COMMENTS FROM WORLDWIDE ERC®
REGARDING THE PROPOSED REGULATION ON
CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES
23 NYCRR 500
NOVEMBER 14, 2016

Background Information Regarding Worldwide ERC®

Worldwide ERC® is a trade association representing the global employee relocation industry and the employers, relocation management companies, and suppliers which provide relocation services to employers and their employees around the world. A number of the employers which are a member of Worldwide ERC® are entities which would fall within the definition of a Covered Entity in the proposed rule and therefore many of the relocation management companies and suppliers which provide services to these entities would fall within the scope of the third parties doing business with Covered Entities as is contemplated by Section 500.11 of the proposed regulation.

Executive Summary

Worldwide ERC® believes that the proposed regulation is overly broad in a number of respects which are set forth in detail below and would impose unnecessary and unduly burdensome obligations upon these entities, the relocation management companies, and their suppliers which are unintended and not necessary to achieve the customer protection objectives of the proposed regulation.

Stated Intent of the Proposed Regulation and Flowdown Obligations

The proposed regulation states that it "is designed to promote the protection of customer information as well as the information technology systems of regulated entities." In furtherance of this goal and recognizing that regulated entities frequently engage subcontractors and furnish those subcontractors with customer information, the regulation at Section 500.11 (a) requires flow down of requirements to "ensure the security of Information Systems and Nonpublic Information that are accessible to or held by, third parties doing business with the Covered Entity." The definition of Nonpublic Information at Section 500.01 (g) includes: "(4) Any information that can be used to distinguish or trace an individual's identity…including occupational or employment information…"Section 500.11 (a) (4) requires that the Covered Entity, at least annually, assess such third party providers and the adequacy of their cybersecurity practices.

Request for Exclusion of Employee Benefit Service Providers

Worldwide ERC® believes that the combination of the broad definition of Nonpublic Information combined with the subcontractor flowdown requirements leads to a consequence that exceeds the stated goal of the regulation by requiring compliance by subcontractors that may have *employee* data, but not *customer* data. Accordingly, we request clarification that the regulation does not apply to third

party providers which provide employee benefit services to Covered Entities but which do not receive customer data from Covered Entities.

By including employee benefit providers within the scope of the third parties which are subject to the flowdown provisions, the regulation will impose upon the Covered Entities (many of which are large financial institutions and insurance companies who presumably have thousands of subcontractors) the burdensome requirement to audit all of their third party providers, even those which have not received any customer information from the Covered Entity.

Alternative Request for Various Changes the Proposed Regulation

If the regulation is not narrowed to exclude employee benefit providers, we would submit the following as issues:

1. Knowledge Qualification. Section 500.11 (b) (5) requires an absolute representation that the service/product is free of viruses, etc. that would impair the security of the Covered Entity's Information Systems or Nonpublic Information. We request that this representation be qualified as being "to the best of the knowledge of the third party service provider, …".

2. Scope and Confidentiality of Audits. Section 500.11 (b) (6) requires that the Covered Entity "or its agents" may perform cybersecuritys audits of the third party service provider. Such audits could put data of other persons and entities at risk. We request that this section be clarified to specify what types of audits and information may be accessed, under what circumstances, and subject to what confidentiality obligations which will assure that both the process and the results of the audit will protect the confidentiality of the underlying information. Any Covered Entity or its agents should be required to agree to strict confidentiality requirements in performing these audits.

3. No Access to Information by NY State Regulators. Any third party service provider which does business in the EU would be concerned with providing unfettered access to its information systems to any Covered Entity, especially if that information might then be made available to government regulators which have jurisdiction over Covered Entities. During the recent Privacy Shield negotiations between the EU and US, it was abundantly clear that the EU is very concerned over who in the US has access to data. We request that this provision should state that the NY state regulators would not have access to information of the third party service providers.

4. Definition of Nonpublic Information. The definition of "Nonpublic Information" is overly broad. We believe that, when the overly broad definition of "Nonpublic Information" is considered together with the requirement (i) to encrypt such information in transit and at rest; (ii) for the Covered Entity to perform annual audits with respect to how such information is protected; and (iii) the lack of an exclusion for employee information, an unduly burdensome obligation is created for both the Covered Entities and their third party service providers which will increase costs and create operational impediments without achieving the stated purpose of the regulations of promoting the protection of customer information of the Covered Entities. We

request that the definition of "Nonpublic Information" be narrowed to more clearly track other established definitions of personally identifiable information ("PII"), preferably either the US definition of PII or the EU definition of personal data.

5. Definition of Cybersecurity Event. The definition of "Cybersecurity Event" also is overly broad. This definition includes both successful and unsuccessful attempts to gain unauthorized access to systems or information. Then Section 500.11 (b) (3) requires the third party service provider to provide "prompt notice" to the Covered Entity in the "event of a Cybersecurity Event affecting the third party service provider". Daily reconnaissance, probes, and attempts to exploit potential vulnerabilities are the norm for any company, including both Covered Entities and third party service providers. Section 500.11 (b) (3) would require third party service providers to provide, and would result in Covered Entities being inundated with, notices of attempted access to third party systems or information, the vast majority of which were stopped before access was gained or information was misused. We request that Section 500.11 (b) (3) be revised to require notice only in the event that customer information was accessed or reasonably believed to have been accessed.

For further information regarding these comments, please contact Tristan North, Government Affairs Adviser for Worldwide ERC® at tnorth@worldwideerc.org or 703-610-0216.