507F.10 Cybersecurity event reinsurers.

1. If a cybersecurity event involves nonpublic information used by, or that is in the possession, custody, or control of, a licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with consumers affected by the cybersecurity event, the assuming insurer shall notify each of the assuming insurer's affected ceding insurers and the commissioner of the assuming insurer's state of domicile within three business days of determining that a cybersecurity event has occurred. A ceding insurer that has a direct contractual relationship with a consumer affected by the cybersecurity event shall comply with the applicable provisions of section 715C.2, and all other applicable notification requirements pursuant to federal or state law.

2. If a cybersecurity event involves nonpublic information that is in the possession, custody, or control of a third-party service provider of a licensee that is acting as an assuming insurer, the assuming insurer shall notify each of the assuming insurer's affected ceding insurers and the commissioner of the assuming insurer's state of domicile within three business days of the date the assuming insurer receives notice from the assuming insurer's third-party service provider that a cybersecurity event involving nonpublic information has occurred. A ceding insurer that has a direct contractual relationship with a consumer affected by the cybersecurity event shall comply with the applicable provisions of section 715C.2, and all other applicable notification requirements pursuant to federal or state law.

3. Notwithstanding any law to the contrary, a licensee acting as an assuming insurer shall have no other notice obligations related to a cybersecurity event or other data breach than the notice requirements pursuant to subsections 1 and 2.

2021 Acts, ch 79, §10, 17
Section effective January 1, 2022; 2021 Acts, ch 79, §17
NEW section