October 18, 2019

Testimony of

Paul Benda

On Behalf of the

American Bankers Association

before the

Task Force on Artificial Intelligence

of the

House Financial Services Committee

Testimony of

Paul Benda

On behalf of the

American Bankers Association

before the

Task Force on Artificial Technology

of the

House Financial Services Committee

October 18, 2019

The American Bankers Association ("ABA") appreciates the opportunity to provide testimony regarding "AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers." The ABA is the voice of the nation's $17.9 trillion banking industry, which is comprised of small, midsized, regional and large financial institutions. Together, these institutions employ more than 2 million people, safeguard $14 trillion in deposits and extend more than $10 trillion in loans. Our members have a substantial interest in technology, including AI and cloud computing, and we look forward to working with you and the Members of the Taskforce on this very important issue.

Introduction

The rise of cloud computing has led to a digital transformation of many industries, from the entertainment sector where streaming music and movies is now the standard, to email and office applications accessed through a web browser. The rise of a ubiquitous internet connection allows users to download data on demand, access advanced applications and have the computing power needed to run these applications from a mobile phone – essentially the "clouds" that the internet runs on today. There are many reasons that the cloud benefits American businesses. For instance, it allows the outsourcing of expensive computing infrastructure to specialists who can reach critical mass and attain significant economies of scale. The cloud's "pay as you go" model

reduces a company's overhead by allowing it to only pay for the infrastructure that it needs, when it is needed. It also allows a rapid ramp-up in capacity when needed, and enhances operational resilience because cloud operators have more assets and a better ability to provide back-up capabilities. Finally, as cloud capabilities advance, cloud service providers (CSPs) have begun to offer advanced analytic and artificial intelligence tools to their customers to allow them to better understand their data in ways they could never achieve in a cost-efficient manner on their own.

With these benefits, it is no surprise that businesses and governments are looking for a way to migrate certain computing functions to the cloud. While some sectors have fully embraced the cloud, others in highly regulated fields, such as financial services and healthcare, have been more cautious in their approach to adopting the use of the cloud. There are a variety of reasons for this more measured approach, including the fact that in the early days of the development of the cloud there was a lack of confidence by many in the financial industry that CSPs could effectively support the rigorous regulatory requirements and oversight that financial institutions and their vendors must operate within. As the CSPs have matured, financial institutions have begun to explore the cloud. For example, a recent Gartner survey of senior finance executives found that by 2020 about 36 percent of enterprises could be using the cloud to support more than half of their transactions[1]. Today, for many financial institutions the benefits of moving to the cloud are becoming more attractive as CSPs and the financial institutions themselves mature in their ability to mitigate and reduce these risks.

The American Bankers Association (ABA) appreciates the opportunity to share our thoughts on how financial data is stored and protected in the cloud. In particular, we highlight the following four points that we believe are relevant to this discussion:

- **Financial institutions are Responsible for Protecting Their Data**. Title V of the Gramm Leach Bliley Act (GLBA) has long-established standards that requires a financial institution to take meaningful steps designed to ensure the security and confidentiality of its customer's information, regardless of

[1] Gartner survey of senior finance executives from January through March 2017 to explore their technology perspective, influence of IT, needs and priorities in technology investment. https://www.gartner.com/en/newsroom/press-releases/2017-09-13-gartner-says-finance-is-moving-to-the-cloudmuch-faster-than-expected

whether that information is stored or handled by a financial institution or its vendor on the financial institution's own system or in a third-party cloud.

- **The Cloud Offers Benefits, But Risks Must be Managed.** The cloud can provide significant benefits, but risks must be managed consistently and effectively. Use of the cloud should remain an option for all financial institutions, but each financial institution must make a determination as to whether it is the right fit for its organization based on its business model, risk analysis and mitigation strategy and consistent with regulatory requirements.

- **All Parties Should Collaborate to Improve Cloud Security and Efficiency.** Financial Institutions inhabit a unique regulatory space and represent a critical aspect of the American economy. Financial institutions, CSPs and regulators, including core providers that provide products and services to smaller banks, should work in a collaborative manner to ensure that the right frameworks, processes and programs are in place to allow adoption of these new technologies while maintaining the safety and soundness of our financial system.

- **Regulatory Clarity is Important.** From a financial services perspective, the GLBA, Bank Services Company Act (BSCA) and banking agency guidance already provide a robust regulatory framework to oversee bank utilization of the cloud, but additional clarity would be helpful on the roles and responsibilities of regulators with respect to their direct oversight of CSPs.

I. Financial institutions are Responsible for Protecting Their Data

The financial sector believes strongly in protecting sensitive personal and financial information. For hundreds of years, customers have relied on banks to protect their financial information. Because banks are literally at the center of people's financial lives, our industry has long been subject to federal data protection laws and oversight. The GLBA required the federal

regulatory agencies to establish standards for safeguarding customer information. These standards require financial institutions to take meaningful steps that are designed to ensure the security and confidentiality of customer information, protect against anticipated threats to such information, and protect against unauthorized access to, or use of, this information that could result in substantial harm or inconvenience to any customer. Moreover, these standards apply equally regardless of whether that information is stored or handled by a financial institution or its vendor on the financial institution's own system or in a third-party cloud. These standards also require that financial institutions have in place incident response programs to address security incidents involving unauthorized access to customer information, including notifying customers of possible breaches when appropriate.

Compliance by banks with GLBA is regularly examined by the federal banking agencies. Unlike other sectors, where violations of statutory and regulatory restrictions must occur before regulatory oversight is likely to occur, financial institutions are subject to strict regulatory oversight and regular exams regarding their compliance with privacy and data protection laws.

The federal banking agencies have formal procedures that govern bank examinations, particularly surrounding security. For example, this oversight includes the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook, which is an extensive document containing multiple booklets with over 1,000 pages of IT guidance and examination instructions. The Handbook not only provides meaningful guidance to financial institutions regarding the regulatory expectations for, among other things, information security, outsourced technology services and business continuity, but also is used by the regulators to examine banks and assess their compliance.

In 2012, the FFIEC issued cloud guidance, "Outsourced Cloud Computing." The guidance identifies critical areas that financial institutions must consider and assess when using the cloud, including due diligence, vendor management, audit, information security, legal, regulatory and reputational considerations and business continuity planning. Of particular note, the cloud guidance stresses that "[a] financial institution's use of third parties to achieve its strategic plan does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws and regulations."[2] Financial institutions have long been required to maintain

[2] FFIEC "Outsourced Cloud Computing" July 10, 2012 page 2

oversight of their vendors, and the use of CSPs is no different, a point reinforced by the FFIEC guidance.

If a bank fails to comply with the GLBA, including in the context of the cloud, the federal banking agencies can bring enforcement actions to recover significant penalties. Specifically, compliance with Section 501(b) of the GLBA, is enforced by the federal banking agencies under Section 8 of the Federal Deposit Insurance Act ("FDIA"). The federal banking agencies can bring an enforcement action alleging that a failure to comply with the Guidance is an unsafe or unsound practice. In this regard, Section 8 of the FDIA includes various penalties and remedies for an unsafe or unsound practice, including:

- a cease-and-desist order;
- an order requiring that the financial institution correct or remedy any conditions resulting from the unsafe or unsound practice;
- Removal or suspension of financial institution parties from office;
- a civil penalty of $5,000 for each day in which the financial institution violates a cease-and-desist order or order requiring the correction of an unsafe or unsound practice;
- a civil penalty of $25,000 for each day in which the financial institution recklessly engages in an unsafe or unsound practice; and
- up to $1,000,000 or 1 percent of assets for knowingly engaging in an unsafe or unsound practice.

The GLBA mandates that financial institutions protect their customer data. While typical cloud implementations follow a shared responsibility model for data security in which the CSPs have certain responsibilities related to the security of, for example, the physical infrastructure of the relevant cloud, the utilization, deployment, security and administration of such resources

made available by the CSP, however, are ultimately the responsibility of the financial institution using the cloud.

II. The Cloud Offers Benefits but Risks Must be Managed.

The economies of scale, cost reductions, flexibility, scalability, improved load balancing and access to advanced technologies all provide a meaningful business case for financial institutions to consider moving at least some aspects of their operations to the cloud, even if only on a small or limited scale. Additionally, large CSPs have data centers spread over wide geographic regions with resilient data architectures and redundancies in place to provide a high degree of operational resilience that is nearly impossible to match except for the largest financial institutions. Although there are compelling business and operational resilience reasons for financial institutions to consider the use of the cloud, it is critical that financial institutions first put in place strong and effective risk mitigation strategies to address the risks that are unique to the cloud.

The robust regulatory regime in place for financial institutions provides a strong framework for financial institutions to make a balanced risk assessment on whether migrating applications to the cloud makes sense for their computing environment and business model. Utilizing the cloud does not necessarily increase the risks a financial institution may face, but simply changes the nature of the risk. A financial institution is in the business of storing sensitive financial data. This data must be protected regardless of where it may be stored, whether hosted on premise or in a public or private cloud. But while data is stored in physical infrastructure that is managed by a third party, such as the cloud, access and other controls must be tailored to the specific cloud implementation. For institutions that conduct appropriate due diligence on their CSP and take a deliberate approach to securing their cloud environment, there may be no difference in risk from an on premise environment and a cloud-based environment. In many ways, in a cloud environment, overall risks may be reduced due to the operational resilience capabilities and scalable architecture that a CSP can provide in the event of some type of capability failure.

Another advantage that the cloud can provide, especially to smaller institutions, is access to advanced analytic and artificial intelligence tools. These tools can help with security as well as

data analytics. For example, Security Information and Event Management (SIEM) monitoring is necessary to monitor your environment and detect, respond and mitigate security events. The challenge is that the amount of log and other data that is generated can hide unusual or nefarious events in the general noise of operations. Advanced tools exist that are designed to help ensure that high-value alerts are not lost in the noise, but these tools can be prohibitively expensive or difficult to deploy for smaller organizations. One thing that some CSPs provide is access to these types of tools as part of their environment, providing a capability that a smaller institution could not afford or replicate on its own.

It is clear that there are potential benefits and risks of the use of the cloud, but that decision should be left to each individual institution to weigh the risks and benefits of such a migration. If done appropriately, the use of the cloud may have little to no adverse effect on the overall risk profile of a financial institution and would most likely improve the resiliency of the financial institution.

III. All Parties Should Collaborate to Improve Cloud Security and Efficiency

There is strong competition among CSPs to obtain and maintain customers. This competition drives investments in new technologies and helps ensure that marginal costs are minimized. However, we also recognize that financial institutions are entering this dynamic space with regulatory oversight requirements that exceed anything applied to most other cloud customers. This can create challenges and barriers to entry. Larger financial institutions may have a better ability to bargain for contracts and products to meet their regulatory challenges, but it can be especially difficult for smaller financial institutions, that simply do not have enough market share, to work effectively with large CSPs to make changes to, for example, standardized contracts or product offerings. In addition, smaller financial institutions may have difficulty gaining access to the oversight data their regulators require them to obtain for any critical third party.

In many ways, this situation is similar to the issue small institutions face when dealing with the large core banking system providers who provide them the back-end systems that process their daily banking transactions. The smaller institutions have to have access to these services, but have little market leverage individually to pressure adoption of new technologies, or

obtain improved portability of data and services to avoid vendor "lock-in," and little capability to customize contracts. Just as the core providers are necessary to do business, the cloud and the tools available may become increasingly essential to a financial institution's competitiveness. As a result, it is critical that there is further collaboration to ensure that financial institutions of all sizes have the option of utilizing cloud products and services in a way that is consistent with regulatory requirements and expectations.

In the United States, there are some self-generated efforts by financial institutions to aid in improving oversight of third parties, including establishment of companies that work to make shared assessments available. While the companies in this space have different approaches, fundamentally the goal is to create efficiencies by performing a single assessment of a third party provider that is used by multiple financial institutions. One of these companies recently issued a press release touting its risk assessment of Microsoft Cloud Services that meets "the rigorous requirements of financial services customers" and covers the major cloud services that Microsoft provides including Azure and Office365. These types of services have the potential of providing significant help, especially to smaller institutions, to access the data necessary to satisfy the regulatory oversight requirements of critical third party providers and other CSPs should be encouraged to participate in these types of programs.

The progress on gaining access to necessary audit and internal control information is important, but several issues still remain. Importantly, this includes the shared responsibility model that is employed by most CSPs. The baseline shared responsibility model places the responsibility for the cybersecurity of a customer's implementation of a cloud offering entirely upon the customer. This approach may be understandable, but from the ABA's perspective it is our hope that the CSPs work more closely with financial institutions to find ways CSPs could be more proactive in helping secure financial institution cloud deployments. In particular, security controls should be standard and should not be subject to an "opt-in" by the customer. In addition, default security settings should be restrictive versus open and coordination among CSPs in the development of a unified security controls baseline for financial institutions would help ensure appropriate controls are used at the start of any deployment. The use of unified controls would also help financial institutions manage their third parties that utilize the cloud by ensuring that baseline controls are in place for their data and mitigating the risk of security control misconfiguration. CSPs understand their environment better than any single customer

and should have in place mechanisms to notify them of potential misconfigurations or security settings that pose a significant risk to the security of stored data.

Along with improved collaboration on security and notification procedures, we believe there is potential for financial institutions, CSPs and regulators to collaborate on a best practices model to provide standardized terms and conditions that provide financial institutions access to required audit and control data. While many CSPs currently publish attestations to the audits their services have undergone, for financial institutions increased transparency into the business continuity, security incident and breach response, and testing programs would help them comply with their regulatory requirements. Additionally, in the shared services model there are some CSPs that provide different options to customers regarding who manages some security controls. Additional transparency into these options and how the control environment is executed would help financial institutions manage both their risk and those of their third parties who utilize the cloud.

As part of a financial institution's cloud deployment, financial institution regulators have significant authority under the Bank Company Services Act to examine CSPs. Examination of a CSP would be a daunting task and would be exacerbated by the fact that a single CSP could service hundreds, potentially thousands of financial institutions. A potentially more efficient approach would be to establish some standardized parameters that financial institutions, CSPs and regulators could follow to ensure the appropriate contractual terms are in place for financial institutions to perform their due diligence and provide an expedited review process for regulators. This harmonization could provide increased transparency and provide the baseline for engagement with international regulators as CSPs and financial institutions cross multiple jurisdictions worldwide.

The challenges in this space are complex, and we believe that every stakeholder wants to ensure that the security of these critical systems is maintained and at the same time innovation is not hindered. A collaborative approach that merges the best of the safety and soundness culture of financial institutions and regulators with the entrepreneurial spirit of the CSPs is most likely to achieve a lasting outcome that is acceptable to all parties.

IV. Regulatory Clarity is Important

The GLBA and other standards provide an existing robust regulatory framework for financial data that resides in the cloud. Financial institutions are required to ensure any data provided to a third party provider is protected regardless of whether that entity itself is regulated. Whether CSPs should be regulated directly is a reasonable question to ask. But that question should be addressed in a broader context than just financial services. Regardless of potential regulation of CSPs, financial institutions will continue to be responsible for the security of their data, even when that data is handled or stored by vendors. Careful consideration, however, should be taken to ensure that any proposed path forward not impinge upon the ability of CSPs to innovate and offer new tools, nor single out financial services deployments and potentially increase costs or limit access to new or advanced capabilities.

One area worthy of consideration is the applicability of the Bank Services Company Act in the cloud context. Under the BSCA, "a depository institution that is subject to examination by that agency, causes to be performed for itself, by contract or otherwise, any services authorized under this chapter, whether on or off its premises— (1) such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the depository institution itself on its own premises." The services authorized include, "check and deposit sorting and posting, computation and posting of interest, preparation and mailing of checks or statements, and other clerical, bookkeeping, accounting, statistical, or similar functions." We believe that cloud services would be considered services to assist in, for example, bookkeeping and similar functions. As regulators contemplate their role and responsibilities with respect to CSPs, in our view a collaborative approach would benefit all. For instance, it would be helpful to convene discussions with all stakeholders to help maintain the transparency of the financial regulatory oversight process and produce the most efficient outcome for all involved parties. At a minimum, regulators should update their July 2012 guidance on Cloud Computing to more specifically speak to any expectations they have for risk management of CSPs whether already in guidance or more unique to the cloud. In addition, it would be appropriate for the agencies to evaluate the BCSA to determine when CSPs should be included in their oversight and at what level.

Conclusion

The cloud is an exciting innovation that provides many benefits for financial institutions and their customers. At the same time, the unique regulatory environment faced by the financial sector presents certain challenges to CSPs that we believe can be addressed through greater collaboration with CSPs and the financial regulators. As the AI Task Force continues its exploration of these issues, we hope that you will consider the four points we have addressed in this testimony: financial institutions are required to ensure the security and confidentiality of their customer's information, regardless of whether that information is stored on a financial institution system or in a third party cloud; the cloud offers significant benefits but risks must be managed consistently and effectively; financial institutions must determine whether use of the cloud makes sense based on their business model, risk analysis and mitigation strategy and consistent with regulatory requirements; all parties, including core providers, should collaborate to improve cloud security and efficiency; and additional clarity on the roles and responsibilities of regulators with respect to their oversight of CSPs would be helpful.

Thank you for inviting me to testify today and I look forward to your questions.