United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510–6075

September 20, 2019

Frederick S. Humphries
Corporate Vice President for US Government Affairs
Microsoft Corporation
901 K St NW, 11th Floor
Washington, DC 20001

Dear Mr. Humphries:

Organizations are increasingly adopting public cloud technologies that represent significant changes in resource allocation and the provision of products and services across the economy. Capital One's decision to migrate core business and consumer applications to the Amazon cloud is an example within financial services. Still, traditional financial institutions have been slower to public cloud adoption over concerns relating to data security and potential loss from fraud and theft. Given these institutions' unique responsibilities in safeguarding customer information, they are right to take particular care. It is therefore crucial that financial institutions and cloud service providers understand their respective obligations and responsibilities; comply with all applicable laws and regulations related to data security regardless of whether data is stored on the cloud; continuously monitor for, identify and address potential system weaknesses and vulnerabilities; take all measures needed to ensure information is protected and secure from internal and external threats; and work closely and cooperatively with appropriate Federal banking agencies.

The Committee on Banking, Housing, and Urban Affairs would appreciate additional information on these topics to better understand the management of systems, data security, the division of responsibilities between financial institutions and cloud service providers, data security incident response, and federal oversight of these relationships and services.

1. Please clearly describe the respective obligations and responsibilities of a financial institution and Microsoft Azure as it relates to data security in the provision of cloud-based services across different deployment and service models.

2. Please clearly describe the respective obligations and responsibilities of a financial institution and Microsoft Azure as it relates to data security incident response in the provision of cloud-based services across different deployment and service models.

3. Please describe the data security products or services offered by Microsoft Azure to financial institutions, including by differentiating between default and non-default services. Please also describe how particular data security products or services that are available for data stored on Microsoft Azure differ from products or services available for data stored on-premises, and if/how particular data security products or services are specifically tailored to financial institutions.

4. Please describe the following:
    a. how data stored in Microsoft Azure is encrypted or tokenized both at rest and in transit, including delineating those which are default settings across industries and those which must be chosen by a financial institution;
    b. which entity is responsible for encryption across service models;
    c. how encryption keys are stored; and
    d. who has access to encryption keys, and how the use of an encryption key is monitored for privacy and security.

5. Please describe how Microsoft Azure communicates its data security policies and practices, and available data security services and resources, to a financial institution, including any subsequent changes to those policies, practices and/or expectations of service.

6. Please describe what rights a financial institution has to audit Microsoft Azure's operations and data security and risk management policies, procedures, and practices.

7. Describe what authority, if any, a financial institution has to request and receive changes to Microsoft Azure's data operations and data security policies and risk management policies, procedures, or practices, if a financial institution determines it does not meet its data security standards or is not compliant with applicable laws and regulations.

8. Please describe your understanding of the authority Federal financial regulators or other Federal regulators have to oversee the relationship between a financial institution and Microsoft Azure, including to conduct examinations on, collect information from, or take corrective actions against either entity with respect to data security.

9. Please describe the process, including the relative cost and resources (or general difficulty) to: (a) switch from Microsoft Azure to another cloud service provider; and/or (b) move data back from Microsoft Azure to on premises.

Sincerely,

Mike Crapo
Chairman

Sherrod Brown
Ranking Member

United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510–6075

September 20, 2019

Pablo Chavez
Vice President
Google Cloud
25 Massachusetts Ave, NW, Suite 900
Washington, DC 20005

Dear Mr. Chavez:

Organizations are increasingly adopting public cloud technologies that represent significant changes in resource allocation and the provision of products and services across the economy. Capital One's decision to migrate core business and consumer applications to the Amazon cloud is an example within financial services. Still, traditional financial institutions have been slower to public cloud adoption over concerns relating to data security and potential loss from fraud and theft. Given these institutions' unique responsibilities in safeguarding customer information, they are right to take particular care. It is therefore crucial that financial institutions and cloud service providers understand their respective obligations and responsibilities; comply with all applicable laws and regulations related to data security regardless of whether data is stored on the cloud; continuously monitor for, identify and address potential system weaknesses and vulnerabilities; take all measures needed to ensure information is protected and secure from internal and external threats; and work closely and cooperatively with appropriate Federal banking agencies.

The Committee on Banking, Housing, and Urban Affairs would appreciate additional information on these topics to better understand the management of systems, data security, the division of responsibilities between financial institutions and cloud service providers, data security incident response, and federal oversight of these relationships and services.

1. Please clearly describe the respective obligations and responsibilities of a financial institution and Google Cloud Platform (GCP) as it relates to data security in the provision of cloud-based services across different deployment and service models.

2. Please clearly describe the respective obligations and responsibilities of a financial institution and GCP as it relates to data security incident response in the provision of cloud-based services across different deployment and service models.

3. Please describe the data security products or services offered by GCP to financial institutions, including by differentiating between default and non-default services. Please also describe how particular data security products or services that are available for data stored on GCP differ from products or services available for data stored on-premises, and if/how particular data security products or services are specifically tailored to financial institutions.

4. Please describe the following:
    a. how data stored in GCP is encrypted or tokenized both at rest and in transit, including delineating those which are default settings across industries and those which must be chosen by a financial institution;
    b. which entity is responsible for encryption across service models;
    c. how encryption keys are stored; and
    d. who has access to encryption keys, and how the use of an encryption key is monitored for privacy and security.

5. Please describe how GCP communicates its data security policies and practices, and available data security services and resources, to a financial institution, including any subsequent changes to those policies, practices and/or expectations of service.

6. Please describe what rights a financial institution has to audit GCP's operations and data security and risk management policies, procedures, and practices.

7. Describe what authority, if any, a financial institution has to request and receive changes to GCP's data operations and data security policies and risk management policies, procedures, or practices, if a financial institution determines it does not meet its data security standards or is not compliant with applicable laws and regulations.

8. Please describe your understanding of the authority Federal financial regulators or other Federal regulators have to oversee the relationship between a financial institution and GCP, including to conduct examinations on, collect information from, or take corrective actions against either entity with respect to data security.

9. Please describe the process, including the relative cost and resources (or general difficulty) to: (a) switch from GCP to another cloud service provider; and/or (b) move data back from GCP to on premises.

Sincerely,

Mike Crapo
Chairman

Sherrod Brown
Ranking Member

United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510–6075

September 20, 2019

Steve Schmidt
Chief Information Security Officer
Amazon Web Services
12900 Worldgate Dr
Herndon, VA 20170

Dear Mr. Schmidt:

Organizations are increasingly adopting public cloud technologies that represent significant changes in resource allocation and the provision of products and services across the economy. Capital One's decision to migrate core business and consumer applications to the Amazon cloud is an example within financial services. Still, traditional financial institutions have been slower to public cloud adoption over concerns relating to data security and potential loss from fraud and theft. Given these institutions' unique responsibilities in safeguarding customer information, they are right to take particular care. It is therefore crucial that financial institutions and cloud service providers understand their respective obligations and responsibilities; comply with all applicable laws and regulations related to data security regardless of whether data is stored on the cloud; continuously monitor for, identify and address potential system weaknesses and vulnerabilities; take all measures needed to ensure information is protected and secure from internal and external threats; and work closely and cooperatively with appropriate Federal banking agencies.

The Committee on Banking, Housing, and Urban Affairs would appreciate additional information on these topics to better understand the management of systems, data security, the division of responsibilities between financial institutions and cloud service providers, data security incident response, and federal oversight of these relationships and services.

1. Please clearly describe the respective obligations and responsibilities of a financial institution and Amazon Web Services (AWS) as it relates to data security in the provision of cloud-based services across different deployment and service models.

2. Please clearly describe the respective obligations and responsibilities of a financial institution and AWS as it relates to data security incident response in the provision of cloud-based services across different deployment and service models.

3. Please describe the data security products or services offered by AWS to financial institutions, including by differentiating between default and non-default services. Please also describe how particular data security products or services that are available for data stored on AWS differ from products or services available for data stored on-premises, and if/how particular data security products or services are specifically tailored to financial institutions.

4. Please describe the following:
   a. how data stored in AWS is encrypted or tokenized both at rest and in transit, including delineating those which are default settings across industries and those which must be chosen by a financial institution;
   b. which entity is responsible for encryption across service models;
   c. how encryption keys are stored; and
   d. who has access to encryption keys, and how the use of an encryption key is monitored for privacy and security.

5. Please describe how AWS communicates its data security policies and practices, and available data security services and resources, to a financial institution, including any subsequent changes to those policies, practices and/or expectations of service.

6. Please describe what rights a financial institution has to audit AWS operations and data security and risk management policies, procedures, and practices.

7. Describe what authority, if any, a financial institution has to request and receive changes to AWS data operations and data security policies and risk management policies, procedures, or practices, if a financial institution determines it does not meet its data security standards or is not compliant with applicable laws and regulations.

8. Please describe your understanding of the authority Federal financial regulators or other Federal regulators have to oversee the relationship between a financial institution and AWS, including to conduct examinations on, collect information from, or take corrective actions against either entity with respect to data security.

9. Please describe the process, including the relative cost and resources (or general difficulty) to: (a) switch from AWS to another cloud service provider; and/or (b) move data back from AWS to on premises.

Sincerely,

Mike Crapo
Chairman

Sherrod Brown
Ranking Member

United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510–6075

September 20, 2019

Rob Nichols
President and CEO
American Bankers Association
1120 Connecticut Ave NW
Washington, DC 20036

Dear Mr. Nichols:

Organizations are increasingly adopting public cloud technologies that represent significant changes in resource allocation and the provision of products and services across the economy. Capital One's decision to migrate core business and consumer applications to the Amazon cloud is an example within financial services. Still, traditional financial institutions have been slower to public cloud adoption over concerns relating to data security and potential loss from fraud and theft. Given these institutions' unique responsibilities in safeguarding customer information, they are right to take particular care. It is therefore crucial that financial institutions and cloud service providers understand their respective obligations and responsibilities; comply with all applicable laws and regulations related to data security regardless of whether data is stored on the cloud; continuously monitor for, identify and address potential system weaknesses and vulnerabilities; take all measures needed to ensure information is protected and secure from internal and external threats; and work closely and cooperatively with appropriate Federal banking agencies.

The Committee on Banking, Housing, and Urban Affairs would appreciate additional information on these topics to better understand the management of systems, data security, the division of responsibilities between financial institutions and cloud service providers, data security incident response, and federal oversight of these relationships and services.

1. Please clearly describe the respective obligations and responsibilities of a financial institution and a public cloud service provider (CSP) as it relates to data security in the provision of cloud-based services across different deployment and service models.

2. Please clearly describe the respective obligations and responsibilities of a financial institution and a CSP as it relates to data security incident response in the provision of cloud-based services across different deployment and service models.

3. Please describe the data security products or services offered by a CSP to financial institutions, including by differentiating between default and non-default services. Please also describe how particular data security products or services that are available for data stored on the public cloud differ from products or services available for data stored on-premises, and if/how particular data security products or services are specifically tailored to financial institutions.

4. Please describe the following:
    a. how data stored in a public cloud is encrypted or tokenized both at rest and in transit, including delineating those which are default settings across industries and those which must be chosen by a financial institution;
    b. which entity is responsible for encryption across service models;
    c. how encryption keys are stored; and
    d. who has access to encryption keys, and how the use of an encryption key is monitored for privacy and security.

5. Please describe how a CSP communicates its data security policies and practices, and available data security services and resources, to a financial institution, including any subsequent changes to those policies, practices and/or expectations of service.

6. Please describe what rights a financial institution has to audit a CSP's operations and data security and risk management policies, procedures, and practices.

7. Describe what authority, if any, a financial institution has to request and receive changes to a CSP's data operations and data security policies and risk management policies, procedures, or practices, if a financial institution determines it does not meet its data security standards or is not compliant with applicable laws and regulations.

8. Please describe your understanding of the authority Federal financial regulators or other Federal regulators have to oversee the relationship between a financial institution and a CSP, including to conduct examinations on, collect information from, or take corrective actions against either entity with respect to data security.

9. Please describe the process, including the relative cost and resources (or general difficulty) to: (a) switch from one CSP to another; and/or (b) move data back from a CSP to on premises.

Sincerely,

Mike Crapo
Chairman

Sherrod Brown
Ranking Member