Google Cloud Whitepaper
August 2022

United States Gramm-Leach-Bliley Act

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of August 2022 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

At Google Cloud, privacy plays a critical role in the development and operation of our products and services. We've set a high bar for what it means to host, serve, and protect customer data by centering security and data protection at the core of how we design and build our products. We start from the fundamental premise that as a Google Cloud customer, you[1] own your customer data. We implement stringent security measures to help safeguard your customer data and provide you with tools and features to help control it on your terms.

This whitepaper provides information to our customers about the Gramm-Leach-Bliley Act and how Google Cloud uses Google's industry-leading data privacy and security capabilities to help store, process, maintain, and secure customer data[2]. We are committed to partnering with our customers so they can deploy workloads using Google Cloud services and Google Workspace for their productivity needs in a manner that aligns with Gramm-Leach-Bliley Act requirements. We describe our data protection features and outline how they map to its requirements. However, please note that, as a provider of cloud services, we are not in a position to provide you with legal advice - that is something only your legal counsel can provide.

Overview of the U.S. Gramm-Leach-Bliley Act

Title V of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§ 6801 to 6809, regulates how financial institutions collect and share the nonpublic personal information ("NPI") of "consumers," who are individuals who obtain financial services for personal, family, or household use. GLBA requires financial institutions to protect both the privacy and security of NPI.

Whether an entity is a "financial institution" under the GLBA depends on whether it engages in "financial activities" such as lending, insuring, financial advising, issuing or selling asset pool instruments, and underwriting securities. The size of an entity does not determine whether it is subject to GLBA: even a small business can be a regulated financial institution under the law if it engages in financial activities. Financial institutions include entities like banks, mortgage lenders, finance companies, mortgage brokers, account servicers, wire transferors, collection agencies, credit counselors and other financial advisors, tax preparation firms, credit unions, investment advisors, lenders (including universities who provide financial aid), check cashers, wire transfer services, and sellers of money orders.

GLBA applies to the NPI collected by financial institutions. Personally identifiable financial information collected by a financial institution is NPI if it is not publicly available. Personally identifiable financial information is defined in the GLBA's implementing regulations as any information (1) provided by the consumer to obtain a financial product or service from a financial institution; (2) about a consumer resulting from any transaction involving a financial product or service between the institution and the consumer; or (3) otherwise obtained about a consumer in connection with providing a financial product or service to the consumer. Information derived in whole or in part from NPI, such as a list of

[1] In this whitepaper, "you/your" refers to Google Cloud and Google Workspace customers as well as Google Cloud partners. Unless indicated otherwise, references to "customers" will include Google Cloud partners and references to "customer data" will include Google Cloud partner data.
[2] In this whitepaper "customer data" and "your data" refers to the customer data we process according to your Google Cloud agreement(s).

consumers' names and addresses that was derived using information such as account numbers, also may be NPI.

The GLBA is implemented by two sets of regulations. Regulations implementing the privacy provisions of the GLBA (referred to herein as "Privacy Rules")[3] require financial institutions to provide consumers with privacy notices that describe the types of NPI they collect and the types of affiliates and nonaffiliated third parties to which they may disclose NPI. The Privacy Rules also only permit the sharing of a consumer's NPI with third parties if the financial institution offers the consumer the ability to opt out from that sharing, subject to certain exceptions.[4]

Regulations implementing the data security provisions of the GLBA (referred to herein as "Safeguards Rules") require financial institutions to implement administrative, technical, and physical measures to adequately protect the security of NPI.[5] Various Federal financial regulators, as well as state insurance authorities, have issued Safeguards Rules. While these rules are similar in many respects, there are some meaningful differences across the regulations, summarized below in this white paper.

Federal banking agencies, state insurance authorities, the SEC, and the FTC each have GLBA enforcement authority over financial institutions subject to those agencies' respective jurisdictions. The agencies also have a variety of enforcement capabilities. For example, the CFPB has authority to issue cease and desist orders; commence administrative proceedings; bring suit, including for injunctive relief; seek civil monetary penalties that escalate according to culpability levels; and refer matters to the U.S. Department of Justice for criminal proceedings. There is no private right of action for consumers under the GLBA.

This Whitepaper generally discusses the requirements of the CFPB's privacy regulations, Regulation P, and the FTC's security regulations, the Safeguards Rule. However, the rules and regulations that

---

[3] The term "Privacy Rules" refers to the regulations issued by the Federal financial regulators to implement the privacy provisions of the GLBA. With respect to those provisions, the Consumer Financial Protection Bureau ("CFPB") and Securities and Exchange Commission ("SEC") have general rulemaking authority, and those regulators issued Regulation P, 12 C.F.R. Part 1016, and Regulation S-P, 17 C.F.R. Part 248, respectively. In addition, the Commodity Futures Trading Commission ("CFTC") has authority to prescribe regulations for entities subject to its jurisdiction, and the Federal Trade Commission ("FTC") has rulemaking authority with respect to auto dealers. Those regulators have issued privacy rules at 17 C.F.R. Part 248 and the Privacy Rule, 16 C.F.R. Part 313, respectively.

[4] For example, under the CFPB's version of the Safeguards Rule, Regulation P, opt-out rights do not attach when the institution discloses NPI to non-affiliates to administer, process, or enforce a transaction that a customer requests or authorizes; with the consent or at the direction of the consumer; to protect the confidentiality or security of records pertaining to the consumer, service, product, or transaction; and in certain other circumstances. *See* 12 C.F.R. §§ 1016.14-1016.15.

[5] The term "Safeguards Rules" refers to the regulations issued by the Federal financial regulators to implement the data security provisions of the GLBA. With respect to those provisions, the Federal Reserve Board ("FRB"), Federal Deposit Insurance Corporation ("FDIC"), and Office of the Comptroller of the Currency ("OCC") have jointly issued regulations titled "Interagency Guidelines Establishing Information Security Standards." The CFTC sets customer data protection standards in 17 C.F.R. § 160.30 and in guidance documents, and the SEC issued regulations implementing the Safeguards Rule in 17 C.F.R. § 248.30. The FTC has rulemaking authority for all entities not subject to the jurisdiction of other Federal financial regulators and has issued its Safeguards Rule at 16 C.F.R. Part 314, amended in 2021.

ultimately will govern an entity in any particular situation is a fact-specific determination. You should confirm with your legal counsel which laws may apply to you, including state laws.[6]

Google Cloud data protection overview & the Shared Responsibility Model

Google Cloud's robust security and privacy controls can give customers the confidence to utilize Google Cloud services and Google Workspace in a manner aligned with the requirements of the U.S. Gramm-Leach-Bliley Act. Moreover, we are constantly working to expand our privacy and security capabilities. To help customers with compliance and reporting, Google shares information and best practices, and provides easy access to documentation. In this section, we describe our comprehensive data protection and privacy capabilities and our robust data security features most relevant to the PDPA. We then explain how we share security and compliance responsibilities according to the Shared Responsibility Model.

Google Cloud's approach to security and data protection

Google's focus on security and protection of information is among our primary design criteria. Security is at the core of everything we do; it is embedded in our culture and our architecture, and we focus on improving it every day. In this section, we provide an overview of the organizational and technical controls we use to protect your data. To learn more about our approach to security and compliance, refer to the Google security whitepaper for Google Cloud services and the Google Workspace Security whitepaper.

Topics

Google Cloud's approach to data protection and privacy
- Data privacy trust principles
- Dedicated privacy team
- Data access and customer control
- Restricted access to customer data
- Law enforcement data requests

Google Cloud's approach to data security
- Strong security culture
- Security team
- Trusted infrastructure
- Infrastructure redundancy
- State-of-the-art data center security
- Data encryption
- Cloud-native technology
- The Shared Responsibility Model

[6] *E.g.*, the California Information Privacy Act, Cal. Fin. Code § 4050 et seq.

Google Cloud's approach to data protection and privacy

Data protection and privacy are fundamental to Google. We design our products and services from the start with privacy and trust as guiding principles. Google Cloud works to help ensure the protection and privacy of customers' data in three ways: 1) we provide superior data protection through a secure core infrastructure that is designed, built, and operated to help prevent threats; 2) we give customers robust security controls to help them meet policy, regulatory, and business objectives; and 3) we work to fulfill our compliance responsibilities and to make compliance easier for our customers.

Data protection and privacy trust principles

We want our customers to feel confident when using Google Cloud and Google Workspace products. We believe that trust is created through transparency, and we want to be open about our commitments and offerings to our customers when it comes to protecting their data in the cloud.

Our commitments to you about your data

Your data is critical to your business, and you take great care to keep it safe and under your control. We want you to feel confident that taking advantage of Google Workspace and Google Cloud services doesn't require you to compromise on security or control of your business's data.

At Google Cloud, we believe that trust is created through transparency, and we want to be transparent about our commitments and what you can expect when it comes to our shared responsibility for protecting and managing your data in the cloud.

When you use Google Workspace or Google Cloud services, you can:

1. **Know that your security comes first in everything we do.**
   We promptly notify you if we detect a breach of security that compromises your data.
2. **Control what happens to your data.**
   We process customer data according to your instructions. You can access it or take it out at any time.
3. **Know that customer data is not used for advertising.**
   We do not process your customer data to create ads profiles or improve Google Ads products.
4. **Know where Google stores your data and rely on it being available when you need it.**
   We publish the locations of our Google data centers; they are highly available, resilient, and secure.
5. **Depend on Google's independently-verified security practices.**
   Our adherence to recognized international security and privacy standards is certified and validated by independent auditors — wherever your data is located in Google Cloud.
6. **Trust that we never give any government entity "backdoor" access to your data or to our servers storing your data.**

> We reject government requests that are invalid, and we publish a transparency report for government requests.
>
> To learn more about our commitments to safeguarding customer information, refer to the Google Cloud Privacy page. See data processing terms for Google Workspace and Google Cloud.

Dedicated privacy team

The Google privacy team operates separately from product development and security organizations, but participates in Google product launches by reviewing design documentation and performing code reviews to help ensure that privacy requirements are followed. They help release products that reflect strong privacy practices: transparent collection of user data, providing users and administrators with meaningful privacy configuration options, and continuing to be good stewards of information stored on our platform. To learn more about our privacy team, refer to the privacy team section of the Google security whitepaper for Google Cloud services and the Google Workspace Security whitepaper.

Data access and customer control

Google Cloud customers own their data, not Google. Google will only process customer data in accordance with contractual obligations. We also provide customers with solutions that allow granular control of resource permissions. For example, using Cloud Identity and Access Management, customers can map job functions to groups and roles so users only access the data they need to get the job done. Furthermore, customers may delete customer data from our systems or take it with them if they choose to stop using our services.

Restricted access to customer data

To keep data private and secure, Google logically isolates each customer's data from that of other customers and users, even when the data is stored on the same physical server. Only a small group of Google employees has access to customer data pursuant to explicit reasons based on job function and role. Any additional access is granted according to stringent procedures and tracked through audit records which are available in near real-time via Access Transparency.

Google Cloud's approach to data security

In this section, we provide an overview of the organizational and technical controls that we use to protect your data at Google Cloud. Please refer to Google security whitepaper, and Google Workspace Security whitepaper for additional information on our security practices.

Strong security culture

Security is central to Google culture. It is reinforced in employee security training and company-wide events to raise awareness and drive innovation in security and privacy.

To learn more about our security culture, refer to the security culture sections in our Google security whitepaper and our Google Workspace Security whitepaper.

Security team

Google employs more than 850 security professionals, including some of the world's foremost experts. This team maintains the company's defense systems, develops security review processes, builds security infrastructure, implements Google's security policies, and actively scans for security threats. Our team also takes part in research and outreach activities to protect the wider community of Internet users, beyond just those who choose Google solutions. Our research papers are available to the public. As part of our outreach efforts, we have a team known as Project Zero that aims to prevent targeted attacks by reporting bugs to software vendors.

In addition, our security team works 24/7 to quickly detect and resolve potential security incidents. Our security incident management program is structured around industry best practices and tailored into our "Incident Management at Google (IMAG)" program, which is built around the unique aspects of Google and its infrastructure. We also test our incident response plans regularly, so that we always remain prepared.

To learn more, refer to the security team, vulnerability management, and monitoring sections in the Google security whitepaper. In addition, refer to the security team, vulnerability management, and monitoring sections in the Google Workspace Security whitepaper.

Trusted infrastructure

We conceived, designed, and built Google Cloud to operate securely. Google is an innovator in hardware, software, network, and system management technologies. We custom design our servers, proprietary operating system, and geographically distributed data centers. Using "defense in depth" principles, we have created an IT infrastructure that is generally more secure and easier to manage than most other deployment options. Our infrastructure can provide secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the Internet, and safe operation by administrators. We maintain the security of this infrastructure in progressive layers, starting from the physical security of our data centers, building with underlying security-designed hardware and software, continuing with secure service deployment, secure data storage, and secure internet communication, and finally, operating the infrastructure in a secure fashion.

To learn more, refer to the Google Cloud Infrastructure Security Design Overview, as well as the Google Cloud Data Processing and Security Terms, Appendix 2: Security Measures and Google Workspace Data Processing Amendment, Appendix 2: Security Measures.

Infrastructure redundancy

Google's infrastructure components are designed to be highly redundant. This redundancy applies to server design and deployment, data storage, network and Internet connectivity, and the software services themselves. This "redundancy of everything" creates a robust solution that is not dependent on a single server, data center, or network connection. Our data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as natural disasters and local

outages. In the event of hardware, software, or network failure, platform services and control planes are capable of automatically changing configuration so that customers can continue to work without interruption. Our highly redundant infrastructure also helps customers protect themselves from data loss. Customers can create and deploy our cloud-based resources across multiple regions and zones, allowing them to build resilient and highly available systems. To learn more, refer to the low latency and highly available solution in the Google security whitepaper and the Google Workspace Security whitepaper.

State-of-the-art data center security

Google data centers feature layers of physical security protections. We limit access to these data centers to only a very small fraction of employees and have multiple physical security controls to protect our data center floors such as biometric identification, metal detection, vehicle barriers, and custom-designed electronic access cards. We monitor our data centers 24/7/365 to detect and track intruders. Data centers are routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more, refer to our Data Center Innovation page.

Data encryption

Google encrypts data at rest and encrypts data in transit, by default. The type of encryption used depends on the OSI layer, the type of service, and the physical infrastructure component. By default, we encrypt and authenticate data in transit at one or more network layers when data moves outside physical boundaries not controlled by or on behalf of Google. To learn more, refer to the Encryption in Transit in Google Cloud whitepaper.

Cloud-native technology

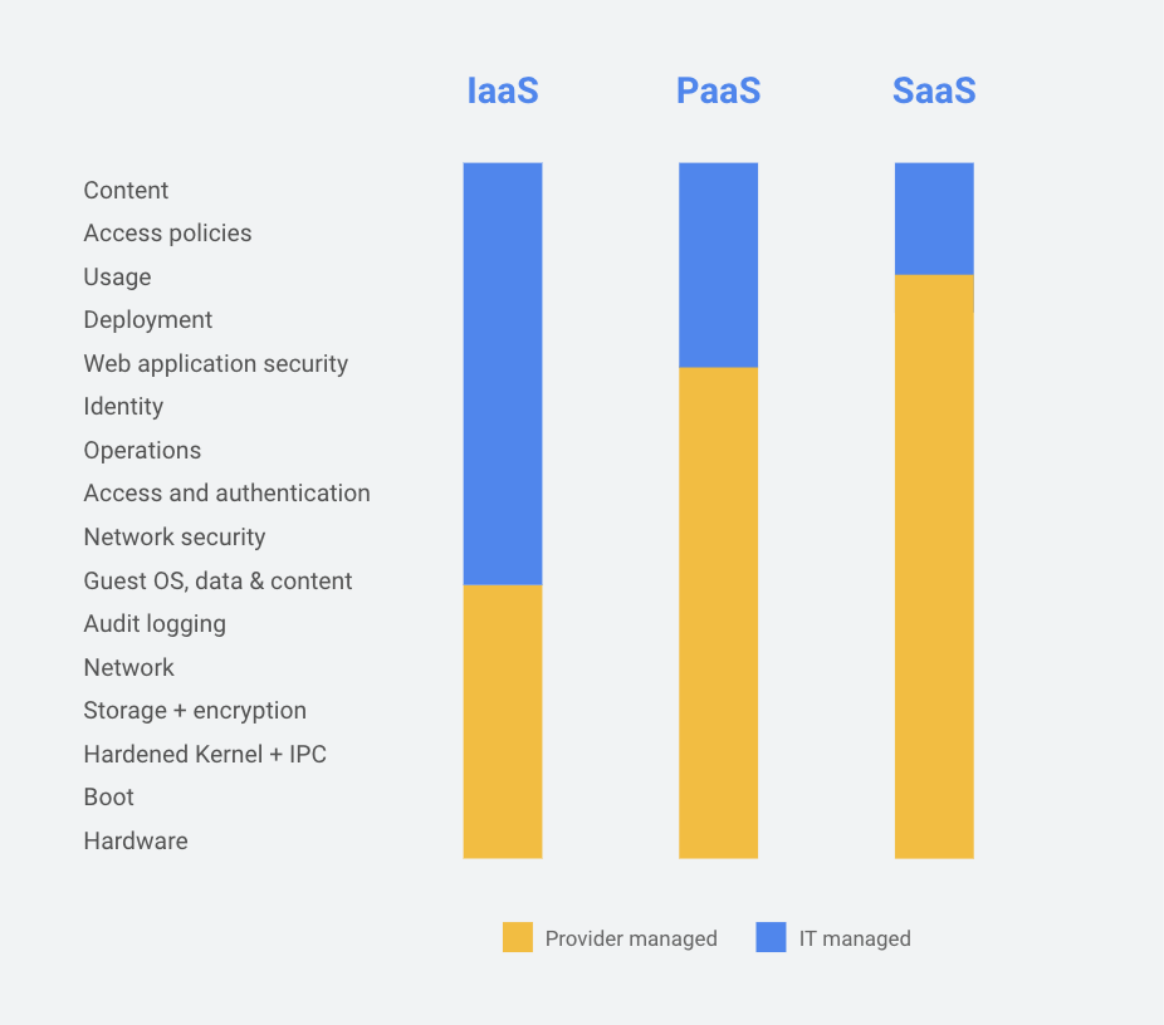
We continue to invest heavily in security, both in the design of new features and the development of cutting-edge tools so customers can more securely manage their environments. Some examples are the Cloud Security Command Center for Google Cloud and the Security Center for Google Workspace that bring actionable insights to security teams by providing security analytics and best practice recommendations from Google, and VPC Service Controls, which help to establish virtual security perimeters for sensitive data. To learn more about our security technologies, refer to our security products & capabilities page.

The Shared Responsibility Model

Under our Shared Responsibility Model, the cloud customer and its CSP share the responsibilities of managing the IT environment, including those related to security and compliance. As a trusted partner, Google Cloud's role in this model includes providing services on a highly secure and controlled platform and offering a wide array of security features from which customers can benefit. Shared responsibility enables our customers to allocate resources more effectively to their core competencies and concentrate on what they do best. The shared responsibility model does not remove the accountability and risk from customers using Google Cloud services, but it does help relieve the burden as we manage and control system components and physical control of facilities. It also shifts a portion of the cost of security and compliance onto Google Cloud and away from our customers. The figure below visually demonstrates an example of the shared responsibility model across on-prem,

infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings. Keep in mind that responsibilities will vary depending on the specific services being used.

For more information on Google Cloud product and security configurations, customers should reference the applicable product documentation.



How Google Cloud helps customers meet the requirements of the GLBA

Data Protection Obligations	How Google Supports GLBA Requirements
Collection, use, and disclosure of personal information	
Notice of Collection ● Financial institutions must issue a clear and conspicuous initial privacy notice that accurately reflects the institution's privacy policies to customers. ○ This notice must be issued no later than the time the customer relationship starts, unless an exception applies. ○ Privacy notices must contain certain disclosures, including the categories of NPI collected and shared, the categories of third parties with which NPI is shared, and the purposes for which NPI is shared. ○ Furthermore, the privacy notices must set forth the consumer's right to opt out of certain types of disclosures of NPI. ● Financial institutions must also issue annual privacy notices, which have the same form and content as the initial privacy notices, to customers under certain circumstances.	Customer Responsibility: ● Ensure the personal information is collected in a lawful manner. ● Customers must also make disclosures about how they collect and process personal information. Google Cloud Commentary: ● Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms.
Purpose Limitation ● Financial institutions must describe the categories of NPI that they collect and the purposes for which they disclose NPI to third parties in their privacy notices. ● Recipients of NPI must only use the NPI for certain specified purposes, unless consumers are given notice and the right to opt out of the disclosure of their NPI.	Customer Responsibility: ● Ensure collection, use, or disclosure of personal information is limited to the lawful purposes specified. Google Cloud Commentary: ● Google gives you control to decide what information to put into the services and which services to use, how to use them, and for what purpose. ● Google commits to only access or use your data to provide the services ordered by you and in accordance with the

	contract terms. Google will not use your data for any other products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.
Source ● Financial institutions must describe how they collect the NPI of consumers, including whether they collect information from other companies such as credit bureaus.	Customer Responsibility: ● Customers should make all reasonable efforts to collect information directly from the individual, unless certain circumstances apply. Google Cloud Commentary: ● Google gives you control to decide which Services to use, how to use them, and what information to collect.
Personal Information/Data Use ● Financial institutions must disclose how they collect and disclose NPI in their privacy notices. ● Recipients of NPI must only use the NPI for certain specified purposes, unless consumers are given notice and the right to opt out of the disclosure of their NPI.	Customer Responsibility: ● Ensure collection, use, or disclosure of personal information is lawful and is accurately reflected in privacy notices. Google Cloud Commentary: ● Google gives you control to decide what information/data to put into the services and which services to use, how to use them, and for what purpose. ● Google commits to only access or use your data to provide the services ordered by you and in accordance with the contract terms. Google will not use it for any other products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.
Personal Information/Data Disclosure ● A financial institution generally may not disclose NPI to affiliates unless it provides prior notice to the consumer. Consumers must also be given the ability to opt out of disclosures of their NPI to affiliates for marketing purposes or disclosures of creditworthiness information to affiliates. ● A financial institution may not make a nonexempt disclosure of NPI to a nonaffiliated third party unless it satisfies the following requirements: ○ (1) It has provided the consumer with an initial privacy notice;	Customer Responsibility: ● Develop a disclosure handling process. Google Cloud Commentary: ● Google Cloud makes robust confidentiality, data protection, and security commitments in our contracts. ● Google commits to processing your data to provide the services ordered by you and in accordance with the contract terms. Google will not use it for any other products or to serve advertising. Refer to the Data Usage section of the Google Security whitepaper.

○ (2) It has provided the consumer with the ability to opt out of such disclosures; ○ (3) It has given the consumer a reasonable opportunity to opt out; and ○ (4) The consumer has not opted out. ● Some exceptions apply to the opt-out requirement, including for disclosures of NPI to service providers. ○ The service provider exception applies to the extent that the financial institution provides a privacy notice to the consumer and enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the NPI was disclosed.	
Accountability	
Privacy impact assessments/Risk assessments ● Although the GLBA does not require privacy risk assessments, the Safeguards Rules require that a financial institution base its information security program on a written risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks. ● The risk assessments must meet certain criteria set forth in the Safeguards Rules, including, for example, criteria for the evaluation and categorization of identified security risks, and criteria for the assessment of the confidentiality, integrity, and availability of information systems and customer information, and should be conducted periodically.	Customer Responsibility: ● If you are a public institution you conduct a risk assessment, if required. Google Cloud Commentary: ● Google Cloud recognizes that you need certain information in order to conduct a risk assessment. Our data processing agreements for Google Workspace and Google Cloud services clearly articulate our privacy and security commitment to customers. ● In addition, you can review Google's current certifications and audit reports via See Cloud's compliance reports.

Requests to restrict processing of personal information; Requests to delete personal information ● As noted above, a financial institution must provide consumers with the ability to opt out of the disclosure of their NPI to nonaffiliated third parties. ● Financial institutions must comply with a consumer's request to opt out of these disclosures as soon as reasonably practicable after the institution receives it, and must take affirmative steps to effectuate such opt-outs.	Customer Responsibility: ● If you wish to stop using our services, you can do so at any time. ● Where required, delete personal information in response to requests from data subjects. Google Cloud Commentary: ● Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data. You can use the following functionality of Google Cloud services: ○ Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources. ○ Admin Console: A web-based graphical user interface that customers can use to manage their Google Workspace resources. ○ gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud. A command-line interface is a user interface to a computer's operating system. ○ Google APIs: Application programming interfaces which provide access to Google Cloud.
Annual Security Reporting ● Some versions of the Safeguards Rules, such as the Interagency Guidelines Establishing Information Security Standards may require internal reporting, such as a requirement to report at least annually to the board of directors or an appropriate committee of the board.	Customer Responsibility: ● Customers are responsible for satisfying their annual security reporting obligations. Google Cloud Commentary: ● Google recognizes that to effectively manage your use of the services you need sufficient information about the services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the services on an ongoing basis. ● Google will make information about developments (including security incidents) that materially impact Google's

	ability to perform the services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard for Google Cloud and the Status Dashboard for Google Workspace. • In addition, Google Cloud will notify you of data incidents promptly and without undue delay. More information on Google Cloud's data incident response process is available in our Data incident response whitepaper.
Privacy & Security Program • The Safeguards Rules outline particular security obligations for financial institutions.The FTC's Safeguards Rule, for example, requires, among other obligations, that covered financial institutions develop, implement, and maintain a written information security program with administrative, technical, and physical safeguards designed to protect customer information. See here for guidance from the FTC regarding the Rule. • In designing the information security program, the Safeguards Rule requires financial institutions to: ○ Implement and periodically review access controls; ○ Identify and manage the data, personnel, devices, systems, and facilities that enable the institution to achieve business purposes; ○ Encrypt customer information on systems and when it's in transit; ○ Adopt secure development practices for in-house developed applications used to transmit,	Customer Responsibility: • Customers should implement sufficient security controls to protect the personal information including proper configuration of features in the cloud under customer management. Google Commentary: (1) Security of Google's infrastructure Google manages the security of our infrastructure (ie., the hardware, software, networking and facilities that support the services). Google provides detailed information to customers about our security practices at: • Our infrastructure security page • Our security whitepaper • Our cloud-native security whitepaper • Our infrastructure security design overview page • Our security resources page • Our Cloud compliance page (2) Security of your data and applications in the cloud (a) Security by default • Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from

access, or store customer information, as well as procedures to evaluate, assess, or test the security of externally developed applications; ○ Implement multi-factor authentication for anyone accessing customer information on the entity's system; ○ Dispose of customer information securely; ○ Anticipate and evaluate changes to information systems or networks; and ○ Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.	you. More information is available on the Google Cloud Encryption at rest page. ● Encryption in transit. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products Information on Google's security products is available on our Cloud Security Products page. The below illustrative list of Google Cloud and Google Workspace services may be used to help with your storage and security requirements: **Access control** 2-Step Verification ● 2-Step Verification puts an extra barrier between customer's business and cybercriminals who try to steal usernames and passwords to access business data. With 2-Step Verification, customer's users sign in to their account in two steps with something they know (their password) and something they have (their mobile phone with Google OTP installed) Identity and Access Management (IAM) ● Identity and Access Management (IAM) can be used to assign roles and permissions to administrative groups, incorporating principles of least privilege and separation of duties. VPC Service Controls ● VPC Service Controls allow customers to address threats such as data theft, accidental data loss, and excessive access to data stored in Google Cloud multi-tenant services. It enables clients to

	tightly control what entities can access what services in order to reduce both intentional and unintentional losses. ● VPC Service Controls delivers zero-trust style access to multi-tenant services. Clients can restrict access to authorized IPs, client context, and device parameters while connecting to multi-tenant services from the internet and other services. Examples include GKE, BigQuery, etc. It enables clients to keep their entire data processing pipeline private. **Access Log** Cloud Logging ● Cloud Logging is a fully managed service that allows you to store, search, analyze, monitor, and alert on logging data and events from Google Cloud and Amazon Web Services. You can collect logging data from over 150 common application components, on-premises systems, and hybrid cloud systems. Access Transparency ● Access Transparency Maintain visibility of insider access to your data through near real-time logs from Access Transparency. **Protection from External Threats** Cloud Security Command Center ● Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security posture by evaluating your security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities, and threats; and helping you mitigate and remediate risks. Virtual Machine Threat Detection

	• Virtual Machine Threat Detection, a built-in service of Security Command Center Premium, provides threat detection through hypervisor-level instrumentation. **Monitoring** • The Google Cloud Status Dashboard provides status information on the services. • The Google Workspace Status Dashboard provides status information on the services. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. • Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases • Security blueprints
Care of Personal Information	
Data Breach Notification • Neither GLBA itself nor FTC regulations currently require data breach notification. • However, the Interagency Guidelines Establishing Information Security Standards set forth the supervisory expectation that a banking organization notify its primary federal regulator "as soon as possible" if the organization becomes aware of an incident involving unauthorized access to, or use of, sensitive customer information.	Customer Responsibility: • Customers should develop policies and procedures for effectively addressing and responding to data breaches. Google Cloud Commentary: • Google recognizes that to effectively manage your use of the services, including handling potential data breaches, you need sufficient information about the services on a regular basis. We provide a number of mechanisms to

	assist you to effectively oversee the services on an ongoing basis. • Google will make information about developments that materially impact Google's ability to perform the services in accordance with the SLAs available to you. More information is available at our Incidents & the Google Cloud dashboard for Google Cloud and the Status Dashboard for Google Workspace. • Google will also notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper. • Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents. Refer to our Data incident response whitepaper for more information.
Storage and Security • Financial institutions also have a duty to oversee their service providers. • Financial institutions must also regularly monitor and test the effectiveness of their safeguards, appropriately train staff regarding the safeguards, keep their information security plan up to date, create a written incident response plan, and designate a Qualified Individual to implement and supervise the information security program and report regularly to the Board of Directors.	Customer Responsibility: • Customers should implement sufficient security controls to protect the personal information including proper configuration of features in the cloud under customer management. Google Commentary: (1) Security of Google's infrastructure Google manages the security of our infrastructure (ie., the hardware, software, networking, and facilities that support the services). Google provides detailed information to customers about our security practices at: • Our infrastructure security page • Our security whitepaper • Our cloud-native security whitepaper • Our infrastructure security design overview page • Our security resources page • Our Cloud compliance page

	(2) Security of your data and applications in the cloud (a) Security by default ● Encryption at rest. Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. ● Encryption in transit. Google encrypts and authenticates data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. (b) Security products Information on Google's security products is available on our Cloud Security Products page. The below illustrative list of Google Cloud and Google Workspace services may be used to help with your storage and security requirements: **Access control** 2-Step Verification ● 2-Step Verification puts an extra barrier between customer's business and cybercriminals who try to steal usernames and passwords to access business data. With 2-Step Verification, customer's users sign in to their account in two steps with something they know (their password) and something they have (their mobile phone with Google OTP installed) Identity and Access Management (IAM) ● Identity and Access Management (IAM) can be used to assign roles and permissions to administrative groups, incorporating principles of least privilege and separation of duties.

	[VPC Service Controls] • VPC Service Controls allow customers to address threats such as data theft, accidental data loss, and excessive access to data stored in Google Cloud multi-tenant services. It enables clients to tightly control what entities can access what services in order to reduce both intentional and unintentional losses. • VPC Service Controls delivers zero-trust style access to multi-tenant services. Clients can restrict access to authorized IPs, client context, and device parameters while connecting to multi-tenant services from the internet and other services. Examples include GKE, BigQuery, etc. VPC Service Controls enable clients to keep their entire data processing pipeline private. **Access Log** [Cloud Logging] • Cloud Logging is a fully managed service that allows you to store, search, analyze, monitor, and alert on logging data and events from Google Cloud and Amazon Web Services. You can collect logging data from over 150 common application components, on-premises systems, and hybrid cloud systems. [Access Transparency] • Access Transparency can maintain visibility of insider access to your data through near real-time logs from Access Transparency. **Protection from External Threats** [Cloud Security Command Center] • Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security

	posture by evaluating your security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities, and threats; and helping you mitigate and remediate risks. Virtual Machine Threat Detection ● Virtual Machine Threat Detection, a built-in service of Security Command Center Premium, can provide threat detection through hypervisor-level instrumentation. **Monitoring** ● The Google Cloud Status Dashboard provides status information on the services. ● The Google Workspace Status Dashboard provides status information on the services. ● Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services. ● Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. (c) Security resources Google also publishes guidance on: ● Security best practices ● Security use cases ● Security blueprints
Unique Identifiers ● Some unique identifiers, such as customer account numbers, have additional restrictions on disclosure.	Customer Responsibility: ● Customers should assign unique identifiers only if necessary and implement procedures for the management and protection of personal identifiers.

	Google Cloud Commentary: ● Google commits to process and protect your data in accordance with the contract terms. For more information on how Google protects customer data, see above.

Conclusion

At Google, we recognize that your data is yours only and guaranteeing the privacy of your data is key. The protection of your data is a primary design consideration for all our infrastructure, products and personnel operations. We believe that Google can offer a level of protection that very few public cloud providers or private enterprise IT teams can match. Because protecting data is core to Google's business, we can make extensive investments in security, resources, and expertise at a scale that others cannot. Our investment can free you to focus on your business and innovation.

Data protection and privacy is more than just security. Google's strong contractual commitments help make sure you maintain control over your data and how it is processed, including the assurance that your data is not used for advertising or any purpose other than to deliver Google Cloud services.

The information within this whitepaper should be used to help customers determine whether Google Cloud and Google Workspace products or services are suitable for them in light of the Gramm-Leach-Bliley Act.