South Carolina Department of Insurance

Capitol Center
1201 Main Street, Suite 1000
Columbia, South Carolina 29201

Mailing Address:
P.O. Box 100105, Columbia, S.C. 29202-3105
Telephone: (803) 737-6160

HENRY McMASTER
Governor

RAYMOND G. FARMER
Director

BULLETIN NUMBER 2018-09

TO: All Licensees of the South Carolina Department of Insurance

FROM: Raymond G. Farmer
Director of Insurance

SUBJECT: Cybersecurity Event Reporting Form
South Carolina Insurance Data Security Act, 2018 S.C. Act No. 171

DATE: September 4, 2018

I. 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.

II. 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.

III. 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.

The Department recognizes that detailed information may not be available within 72 hours of the discovery of a Cybersecurity event. The law contemplates that the licensee will notify the Director as soon as it is confirmed that there was unauthorized access, misuse or disruption to nonpublic information from the licensee's information system or that of the licensee's third-party service provider. Licensees must fill out as much information as possible on the form for the initial notification. Licensees will be assigned an "Event Number" when they first access the form which will allow them to return to the form to update information as it becomes available. Licensees have a continuing obligation under the law to update and supplement initial and subsequent notifications to the Director concerning the Cybersecurity event.

Certain Licensees may qualify for an exemption from the Information Security Program requirements contained in the Act. Additional guidance regarding exemptions will be provided in a subsequent bulletin.

IV. Questions

Questions concerning this bulletin should be directed to the attention of Melissa Manning, Associate General Counsel at mmanning@doi.sc.gov.

SOUTH CAROLINA
DEPARTMENT of INSURANCE

South Carolina Department of Insurance
Street Address: 1201 Main Street, Suite 1000, Columbia, S.C. 29201
Mailing Address: P.O. Box 100105, Columbia, S.C. 29202-3105
Telephone: (803) 737-6160 or 1 (800) 768-9999
Fax: (803) 737-6231 | Email: datasecurity@doi.sc.gov

REPORT A CYBERSECURITY EVENT

Under the South Carolina Insurance Data Security Act, licensees are required to report Cybersecurity Events to the S.C. Department of Insurance in accordance with the requirements of Section 38-99-40.

Section 1. Information of Entity Experiencing Cybersecurity Event

Licensee Type: Company ▼ Search for Licensee

NAIC Code | NPN # | SBS # | FEIN Code

Name
Address 1
Address 2
Suite/Apt/Building
City, State, Zip

Telephone
Fax
Email Address

Section 2. Event Dates

Estimated Occurrence ☐ Unknown | Estimated End ☐ Unknown | Date Discovered

Section 3. Event Type (Check all that apply)

☐ Data Theft by Employee/ Contractor
☐ Hackers/ Unauthorized Access
☐ Lost During Move
☐ Phishing
☐ Improperly Released/ Exposed/ Displayed
☐ Stolen Laptop(s)
☐ Computer and Equipment
☐ Improperly Disposed
☐ Other

Section 4. Circumstances Surrounding the Cybersecurity Event

How was the information exposed, lost, stolen, or accessed? Include the identity of the source of the Cybersecurity Event, if known.

How was the Cybersecurity Event discovered?

What actions are being taken to recover lost, stolen or improperly accessed information?

Section 5. Third-Party Involvement

Did the Cybersecurity Event occur within the information / systems maintained by the licensed entity or individual reporting the Cybersecurity Event or within the information / systems maintained by a third-party service provider? Our Information / Systems

Name of the Third-Party Service Provider

Description of the Third-Party Service Provider

What were the specific roles and responsibilities of the Third-Party Service Provider?

Section 6. Information Involved (Check all that apply)

Demographic Information
- Name
- Date of Birth
- Address
- Mother's Maiden Name
- Driver's License
- SSN
- Passport
- Other

Health Information
- Medical Records
- Lab Results
- Medications
- Treatment Information
- Physician's Notes
- Other

Financial Information
- Bank Account Information
- Credit Card
- Debit Card
- Other

Other

Was the electronic information involved in the Cybersecurity Event protected in some manner? Yes No N/A It involved paper records only

Describe the efforts being undertaken to remediate the situation which permitted the Cybersecurity Event to occur

Section 7. Number of Individuals / Entities Affected

Number affected nationally — Unknown

Number affected in South Carolina — Unknown

Section 8. Business-Related Information

If the licensee's own business data was involved, please provide details about the type(s) of data involved

Section 9. Notification Requirements

Is a notice to impacted South Carolina residents / entities required under South Carolina or federal law? Yes No Unknown

If yes, provide the date of notification. (Note: You should also upload a copy of the notice if not already provided to the SCDOI.)

Copy of notice will be sent on a subsequent date

Section 10. Law Enforcement

Has a police report been filed? Has any regulatory, governmental, or other law enforcement agency been notified? (If yes, please attach documentation of report / notification unless already provided to the SCDOI.)

Police Report: (•) Yes ( ) No ( ) Will be responding on a subsequent date

If yes, provide the date of notification

Regulatory Agency: (•) Yes ( ) No ( ) Will be responding on a subsequent date

If yes, provide the date of notification

Section 11. Contact Information of Individual Familiar with Cybersecurity Event and Authorized to Act on Behalf of the Licensee

First | Middle | Last

Title

Address 1

Address 2

Suite/Apt/Building

City, State, Zip

Telephone

Fax

Email Address

Section 12. Attachments

Items to Attach:

1. A report of the results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.
2. A copy of the licensee's privacy policy.
3. A statement outlining the steps the licensee will take to investigate and notify consumers affected by the Cybersecurity Event.

File	Document Type	Action
Click to select file	Internal Review	
Click to select file	Privacy Policy	
Click to select file	Investigation Outline	

Click to Add File(s)

Section 13. Attestation

I attest, to the best of my knowledge, that the information submitted on this form is true and correct to the best of my information and belief. By submitting this form, I am acknowledging that I am authorized to submit this form on behalf of the licensee or company. I further understand and agree that Section 38-99-60 of the South Carolina Code of Laws affords confidential treatment to certain information submitted to the SCDOI in accordance with Chapter 99. However, I understand that under state or federal law, the South Carolina Department of Insurance may be required to release statistical or aggregate information provided in this cybersecurity event notification. I acknowledge that copies of consumer notices may also be made available via the Department's website and the Department may also make available summary information related to cybersecurity events requiring public notification such as the identity of the licensee or third-party service provider, the number of individuals affected, the actions taken by the licensee to remedy the cybersecurity event and services available to consumers. I understand that Section 38-99-60 also gives the Director the authority to use the documents, materials or other information furnished by a licensee or someone acting on the licensee's behalf in furtherance of regulatory or legal actions brought as a part of the director's duties.

Yes

Submit Report