PETER DROGAN
Chairperson

CHARLES P. KWOLEK, JR.
President

"Serving the Insurance Industry"

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES 23 NYCRR 500

Third Party Service Provider Cybersecurity Statement of Compliance

April 10, 2019

On March 1, 2017, New York became the first state to adopt a cybersecurity regulation (23 NYCRR 500) requiring individuals and non-governmental entities that are licensed or authorized to do business by the New York State Department of Financial Services ("DFS") to comply with its requirements. As a provider of insurance services in the automobile residual market, AIPSO, on behalf of the New York Automobile Insurance Plan ("NYAIP"), recognizes the importance of compliance with these new cybersecurity requirements. AIPSO is committed to protecting and securing its customer's information and is closely monitoring state and federal laws to ensure it takes appropriate action to ensure compliance with new and emerging requirements. While AIPSO/NYAIP has performed a comprehensive risk assessment and addressed every aspect of the New York State DFS cybersecurity regulation, this statement focuses on its commitment as a Third Party Service Provider.

As part of its cybersecurity program, AIPSO/NYAIP has implemented measures to comply with the New York State DFS cybersecurity regulation. The AIPSO/NYAIP cybersecurity program is designed to protect the confidentiality, integrity and availability of its systems and data. This program is applied using an effective combination of processes, technology, and people.

The program is implemented though adoption of the defense in depth concept where a series of defensive mechanisms are put in place such that if one mechanism fails, another will already be in place to thwart an attack. In addition, AIPSO is protected by a comprehensive Cyber Liability policy and its network and application infrastructure is regularly monitored and reviewed by AIPSO employees and consultants.

Section 500.11 of the New York cybersecurity regulation, Third Party Service Provider Security Policy, requires all covered entities [(1)] to implement written policies and procedures designed to ensure that Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers [(2)] are secure. In accordance with section 500.11, AIPSO/NYAIP:

1. Implemented policies and procedures for access controls, including the use of Multi-Factor Authentication as required by section 500.12 of the cybersecurity regulation, to limit access to relevant Information Systems and Nonpublic Information;

2. Implemented policies and procedures for the use of encryption as required by section 500.15 of the cybersecurity regulation to protect Nonpublic Information in transit and at rest; and

3. Will provide notice to the Covered Entity in the event of a Cybersecurity Event which directly impacts the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by AIPSO/NYAIP.

(1) Covered Entity means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

(2) Third Party Service Provider(s) means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

302 Central Avenue, Johnston, RI 02919
(401) 946-2310 • Fax (401) 528-1350
https://www.aipso.com