SaaS) Diagram*, DAVID CHOU BLOG (Sept. 28, 2018), https://dachou.github.io/2018/09/28/cloud-service-models.html.

[23] Banking Transformation, *supra* note 6, at 16.

[24] Hoffman et al., *supra* note 1.

[25] Matt VanderZwaag, *The Financial Services Industry Looks to the Cloud*, DATA CENTER KNOWLEDGE (Mar. 5, 2018), https://www.datacenterknowledge.com/industry-perspectives/financial-services-industry-looks-cloud.

[26] Treasury Report, *supra* note 6, at 49.

[27] *See id.* at 50–51.

[28] For additional information on clearinghouses, see Colleen Baker, Incomplete Clearinghouse Mandates, 56 Am. Bus. L. J. 507–581 (2019).

public cloud market in 2018,[29] followed by Microsoft Azure, and then Google. Market share data for cloud service providers is difficult to aggregate for two reasons: little information is available in public disclosures, and any published data quickly becomes outdated. Although determining the three providers' exact share of the market is difficult, estimates range from approximately 53-73%.[30] An inherent barrier to market entry is the tremendous resources needed to compete in this area. Hence, competition is limited. Substitutability is also limited should problems arise at a provider. Such concerns have long plagued SIFMUs. In sum, disruption at AWS or another significant cloud provider could prove fatal to one or more banks or financial institutions and send shockwaves throughout our financial system. Such entities are undoubtedly a new source of risk in financial markets.

III. BENEFITS, COSTS, AND RISKS OF USING CLOUD SERVICES

A. Benefits

Cloud computing enables banks and financial institutions to nimbly and rapidly respond to customer demands for customized products and experiences.[31] Indeed, banking on the cloud has many benefits, including this flexibility, potential for rapid innovation, reduced capital investment, superior resource allocation, global presence, operational resiliency, and heightened cybersecurity. Cloud resources are scalable to demand; banks can use as much or as little of a provider's resources as needed. On an appropriate cloud infrastructure, the capacity available to a bank can be effectively unlimited. From a business strategy perspective, updated applications and platform transformations are significantly simpler on a cloud system. This allows cloud-enabled businesses to respond more

[29] Hoffman et al., *supra* note 1.

[30] *See AWS vs Azure vs IBM Cloud, Which Is the Best For Me?*, NODERICKS TECHNOLOGIES (Feb. 21, 2018), http://www.nodericks.com/aws-vs-azure-vs-google-vs-ibm-cloud-best/; *Custom Applications and IaaS Trends* CLOUD SECURITY ALLIANCE, (2017), https://downloads.cloudsecurityalliance.org/assets/survey/custom-applications-and-iaas-trends-2017.pdf.

[31] *See* Institute of International Finance, *Cloud Computing in the Financial Sector Part 1: An Essential Enabler* (2018). https://www.iif.com/portals/0/Files/private/32370132_cloud_computing_in_the_financial_sector_20180803_0.pdf.

quickly to consumer demands and rapidly deliver new or updated products to market.[32]

The tremendous computing resources of cloud providers also increase banks and financial institutions' opportunities to fully leverage their data. Data is one of today's most valuable commodities. Cloud use not only facilitates the collection and storage of massive amounts of data, but also sophisticated and innovative analyses of this information.[33] Reams of data can be analyzed and deployed by cutting-edge artificial intelligence, machine learning and blockchain technologies that most banks' and financial institutions' IT systems would be unable to support.[34]

Use of cloud services also enables banks to reduce costs associated with maintaining a complex, internal information technology infrastructure requiring significant staff, maintenance, updates, and provision for maximum potential resource use. Unlike most banks and financial institutions, significant cloud providers have the tremendous resources necessary to continuously invest in cutting-edge security technologies.[35] Cybersecurity risk is likely the greatest potential cost banks face. However, the overall security benefit to the financial system remains unclear. Cloud computing might provide individual institutions a higher level of security, but ultimately a lower level of security to the overall system as the concentration of providers focuses the efforts of cybersecurity attackers.

Currently, however, such cost savings are a secondary motivation inducing banks and financial institutions to undertake the investment of switching from enterprise to cloud computing.[36] Three factors are ultimately of greater importance. First, cloud computing lowers barriers

---

[32] *See* IBM INSTITUTE FOR BUSINESS VALUE, *Cloud For Financial Markets: Driving Growth, Gaining Competitive Advantage and Improving Efficiency* 2 (2015), https://ibm.com/downloads/cas/KO5LM4DG.

[33] Banking Transformation, supra note 6, at 17.

[34] *Id.*

[35] *E.g.*, Philip Stafford, *Cyber Threats Force US Clearing House on to Cloud*, Fin. Times, (Mar. 14, 2018), https://www.ft.com/content/f61770b4-2784-11e8-b27e-cc62a39d57a0 (quoting Jon Davidson, then COO of the Options Clearing Corporation, stating that "Amazon is going to spend billions on information security for Amazon Web Services this year."

[36] *See* THE ECONOMIST INTELLIGENCE UNIT, *Mapping the Cloud Maturity Curve: Measuring Organisational Excellence in the New Era of IT* 8 n.d. (discussing a cloud maturity curve. In an industry survey, banking and financial services executives listed the top three impacts of cloud computing services to be: (1) improved data access, analysis and utilization; (2) speedy delivery of new IT services and capabilities; and (3) improved internal business process efficiency.).

to entry and facilitates disruptive innovation by providing scaled resources with minimal marginal cost. Second, the time-to-market advantage of cloud computing allows organizations to quickly launch new products and integrate newly acquired capabilities. Third, it facilitates greater responsiveness to customers. Because cloud-enabled organizations benefit from better infrastructure and computing platforms, applications can be more quickly refined to meet rapidly shifting consumer demands.[37]

B. Costs and Risks, Old and New

As a new technology, cloud computing has risks both known and unknown. These unknown risks are the greatest potential cost of cloud computing. Yet not migrating to the cloud and "being left behind" might also be among an institution's greatest risks in this context. [38] A top concern of banks and financial institutions in using cloud services is security. The recent hack of Capital One's cloud-stored data validates this worry. Costs of using cloud computing also include those associated with transitioning from old IT systems, potential connectivity issues, maintaining data confidentiality, the risk of provider lock-in, limited leverage around pricing, and legal/regulatory risk domestically and internationally.[39]

The Federal Financial Institutions Examination Council (FFIEC) views cloud computing as "another form of outsourcing with the same basic risk characteristics and risk management requirements as traditional forms of outsourcing."[40] The FFIEC Information Technology Examination Handbook for risk and risk management considerations is applicable to the cloud services context.[41] Outsourcing to third-parties creates legal, regulatory, business, and reputational risk for banks and financial institutions. Hence, even if vendor relationships with cloud service providers minimize certain costs for banks, they create others. For example, as with traditional third-party outsourcing arrangements, when contracting with a cloud service provider, banks must be concerned with

---

[37] *See id.*

[38] Institute of International Finance, *Cloud Computing in the Financial Sector Part 1: An Essential Enabler* 7 (2018).

[39] *See* TREASURY REPORT*, supra* note 6, at 50.

[40] FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, OUTSOURCED CLOUD COMPUTING 1 (2012).

[41] *See id.*

appropriate due diligence, vendor management, monitoring and auditing, information security issues, operational resiliency, and disaster planning.[42]

Proper due diligence requires understanding the service provider's data protection processes, the potential sharing among clients of cloud network and server resources, the safeguarding of data privacy and confidentiality, and the provision for disaster, recovery, and business continuity.[43] Banks' relationships with cloud service providers must contractually address issues such as data ownership, storage and location, accessibility, format, and protection as well as deletion once the vendor relationship terminates.[44] The service provider should be familiar with financial industry requirements related to the suitability of its internal controls, which will eventually be audited for effective risk management, and customers' legal and regulatory compliance requirements.[45] Banks can contractually require a cloud service provider to comply with relevant laws and regulations, and attempt to ensure such compliance through monitoring and audits.[46] Nevertheless, a bank's board of directors and senior management are ultimately responsible for ensuring that third-parties to whom they outsource – such as cloud providers – meet legal and regulatory requirements, in addition to operating in a safe and sound manner.[47]

Industry participants report that significant service providers such as AWS, Google, and Microsoft Azure seem to be increasingly attuned to banks' regulatory environment, and "[t]here appears to have been a shift from cloud providers to address regulators' concerns over security, privacy and financial services regulation – alongside a corresponding willingness from regulators to work with cloud service providers on adoption guidelines."[48]

Commentators have cautioned that banks and financial institutions outsourcing relationships to traditional third-parties – a one to one arrangement – are importantly distinct from their outsourcing

---

[42] *See id.* at 2–4.

[43] *See id.* at 2.

[44] *See id.* at 3.

[45] *See id.*

[46] *See* BANKING TRANSFORMATION, *supra* note 6, at 187.

[47] *See* FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, *supra* note 40, at 2.

[48] Andrew Reeves, *Is a More Favourable Wind From Regulators Blowing Away Cloud Concerns Among Banks?*, TEMENOS (July 4, 2019), https://www.temenos.com/news/2019/07/04/are-regulators-reducing-cloud-concerns/.

arrangements to a cloud environment – a many to one arrangement. [49] Therefore, certain aspects of regulatory frameworks designed for the traditional outsourcing arrangement will be inapposite. [50]

Undoubtedly, however, cloud computing creates new risks. Cloud service providers are single points of failure. Widespread use of cloud computing introduces multiple sources of systemic risk to financial markets, including their operational centrality to banks and financial institutions, limited substitutability and the related problem of significant service provider pricing leverage, potential market disruptions arising from a crisis of public confidence, and the possibility of widespread data integrity failures.

First, the operational centrality of computing services to banks and financial institutions presents the clearest risk. For example, BoA is migrating 80% of their technology workloads to virtual platforms, utilizing computing infrastructure on the public cloud. [51] Given the modern reality of highly interconnected and tightly coupled market processes, any service disruption, such as a network connectivity breakdown, cybersecurity breach, or data storage failure, will grind BoA's – or any other large bank's – operations to a halt. This risk can be mitigated somewhat by diversifying cloud service providers. Most financial institutions do work with more than one cloud service provider. However, the lion's share of a firm's cloud outsourcing will be with one primary vendor – like Capital One with AWS.

The second source of systemic risk is the lack of cloud computing provider substitutability, especially for the largest institutional clients. In 2017, the Office of Financial Research highlighted how a lack of substitutability for services provided by a handful of firms (central banks, custodian banks, and payment, clearing, settlement, and messaging systems) creates systemic risks because a cyber incident at one of these firms would disrupt the entire financial system. [52]

Cloud service providers strategically offer products to maximize customer lock-in. Software tools are built on top of cloud products,

---

[49] *See* HAL S. SCOTT ET AL., CLOUD COMPUTING IN THE FINANCIAL SECTOR: A GLOBAL PERSPECTIVE, PROGRAM ON INTERNATIONAL FINANCIAL SYSTEMS 30 (July 2019).

[50] *See id.*

[51] *See* Microsoft News Center, *Bank of America Chooses the Microsoft Cloud to Support Digital Transformation*, MICROSOFT (Oct. 2, 2017) https://news.microsoft.com/2017/10/02/bank-of-america-chooses-the-microsoft-cloud-to-support- digital- transformation/.

[52] OFFICE OF FINANCIAL RESEARCH, CYBERSECURITY AND FINANCIAL STABILITY: RISKS AND RELIANCE, U.S. DEP'T TREASURY 3 (Feb. 15, 2017).

creating immense switching costs.[53] As the financial institution's customer-facing applications (also hosted on the cloud) develop in line with evolving business strategies, entrenchment of the computing infrastructure and other supporting services is enhanced. In addition, the advantages of bundling all services with one provider are unavoidable. The complex interplays of hardware, software, servers, and related processes are best synced through a single cloud provider. This leaves financial firms vulnerable to disruptions at their cloud provider. For example, in the case of BoA, even a short-term disruption in its network connection with Microsoft Azure would be highly problematic. And were network problems to become more significant, BoA would not be able to immediately and seamlessly switch to AWS.

The third source of systemic risk is the vulnerability of institutions to a crisis of public confidence in this infrastructure. This concern relates to multiple aspects of cloud computing such as transaction execution, data storage and integrity, and customer interface reliability. A lack of confidence that transactions are being executed efficiently in the cloud or of data accuracy will diminish accurate price discovery for financial products. Alternatively, a decline in public confidence in the security of personally identifiable financial information shared with financial institutions through products supported by cloud service providers will at best decrease consumer interaction with the financial industry and, at worst, create the computing version of a depression-era bank run in the future.

Data integrity is a fourth source of systemic risk. Financial markets require public confidence which cannot be secured without data integrity. The offsite and shared nature of cloud service environments, particularly multi-tenant community or public cloud models, heightens the risk that the underlying data on which financial institutions rely is vulnerable to loss or manipulation. Additionally, many financial market activities occur on a just-in-time basis, raising the stakes of data integrity because of the difficulty of unwinding and rewinding executed transactions.[54] When multiple clients share a common server, significant security technology is deployed to partition the cloud and create secure areas of access for each

---

[53] *See* Eugene Kim, *Amazon's Cloud Sitting on at Least $12.4 Billion of Future Revenue*, CNBC (May 9, 2018) (highlighting the observation of Tom Roderick, an analyst at Stifel Nicalous, that AWS's impressive current and projected financial performance results partly from the sticky nature of their service for enterprise clients).

[54] *See* OFFICE OF FINANCIAL RESEARCH, *supra* note 52, at 3–4.

client that eliminates the risk of each contaminating the other's data facilities. Many current cloud service and cybersecurity regulatory guidelines encourage a variety of data backup processes. Still, tradeoffs exist between rapid data recovery after a crisis and confidence in the completeness, accuracy, and safety of the restored dataset.[55]

The fifth factor contributing to systemic risk is the supplier power wielded by a few dominant cloud service providers. For example, should cloud-service providers disengage from smaller, less lucrative, financial institutions, a large part of the financial system would be vulnerable.[56] In most cloud consumer-provider relationships, data centers; networking; data storage processes; servers; and virtualization occur under the control of the service provider.[57] This creates a risk that customers may not have the appropriate controls to ensure provider-managed components of the cloud service consistently conform to regulatory requirements. However, as noted above, industry participants view provider appreciation of the regulatory environment in which they operate as increasing.

IV. LEGAL AND REGULATORY CONSIDERATIONS

Cloud computing is inherently global. Computing resources and customers inhabit multiple jurisdictions. In general, banking regulators across the globe are charged with maintaining the safety and soundness of regulated institutions and the stability of the financial system. Yet even with this shared objective, they operate in distinct regulatory environments. Indeed, no "single authority for cloud law"[58] exists - not even on a domestic basis in the United States! [59] Ideally, global policymakers would take a coordinated approach to cloud computing. In the meantime, however, international regulatory differences will increase the risks and costs accompanying cloud computing. Global banks and financial institutions will need to wrestle with the regulatory requirements of diverse international regimes in their use of such services. Fortunately, global banks and financial institutions are already familiar with the

---

[55] *See id.* at 4.

[56] *See* FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, *supra* note 40, at 3.

[57] Fratto, *supra* note 13 (citing OFFICE OF FINANCIAL RESEARCH, *supra* note 52, at 4).

[58] *See* Reeves, supra note 48.

[59] BANK OF ENGLAND FINANCIAL STABILITY REPORT 49 (July 2019), https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2019/july-2019.pdf (projected that both the United Kingdom's Prudential Regulation Authority and Financial Policy Committee will release cloud computing publications by the end of 2019).

navigation of such issues. Many financial markets are inherently global. Regulation, however, occurs on a national level (and will for the foreseeable future).

In the U.S., the most directly applicable regulatory guidance for outsourced cloud computing services in the financial sector is outlined in the Federal Reserve's SR Letter 13-19: "Guidance on Managing Outsourcing Risk."[60] This guidance details supervisory expectations for appropriate service provider risk management programs. In 2018, the Federal Reserve Bank of Atlanta published an article that highlights how the SR Letter 13-19 specifically applies to cloud service providers. When it comes to examining the relationship between regulated financial institutions and cloud service providers, the article notes that supervisors will focus on contracts, controls, cybersecurity, disaster recovery, and sound practices. It emphasizes that a bank's risk management program should involve scrutiny "commensurate with the level of risk presented by the outsourcing arrangements."[61]

An important regulatory consideration in the U.S. – and likely also present in other countries – is the need for modernization of legal and regulatory frameworks. Some aspects of traditional regulatory structures for banks and financial institutions are simply inapplicable to cloud environments. One example of this problem would be outdated record keeping rules requiring access to an institution's physical premises to conduct physical audits.[62] Similarly, regulatory requirements addressing cybersecurity, data protection, and bank outsourcing must be appropriate to a cloud context.[63] A 2015 survey of financial services firms found that "regulatory restrictions" and "data security concerns" were key reasons behind their cautious approach to cloud usage.[64] Additional regulatory hindrances exist. They include inconsistent expectations or unclear guidance by regulators, the administrative costs associated with securing such guidance from multiple regulators, a lack of technical knowledge and experience by traditional bank examiners to adequately monitor the risks

[60] *See* FED. RES. SYS., GUIDANCE ON MANAGING OUTSOURCING RISK (Dec. 5, 2013).

[61] *Id.* at 2 (stating "[i]t should focus on outsourced activities that have a substantial impact on a financial institution's financial condition; are critical to the institution's ongoing operations; involve sensitive customer information or new bank products or services; or pose material compliance risk.").

[62] *Banking Transformation, supra* note 6, at 6.

[63] *Id.* at 18.

[64] TREASURY REPORT, *supra* note 6, at 50.

associated with cloud adoption, and certain incompatibilities of traditional legal and regulatory frameworks with cloud services use.[65]

Traditional legal and regulatory frameworks must modernize to track technological developments. Indeed, a 2018 report by the U.S. Treasury recognizes cloud computing as a key technology, facilitating innovation and the competitiveness of U.S. financial institutions.[66] Accordingly, it recommends that "federal financial regulators modernize their requirements and guidance (e.g., vendor oversight) to better provide for appropriate adoption of new technologies such as cloud computing, with the aim of reducing unnecessary barriers to the prudent and informed migration of activities to the cloud."[67] It offers a number of specific recommendations[68] and suggests a related working group of financial regulators be formed.[69]

To facilitate banks' adoption of cloud services, commentators have urged international regulatory coordination and a community-based approach to cloud audits.[70] Alternatives to traditional onsite audits for cloud service providers could also include use of third-party certifications or audit reports, or even the internal audit reports of cloud service providers themselves.[71]

Additionally, cloud service providers also outsource to third parties who, in turn, use cloud computing. This creates potential "chain outsourcing" issues,[72] which should be addressed by regulators.

Finally, financial regulators and government agencies are customers of cloud service providers.[73] As a result, a major disruption or failure of a

---

[65] *See id.*

[66] *Id.* at 52.

[67] *Id.*

[68] *Id.* (discussing recommendations including "formally recognizing independent U.S. audit and security standards that sufficiently meet regulatory expectations; addressing outdated record keeping rules like SEC Rule 17a-4; clarifying how audit requirements may be met; setting clear and appropriately tailored expectations for chain outsourcing; and providing staff examiners appropriate training to implement agency policy on cloud services.").

[69] *Id.*

[70] SCOTT, *supra* note 49, at 2.

[71] *Banking Transformation*, *supra* note 6, at 22.

[72] TREASURY REPORT, *supra* note 6, at 51.; *Banking Transformation*, *supra* note 7, at 21 (noting"[i]n Europe, the EBA's cloud outsourcing recommendations mandate that banks must not only ensure that their CSPs fulfil all regulatory requirements, but that any subcontractors of those CSPs do also. Access and audit rights therefore have to be cascaded down in a CSP chain to any subcontractor – which could include a significant number of entities.").

[73] See Stafford, *supra* note 35, at 1.

cloud provider could be even more consequential than that of most private financial institutions. What would happen if a cloud service provider's operational or security issues impacted a financial regulatory agency's ability to make critical decisions surrounding the distress or failure of a significant financial institution or FMU? Such new and potential risks strongly suggest that these entities might eventually be among the most consequential FMUs.

In sum, even before the Capital One data breach, it was clear that existing regulations governing banks and financial institutions' use of the cloud were inadequate. Cloud computing is a new source of systemic risk, and it should be recognized as such. To this end, the next Part argues that significant cloud service providers should be designated SIFMUs under Title VIII.

V. CLOUD SERVICE PROVIDERS: THE NEW SIFMUS?

Cloud service providers are increasingly critical to the infrastructure of financial markets and, therefore, becoming core FMUs. Indeed, the Bank of England's 2019 Financial Stability Report[74] discusses cloud computing in a section entitled "Developments in Financial Market Infrastructure." In its 2018 Annual Report, the FSOC noted that "[m]aintaining confidence in the security practices of third-party service providers has become increasingly important, particularly because different financial institutions are often serviced by the same providers."[75] In an implicit acknowledgement of the inadequacy of the existing regulatory framework governing cloud services, the FSOC recommended that "Congress pass legislation that ensures that the federal banking agencies, FHFA, and NCUA have adequate examination and enforcement powers to oversee third-party service providers."[76] Designating significant cloud providers as SIFMUs would acknowledge these realties. Additionally, it would require that such entities be highly resilient, have governance and risk management standards congruent with their critical infrastructure role, and prioritize the managing of risk over commercial interests.[77]

The usage of cloud services by banks and financial institutions is likely only to increase. Hence, the risk these providers pose to financial market

[74] BANK OF ENGLAND, *supra* note 10, at 44–48.
[75] FINANCIAL STABILITY OVERSIGHT COUNCIL, ANNUAL REPORT 7 (2019).
[76] *Id.* at 8.
[77] BANK OF ENGLAND, *supra* note 10, at 48.

stability will likewise only escalate. As a single point of failure, a significant cloud service provider's operational disruption would compromise the functioning of firms throughout the economy, including banking and financial institutions. This reality is surely one explanation behind the Federal Reserve examiners' spring 2019 Amazon facility visit. For such reasons, significant cloud service providers should be designated SIFMUs under Dodd-Frank's Title VIII.

A. Title VIII in General

Title VIII, entitled *Payment, Clearing, and Settlement Activities*, is short (a mere 20 pages) but packs a regulatory punch. Its overarching purpose is to "mitigate systemic risk in the financial system and promote financial stability."[78] Towards this objective, it provides the Federal Reserve with authority to promote uniform standards of risk management and conduct for designated SIFMUs and also increased authority to supervise them.

In general, a FMU would be designated as systemically important under Title VIII by the FSOC after a notice and comment period. However, emergency designations are possible. In July 2012, the FSOC designated eight FMUs, five being clearinghouses.[79]

B. Designating Significant Cloud Service Providers Under Title VIII

Dodd-Frank defines a financial market utility to be "any person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person."[80] Undoubtedly, cloud service providers operate multilateral systems. Additionally, their services foundationally enable the transactions undertaken both by other financial institutions and by FMUs such as the Options Clearing Corporation (OCC) already designated as systemically important under Title VIII. The OCC has announced "plans to move its operations into cloud computing"[81] and that part of its risk management

[78] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub L. No. 111-203, § 802(b), 124 Stat. 1376 (2010) [hereinafter Dodd-Frank] (codified at 15 U.S.C. § 780).

[79] See Board of Governors of the Federal Reserve System, Designated Financial Market Utilities (2012) https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm.

[80] *Id.* at § 803(6)(A).

[81] Stafford, *supra* note 35 (noting that other exchanges are also migrating parts of their systems to cloud computing).

platform will operate in a cloud environment.[82] Any disruptions in arrangements such as this would create the ultimate chain outsourcing issue.[83]

"Payment, clearing, or settlement activity" is expansively defined to be "an activity carried out by 1 or more financial institutions to facilitate the completion of financial transaction."[84] Title VIII further defines "financial transaction" to include a number of different types of financial contracts such as funds transfers, swaps, securities, forwards, repurchase agreements, and "any similar transaction that the Council [FSOC] determines to be a financial transaction for purposes of this title."[85] Additionally, it states that "[w]hen conducted with respect to a financial transaction, payment, clearing, and settlement activities may include"[86] a number of activities such as "the calculation and communication of unsettled financial transactions between counterparties,"[87] "the movement of funds,"[88] and "other similar functions that the Council [FSOC] may determine."[89] Given its breadth, cloud service providers certainly fall within Title VIII's definition of a FMU. At a minimum, cloud service providers are multilateral systems whose computing resources are used by financial institutions and FMUs to transfer funds among themselves.

Many of Title VIII's definitions, such as for "financial market utility," "financial institutions," and "payment, clearing and settlement activity," do include exclusions. For example, trading exchanges are generally excluded from the definition of "financial market utility." However, even these exclusions have exclusions. An example of this occurs in the definition of "financial market utility" regarding entities that would generally be excluded from the definition but are not excluded because they perform "critical risk management or processing functions of the financial market utility."[90] One of the authors has argued that such exclusions within

---

[82] *OCC Launches Renaissance Initiative to Modernize Technology Infrastructure*, OPTIONS CLEARING CORP. (Jan. 14, 2019), https://www.theocc.com/about/newsroom/releases/2019/january-14-occ-launches-renaissance-initiative-to-modernize-technology-structure.jsp.

[83] This is because banks and financial institutions are outsourcing derivatives risk to clearinghouses such as the Options Clearing Corporation, who in turn are now outsourcing aspects of their operations and risk management to cloud service providers.

[84] Dodd-Frank, *supra* note 78 at, § 803(7)(A).

[85] *Id.* at § 802(7)(B).

[86] *Id.* at § 802(7)(C).

[87] *Id.* at § 803(7)(C)(i).

[88] *Id.* at § 803(7)(C)(vi).

[89] *Id.* at § 803(7)(C)(viii).

[90] *Id.* at § 803(6)(B)(ii).

exclusions allow for a highly expansive interpretation of which entities ultimately fall within Title VIII's definition of "financial market utility."[91] Hence, although such exclusions do exist, they should not prevent a cloud service provider from falling within Title VIII's definition of "financial market utility."[92]

As with the existing SIFMUs, a disruptive event at a significant cloud service provider would propagate throughout the financial system, causing widespread harm. Title VIII proscribes five factors for the FSOC to evaluate when considering the systemic significance or potential systemic significance of an FMU: (1) the overall monetary amount of the transactions processed by the FMU; (2) the aggregate exposure of the FMU to counterparties; (3) the relationship, interdependencies, or other interactions with other FMUs or payment, clearing, or settlement activities; (4) the effect the FMU's failure would have on critical markets, financial institutions, or the broader financial system; and (5) "any other factors that the Council [FSOC] deems appropriate."[93] By enabling transaction processing and providing network linkages between financial institutions, significant cloud service providers satisfy each of the first four factors. Additionally, the fifth factor provides the FSOC virtually limitless latitude to consider other factors for which there is a reasonable basis for their consideration. Given the expansiveness of this fifth factor, there should be no difficulties were the FSOC to find that significant cloud providers are systemically important now and will only become more so in the future.

C. The Impact of Title VIII Designation for Cloud Providers

Being designated a SIFMU would have significant implications for a cloud service provider, particularly in the areas of governance, risk management, and recovery planning.[94] A SIFMU designation would apply to the legal entity providing cloud services. Thus, AWS, a subsidiary of

---

[91] *See* Baker, *supra* note 12, at 105.

[92] Additionally, in forthcoming research, one of the authors argues that Dodd-Frank's conception of systemic risk is too narrow and, therefore, Title VIII should be expanded to generally include entities such as trading exchanges within the definition of financial market utility because of their systemic significance. Colleen M. Baker, *The Exchange As Systemic Risk Regulator* (working title).

[93] Dodd-Frank., *supra* note 78, at § 804(a)(2)(A)-(E).

[94] *See* Dan Ryan, *Financial Market Utilities: Is the System Safer?*, HARV. LAW SCH. F. ON CORP. GOVERNANCE (Feb. 21, 2015), https://corpgov.law.harvard.edu/2015/02/21/financial-market-utilities-is-the-system-safer/.

Amazon, would receive the SIFMU designation, not the parent company Amazon.

Designating AWS, or another cloud service provider, as a SIFMU would require an overhaul of existing corporate governance arrangements, including ensuring the inclusion of independent directors on its board of directors. In some cases, it might actually require that a board be created. For example, AWS currently has its own CEO, but not a board. The SIFMU cloud provider's "board, senior management, risk managers, and internal audit"[95] would be under enhanced regulatory scrutiny, a tremendous change from the status quo. Its regulator, presumably the Federal Reserve,[96] would evaluate the substantive qualifications of board members to oversee a cloud computing business, and examine management's execution of business strategy and risk management in accord with the board's policies.[97]

A SIFMU designation would also require that cloud service providers establish a Chief Risk Officer position and publish a comprehensive risk management framework.[98] This risk management framework would look very different from the risk management frameworks of current SIFMUs, which are primarily focused on credit and liquidity risks. While these risks are still applicable to cloud service providers, the most relevant risk is operational. The risk management frameworks for designated cloud service providers should emphasize business continuity under a variety of circumstances, including natural disasters and cyber-attacks.

Finally, designated cloud service providers will have to file periodic recovery and wind-down plans with their regulator(s).[99] For current SIFMUs, these plans primarily focus on withstanding one or more member defaults. Cloud service providers have a different business model – current SIFMUs are generally member-owned or part of publicly-traded exchange structures. Therefore, their recovery plans can be expected to focus less on the possibility of financial difficulty at one or more of their customers, and more on how they will continue to serve their customers in the event of a financial or operational disruption.

---

[95] *Id.*

[96] *Id.* (The Federal Reserve is the backup regulator for SIFMUs whose primary regulator is the Securities Exchange Commission or the Commodities Futures Trading Commission. Otherwise, it is the SIFMU's primary regulator).

[97] *Id.*

[98] *Id.*

[99] *Id.*

CONCLUSION

Cloud service providers are fast becoming critical aspects of financial market infrastructure. Their importance, in addition to banks' and financial institutions' reliance on them, will only grow. Hence, cloud computing will increasingly be in the regulatory spotlight, and counted among the most significant risks to financial market stability. Currently, no financial regulatory agency has direct supervisory authority over cloud service providers. This must change. To this end, this article argues that significant cloud service providers as critical financial market infrastructure should be designated by the FSOC as SIFMUs.