Dear Hitachi Vantara Client,

It is our understanding that as an institution that is significantly engaged in "financial activities" as described in section 4(k) of the Bank Holding Company Act (12 U.S.C. § 1843(k)) you may be a "financial institution" ("FI") under the Gramm Leach Bliley Act ("GLBA"). As an FI, you may have certain obligations relating to the confidentiality of Customer Information ("CI") that you are required to impose on your "service providers".

According to GLBA regulations, a "service provider" is "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to [GLBA regulations]." See, e.g., FTC "Safeguards Rule" at 16 CFR Part 314.

"Customer Information" is defined as "any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form." "Nonpublic Personal Information" means "(i) personally identifiable financial information; and (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available." "Personally Identifiable Financial Information" means "any information: (i) a consumer provides to you to obtain a financial product or service from you; (ii) about a consumer resulting from any transaction involving a financial product or service between you and a consumer; or (iii) you otherwise obtain about a consumer in connection with providing a financial product or service to that consumer."

Hitachi Vantara, as a provider of back-end data storage products and services, is not a "service provider" under GLBA. Hitachi Vantara does not receive, maintain, process, or access "Customer Information" in any form that is readable by Hitachi Vantara in the course of providing services to your institution. As explained below, the technical infrastructure of Hitachi Vantara is such that any information contained within the system is the equivalent of de-identified information, because Hitachi Vantara does not possess the encryption key or have any other means to derive identifiable information from whatever is maintained on the storage array. Furthermore, Hitachi Vantara does not keep the encryption keys for any of its Customers, and therefore cannot decrypt its customers' data. Therefore, Hitachi Vantara does not consider itself to be a "service provider" for the purposes of GLBA because the transmission of data through the server does not constitute the disclosure to Hitachi Vantara.

In most instances, the data on the disk drives of Hitachi Vantara's products can be encrypted if the Encrypting Back End Controller ("EBED") is installed. Hitachi Vantara recommends the use of encryption to protect "Customer Information" and other "Personally Identifiable Financial Information" for the following reasons. The EBED provides hardware-based strong encryption (AES-256) for data at rest and can be applied to some or all of the internal drives within the disk subsystem. For customers that require encryption of data at rest on external or virtualized storage or data in flight (e.g. data that is being replicated from one storage array to another), Hitachi Vantara can provide partner solutions that will encrypt that information. When encryption is enabled on the EBED or via a partner solution, data is stored as cipher text on individual hard disk drives. In the case where data is stored as cipher text and a disk drive was to either fail and be returned to Hitachi Vantara or fall out of positive control of the data owner, data is protected from unauthorized access. Additionally, Hitachi Vantara does not maintain or escrow the encryption keys for any of its customers, and therefore cannot decrypt customers' data.

In circumstances where a customer does not utilize the encryption controller, data would not be accessible in human readable form to Hitachi Vantara. The data on a single drive is in cleartext format only, meaning that it contains sequences of ones and zeros. Additionally a single drive houses bits of information because the data is sprayed across several drives. Therefore, block data, such as a social security number or name, would not be available on a single drive.

In addition, a single drive that is removed from its set of drives is unusable because the information on the drive is destroyed when and if the drive is introduced to a new system. To explain it more fully, a single drive's residence in a system establishes it as a member of a contiguous set of drives, or "array group," and it is identified as a unique member of that series of drives. Because it is identified as such, once it is removed from its array, it cannot be used in another system until it is formatted to fit the array structure of the new system.

Hitachi Vantara takes data protection seriously and appreciates your concern that a drive being removed for maintenance may compromise the data contained on the drive. Consequently, we want to confirm, that a drive removed from its original system would not be usable in a second system until it is formatted to fit the established structure of the second system. The process of formatting the drive once it is introduced into the second system would destroy the data contained on the drive from the first system as the second system would have the data replaced with information to fit the second system's data structure.

Hitachi Vantara trusts that above explanation on how data on the drives appears to engineers will provide you with satisfactory assurance that your systems will be properly safeguarded. Thank you for your time and attention to this matter. Please contact the Hitachi Vantara Legal Department at 408-970-1000 with any questions or comments you may have.

Sincerely,

Hitachi Vantara Corporation