MAXINE WATERS, CA
CHAIRWOMAN

United States House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

PATRICK MCHENRY, NC
RANKING MEMBER

October 15, 2019

Memorandum

To: Members, Committee on Financial Services

From: FSC Majority Staff

Subject: October 18, 2019, "AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers."

The Task Force on Artificial Intelligence of the House Financial Services Committee will hold a hearing entitled, "AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers," on October 18 at 9:30 AM a.m. in Room 2128 of the Rayburn House Office Building. This single-panel hearing will have the following witnesses:

- **Ms. Meredith Broussard**, Associate Professor, NYU and Affiliate Faculty Member, NYU Center for Data Science
- **Ms. Alla Seiffert**, Director of Cloud Policy and Counsel at Internet Association
- **Mr. Steve Grobman,** Senior Vice President and Chief Technology Officer, McAfee
- **Dr. Jordan Brandt,** CEO and Cofounder, Inpher
- **Mr. Paul Benda,** Senior Vice President, Risk Cybersecurity Policy, American Bankers Association

Overview

Cloud computing has revolutionized the way entities and consumers store, maintain, and protect data. The "cloud" broadly represents business strategies, technologies (information technology ("IT") and security), and architectures (components and subcomponents required for cloud computing) that permit users to receive information, data, and files on demand from a third-party service provider through the internet. There is no agreed upon definition of the "cloud", but one commonly used by industry and regulators is one from the National Institute of Standards and Technology ("NIST") that defines the cloud 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. [1]Artificial intelligence ("AI") is a component of cloud computing because of its ability to (1) further streamline tasks, moving towards self-managed clouds and (2) improve how data is managed by allowing faster updates and indexing.[2]

[1] National Institute of Standards and Technology, "The NIST Definition of Cloud Computing, Special Publication 800-145", Sept. 2011, at 2-3, at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[2] *See generally,* Laurie A. Harris, CRS "Overview of Artificial Intelligence", Oct. 24, 2017 at https://www.crs.gov/Reports/IF10608.

Initially, the financial services sector was slower to adopt cloud computing as compared to other sectors, but that has changed in recent years.[3] Financial institutions mainly adopt cloud computing because of the benefits found in managing IT, compliance with regulatory requirements, and situations that require high performance computing with low latency (e.g., high frequency trading).[4] Most banks have quickly adopted cloud computing for non-core purposes (i.e., human resources, e-mail, analytics, customer relationship management, and development and testing) but have exercised caution when choosing to migrate core services and activities (i.e., treasury, payments, retail banking, and enterprise data) to the cloud because of their critical nature and the cost of moving legacy systems onto new systems.[5] Yet, even for core functions, many analysts expect large banks to move most, if not all, of their computing needs to cloud platforms within the next five to ten years.[6]

<u>Technology, Terminology, and Implementation</u>

There are several basic technologies that cloud service providers ("CSP") leverage and provide to customers. Within the financial industry, there are four main types of cloud deployments and some entities deploy multiple clouds:

1. *Public Clouds* are a digital environment where the computing resources are available in a shared environment and accessed by multiple customers of the CSP.[7]
2. *Private Clouds* provide computing resources dedicated to a single entity. This is more costly than a public cloud because it can involve large capital expenditures on network hardware, software, and maintenance.[8] Private clouds may be on or off premises and jointly owned by the entity and a third-party.
3. *Community Clouds* are available for use by a specific community of users that have shared needs or concerns, like security, compliance or jurisdiction.[9]
4. *Hybrid Clouds* arrange a mix of deployments that enables quick data movability among different deployments.

Within each deployment are three main service implementations, where some entities implement multiple services and some CSPs offer all three services:

1. *Software-as-a-Service* ("SaaS") provides one or more software applications designed for specific purposes, typically vendor-managed and customizable by users. [10] Some examples include, Slack, Microsoft 365, and Salesforce.
2. *Platform-as-a-Service* ("PaaS") is an application platform software (commonly referred to as middleware because it sits between the CSP and customer) that provides customers flexibility

[3] *See* U.S. Department of Treasury, "A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation", Jul. 2018, at https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf; Filip Blazheski, BBVA Research, "Cloud Banking or Banking in the Clouds?", Apr. 29, 2016, at https://www.bbvaresearch.com/wp-content/uploads/2016/04/Cloud_Banking_or_Banking_in_the_Clouds1.pdf, *see also*, Rachel Dines, "How cloud is transforming manufacturing and financial services in 2019", Jun. 26, 2019, at https://www.cloudcomputing-news.net/news/2019/jun/26/how-cloud-transforming-manufacturing-and-financial-services-2019/.

[4] *See* Depository Trust & Clearing Corporation, "Moving Financial Market Infrastructure to the Cloud", May 2017,at http://perspectives.dtcc.com/media/pdfs/13161-Cloud-WhitePaper-05-11-17.pdf.

[5] *Id.*

[6] *See* U.S. Treasury, *supra* 3; *see also*, Keith Horowitz et al., Citi Research, "U.S. Banks: Transformational Changes Unfolding in Journey to the Cloud" Jan. 10, 2018.

[7] *See* U.S. Treasury, *supra* 3 and NIST *supra* 1.

[8] *Id.*

[9] *Id.*

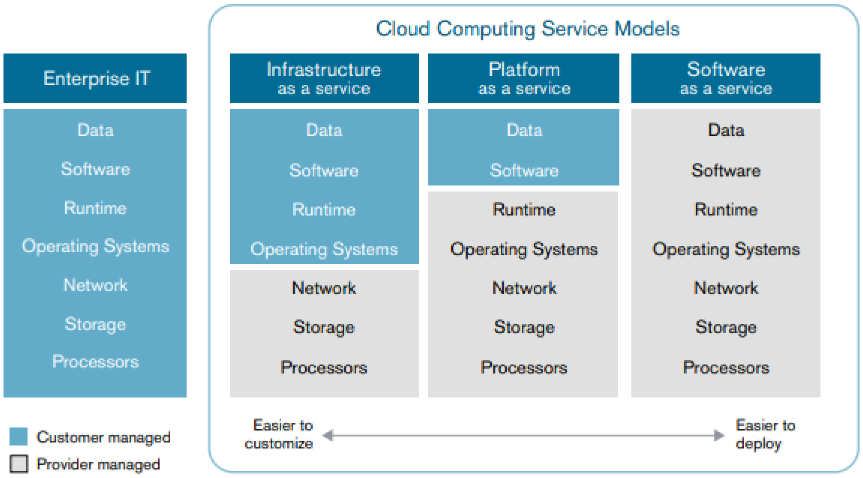
[10] U.S. Department of Transportation, "Uses of Cloud Technology for Geospatial Applications", Nov. 2013, at https://www.gis.fhwa.dot.gov/documents/Cloud_Technologies_for_GIS.htm; *see also* NIST *supra* 1.

to build and deploy custom applications using tools supported by the CSP.[11] Some examples include, Google App Engine, Engine Yard, and Heroku.

3. *Infrastructure-as-a-Service* ("IaaS", pronounced EYE-AS) known as the complete package for competing functionality, includes hardware, software, servers, and networking competing. The customer does not manage or control the underlying cloud but has control over the operating systems.[12] Examples here include: AWS, Azure, and Google Cloud.

Figure 1 below describes how traditional IT Systems compared to cloud computing.

Figure 1. Cloud Computing Contrasted to Traditional IT System[13]



Regulatory Framework for Cloud Providers

As banks deliver more products and services through digital channels and mitigate operational risk, those that lack the in-house expertise to set up and maintain these technologies are increasingly relying upon third-party service providers, including cloud service providers. This has led regulators to scrutinize how banks manage their operational risks.[14] If a bank uses a cloud service to ensure it performs in a safe and sound way, regulators expect the activities performed by the cloud provider to meet the same regulatory requirements as if they were performed by the bank itself.[15] The two main laws currently governing cloud service providers are the Bank Service Company Act ("BSCA")[16] and Gramm-Leach-Bliley Act ("GLBA").[17] The BSCA provides federal depository institution regulators the authority to examine and regulate third-party vendors (includes cloud providers) that provide services to banks. Section 501 of GLBA requires federal agencies to establish appropriate standards for financial institutions to ensure the security and confidentiality of customer information.

However, since the Federal Financial Institution Examination Council's ("FFIEC") July 2012 "Outsourced Cloud Computing Guidance", federal depository institution regulators have provided little

[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *See* Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk*, Jun. 2011, at https://www.bis.org/publ/bcbs195.pdf.
[15] 12 U.S.C. § 1867(c).
[16] P.L.87-856
[17] P.L. 106-102

instruction or further guidance for how financial institutions should deploy or implement cloud service providers.[18] The report noted that it is important to look beyond CSP benefits and still perform a thorough due diligence and risk assessment of cloud providers because storing financial data in the cloud " . . . could increase the frequency and complexity of security incidents."[19] In 2016, federal bank regulators issued an advanced notice of proposed rulemaking on enhanced cyber risk management standards for large banks with more than $50 billion in total assets that would also apply to services provided by third parties to these banks,[20] however the proposal has not been finalized. Additionally, it is unclear to what extent bank regulators have the expertise to examine cloud service providers.[21] Bank regulators may not how to inspect a CSP during an examination, potentially resulting in ineffective supervision. Furthermore, in September, the House approved legislation that enhances the ability of state and federal regulators to at least coordinate when examining a bank's technology service provider, like a cloud company.[22]

Recent reports demonstrate that CSPs, may be hesitant to take on bank clients due to the added supervision and compliance requirements. In April 2019, the Federal Reserve ("Fed") visited Amazon Web Services ("AWS") and it was reported that AWS became wary of the process when Fed examiners asked for documents and information, much like it would during ordinary examinations.[23] AWS "balked" when asked to provide additional information and demanded to first see how the Fed would use, store, and who would access the additional information and for how long.[24] Relatedly, the National Credit Union Administration ("NCUA") does not have authority to examine credit union third party vendors, including CSPs.[25]

Additionally, the Securities and Exchange Commission's ("SEC") Office of Compliance Inspections and Examinations ("OCIE") recently issued a risk alert regarding the use of CSPs by broker-dealers and investor advisers that were using CSPs to store electronic customer records and information based on their recent examinations.[26] The SEC explained in the alert, "Although the majority of these network storage solutions offered encryption, password protection, and other security features designed to prevent unauthorized access, examiners observed that firms did not always use the available security features. Weak or misconfigured security settings on a network storage device could result in unauthorized access to information stored on the device."[27]

[18] *See* Federal Financial Institutions Examination Council, "Outsourced Cloud Computing", Jul. 2012, at https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf.

[19] *Id*.

[20] *See* Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation, "Agencies issue advanced notice of proposed rulemaking on enhanced cyber risk management standards," Oct. 19, 2016, https://www.federalreserve.gov/newsevents/pressreleases/bcreg20161019a.htm

[21] Notably, the federal government has provided CSPs with the Federal Risk and Authorization Management Program ("FedRAMP"). FedRAMP implements standard security baselines and processes to provide both an initial authorization of a cloud service and a mechanism for that security package to be reused across the federal government. *See* FedRAMP, "Cloud Service Providers", at https://www.fedramp.gov/cloud-service-providers/.

[22] The Bank Service Company Examination Coordination Act, H.R. 241 at https://www.congress.gov/116/bills/hr241/BILLS-116hr241rfs.pdf.

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

[24] *Id*.

[25] Elizabeth M. Young LaBerge, "Rumor Has It: NCUA Digging Deeper on Vendor Management", NAFC, Apr. 12, 2019, at https://www.nafcu.org/compliance-blog/rumor-has-it-ncua-digging-deeper-vendor-management.

[26] Office of Compliance Inspections and Examinations, SEC, "Risk Alert: Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features", May 23, 2019, at https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf.

[27] *Id*.

Cyber Security and Privacy, Systemic Risks, and Consumer Protection

As financial institutions migrate to cloud computing and away from proprietary data centers and systems (colloquially known as "on prem"), the operational risks increase, especially without 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 hijackings).[28] To be clear, financial institutions face operational risk whether they operate and maintain cloud services internally or through a third-party CSP. Some argue the risk of system disruptions and failures can be reduced by using a cloud provider, others argue that institutions should manage their own systems to avoid disruptions, and others believe a combination of both is a key strategy for any industry.[29] Thus, as the onus for data and other sensitive information shifts from internal financial institutions operations to external operators, in this instance, the risks become dependent on the activities and events at the CSP.[30] The July 2019 Capitol One security incident illustrates how operational risks are shifting and have the potential of causing harm to consumers and businesses.[31]

Some have expressed concern that cloud service providers could pose risk to the stability of the financial system.[32] This is because of the unique deployment and design of many cloud architectures. Cloud computing resources are pooled, meaning cloud service providers build their resources to service many users all at one time.[33] The concentration of financial institutions across a small number of large CSPs poses new risks. A major security incident at one of the main CSPs could affect several financial institutions simultaneously.[34] Moreover, the cloud services industry is largely concentrated at a few large technology companies. When examining market share, in 2018, it was reported that Amazon (AWS) controlled 48%, Microsoft (Azure) controlled 16%, Alibaba (Ali Cloud) controlled 8%, and Google (Google Cloud) controlled 4%.[35] Furthermore, as data is stored with CSPs and not financial institutions, the ownership of data and corresponding liability questions becomes unclear. For example, if a financial institution or CSP's digital infrastructure is compromised or hacked and consumer data is stolen and misused, does liability fall on the financial institution of the CSP? CSPs could argue that despite physical access to data, they do not own the data, so while it is hosted on their servers, the data is encrypted or otherwise segmented from the CSPs ability to access the contents.[36]

Legislation

- **Strengthening Cybersecurity for Financial Sector Act.** This is a discussion draft that would give the NCUA and FHFA the same oversight of third-party vendors for credit unions, Fannie Mae, Freddie Mac, and FHLBs, that bank regulators have for third-party vendors of banks.[37]

[28] *See* Basel Committee, *supra* note 14.

[29] *See generally*, Sean Peek, "The Pros and Cons of Cloud Storage" U.S Chamber, Sept. 12, 2019, at https://www.uschamber.com/co/run/technology/cloud-storage-pros-and-cons.

[30] European Banking Authority, *EBA Report on the Prudential Risks and Opportunities Arising From Fintech*, July 3, 2018, pp. 50-53.

[31] Emily Flitter and Karen Weise, "Capital One Data Breach Compromises Data of Over 100 Million", NY Times, Jul. 29, 2019, at https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html

[32] For example, *see* David Fratto and Lee Reiners, "A New Source of Systemic Risk: Cloud Service Providers," Duke Law Global Financial Markets Center's FinReg Blog (Aug. 8, 2019), https://sites.duke.edu/thefinregblog/2019/08/08/a-new-source-of-systemic-risk-cloud-service-providers/.

[33] *See* U.S. Treasury, *supra* 3.

[34] *Id*.

[35] Gartner, Inc., "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018" J. 29, 2019, https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-percent-in-2018.

[36] Michael, R. Overly, "Effective Cloud Computing Agreements", Lexis Nexis, last acecesssed Oct. 4, 2019, at https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/posts/drafting-and-negotiating-effective-cloud-computing-agreements.

[37] See GAO, "Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information," July 2, 2015, at https://www.gao.gov/products/GAO-15-509, and FSOC, "Annual Report 2018," pp. 7-8 and 91, at https://home.treasury.gov/system/files/261/FSOC2018AnnualReport.pdf