

Posted on: September 5, 2018

Bulletin 2018-09 Cybersecurity Event Reporting Form

- Purpose

This is the second in a series of bulletins addressing the implementation of the newly enacted South Carolina Insurance Data Security Act (2018 S.C. Act No. 171 (“Act”). The Act is codified as Chapter 99 of Title 38 of the South Carolina Code of Laws. This Bulletin specifically addresses the process for reporting a Cybersecurity event, as defined in the Act. The Act becomes effective on January 1, 2019. Beginning on that date, licensees subject to the Act must provide notice of a Cybersecurity event to the South Carolina Department of Insurance.

- Notice of Cybersecurity Events

Under the Act, a “Cybersecurity event” is defined as “an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System.” The term “Cybersecurity event” does not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process or key is not also acquired, released or used without authorization. Cybersecurity event does not include an event with regard to which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed. Loss of information only in paper format does not constitute a Cybersecurity event.

Licensees will not be required to notify the Department of temporary disruptions in service due to power outages or other benign causes unless that disruption results in the unauthorized access, misuse or disruption of the licensee’s information system or that of its third-party service provider.

Licensees subject to the Act must notify the Director within 72 hours after determining that a Cybersecurity event has occurred if: 1) South Carolina is the licensee’s domicile; or 2) the licensee is not domiciled in South Carolina, but it is reasonably believed to have involved the release of nonpublic information of 250 or more South Carolina consumers and the Cybersecurity event impacts the licensee such that notice must be provided to another state or federal governmental entity, or there is a reasonable likelihood of material harm to a South Carolina consumer or material parts of the licensee’s operations.

- Cybersecurity Event Reports

The Department has developed the reporting form titled “Report a Cybersecurity Event” to simplify the reporting requirements for licensees in case of a Cybersecurity event. See Exhibit A.

This form contains fields for the information required to be reported to the Department following a Cybersecurity incident. A read-only copy of this form is available on our website at www.doi.sc.gov/cyber. An operational, live version of the form will be made available prior to January 1, 2019.

Tools

[RSS](#)

[Notify Me](#)

[View Archived](#)

Categories

- [All Categories](#)
- [Bulletins and Orders](#)
- [Press Releases](#)
- [VW Settlement](#)