Notification of Cybersecurity Event

STATE OF MAINE
Bureau of Insurance
34 State House Station
Augusta, ME 04333-0034

The Maine Insurance Data Security Act, 24-A M.R.S. §§ 2261 – 2272, requires all licensees to notify the Superintendent as promptly as possible, but not later than three business days, after determining that a cybersecurity event has occurred involving nonpublic information in the licensee's possession if the criteria in 24-A M.R.S. § 2266(1)(A) or (B) applies.

The Act treats as confidential, and not subject to subpoena, discovery or admission in evidence in a private civil action, the information in this notification covered by 24-A M.R.S. §§ 2266(2)(B), (C), (D), (E), (H), (J), and (K). The fields below subject to this protection are shown with a yellow lock symbol; the others are not. Thus, the fact that a cybersecurity event has happened, the reporting licensee's identity, whether reports have been filed with law enforcement officials, the types of affected information, the number of affected people, the affected licensee's privacy policy and investigation and notification steps, and the licensee's contact person are public information. The reporting licensee has a continuing obligation to update and supplement this form regarding material changes to information previously provided relating to the cybersecurity event.

If you have questions about the Act, please contact the Bureau at **cybersecurity.boi@maine.gov (mailto:cybersecurity.boi@maine.gov)** or call (800) 300-5000.

* Required

1

Status: *

- ◯ Initial Report of Cybersecurity Event
- ◯ Updated Report of Cybersecurity Event

2

If updated report, date of initial report: *

Format: M/d/yyyy

Part I: 1. Licensee Reporting Cybersecurity Event

3

Name of Entity: *

4

Domicile: *

5

NAIC CoCode, National Producer Number, or Maine License Number: *

6

Licensee Type: *

- ◯ Insurer
- ◯ Producer Agency
- ◯ Individual
- ◯ Other

7

Address Line 1: *

8

Address Line 2:

9

City: *

10

State: *

11

Zipcode: *

12

If the Licensee is reporting for a group or affiliates, identify all entities affected by the cybersecurity event:

Part I: 2. Person Submitting Report

13

Name *

14

Business Name:

15

Address Line 1: *

16

Address Line 2:

17

City: *

18

State: *

19

Zipcode: *

20

Telephone Number *

21

Email Address *

22

Relationship to entity whose information was compromised *

Part II: 1. Cybersecurity Event

The Licensee must provide as much of the following information as possible. 24-A M.R.S. § 2266(2).

1. Cybersecurity Event Dates
24-A M.R.S. § 2266(2)(H)

This group of questions seeks details about the chronology of the cybersecurity event. Depending on the circumstances, the first date of event and the date the licensee discovered evidence of the event might be the same (such as a distributed denial of service attack) or different (such as a phishing attack [the event] in which the attacker went silent for a period of time before accessing the licensee's information systems [the compromise]).

23

Date of Event: *

Format: M/d/yyyy

24

Date evidence of the event was discovered: *

Format: M/d/yyyy

25

Do you know the initial date of the compromise? *

- ◯ Yes
- ◯ No

26

Initial date of compromise. *

Format: M/d/yyyy

27

Do you know the last date of compromise? *

- ◯ Yes
- ◯ No

28

Last date of compromise. *

Format: M/d/yyyy

How was the cybersecurity event discovered? Explain any delay between the date the event occurred and the date evidence of the event was discovered. *

Part II: 2. Cybersecurity Event

24-A M.R.S. § 2266(2)(B)

30

How did the cybersecurity event result in unauthorized access to, disruption of, or misuse of the Licensee's information system or information stored on the Licensee's information system? *

Check all that apply:

- [ ] Data theft by employee or contractor
- [ ] Hacker or unauthorized access
- [ ] Stolen, lost, or missing equipment
- [ ] Phishing
- [ ] Improperly released, exposed, displayed
- [ ] Lost during move
- [ ] Ransomware
- [ ] Lost by USPS/private courier
- [ ] Improperly disposed
- [ ] Only non-electronic information was involved
- [ ]

Other

Part II: 3. Third-Party Service Provider

24-A M.R.S. §§ 2265(2) and 2266(2)(B)

31

Did the cybersecurity event occur within the information or systems maintained by the Licensee or within the information or systems maintained by a third-party service provider (TPSP)? Check the applicable box. *

- ◯ Licensee's information or systems
- ◯ TPSP's information or systems.

32

TPSP Name: *

33

TPSP Address (street/P.O. Box; city; state; ZIP code): *

TPSP's specific roles and responsibilities: *

Part II: 4. Recovery of Information

24-A M.R.S. § 2266(2)(D)

35

Has any lost, stolen, or breached information been recovered? *

- ◯ Yes
- ◯ No

36

If Yes, how was the information recovered? *

Part II: 5. Identity of Event Source

24-A M.R.S. § 2266(2)(E)

37

Has the source of the cybersecurity event been identified? *

- ◯ Yes
- ◯ No

38

If yes, please describe: *

Part II: 6. Notification to Law Enforcement/Other Regulators

24-A M.R.S. § 2266(2)(F)

39

Has a police report been filed or other regulatory, government or law enforcement agencies been notified? *

- ◯ Yes
- ◯ No

40

Name of police or other agency:

41

Date report filed:

Format: M/d/yyyy

Part II: 7. Specific Type(s) of Information

24-A M.R.S. § 2266(2)(G)

42

Was identifying information acquired without authorization? *

- ◯ Yes
- ◯ No

43

Check the specific type(s) of identifying information acquired without authorization. *

- ☐ Name
- ☐ Date of Birth
- ☐ Address
- ☐ Mother's Maiden Name
- ☐ Driver's License
- ☐ Social Security Number
- ☐ Passport
- ☐ Other

44

Was the information protected? *

- ◯ Yes
- ◯ No

45

If the information was protected, was the encryption process or key also acquired? *

- ◯ Yes
- ◯ No

46

Was health information acquired without authorization? *

- ◯ Yes
- ◯ No

47

Check the specific type(s) of health information acquired without authorization. *

- ◯ Medical Records
- ◯ Lab Results
- ◯ Medications
- ◯ Treatment Information
- ◯ Physician's Notes
- ◯ [ ]

Other

48

Was the information protected? *

- ◯ Yes
- ◯ No

49

If the information was protected, was the encryption process or key also acquired? *

- ◯ Yes
- ◯ No

50

Was financial information acquired without authorization?

- ◯ Yes
- ◯ No

51

Check the specific type(s) of financial information acquired without authorization. *

- ◯ Bank Account Information
- ◯ Credit Card
- ◯ Debit Card
- ◯ Other: _____

52

Was the information protected? *

- ◯ Yes
- ◯ No

If the information was protected, was the encryption process or key also acquired? *

- ◯ Yes
- ◯ No

Part II: 8. Number of Consumers Affected by Cybersecurity Event

24-A M.R.S. § 2266(2)(I)

54

How many Maine residents did the event affect? *

55

How many people in total did the event affect? *

Part II: 9. Licensee Controls

24-A M.R.S. § 2266(2)(J)

56

Has a review of automated controls or internal procedures been conducted? *

- ◯ Yes
- ◯ No

57

Is the review complete? *

- ◯ Yes
- ◯ No

58

If No, please explain:

59

Did the review confirm that automated controls and internal procedures were followed? *

- ◯ Yes
- ◯ No

60

Please identify and describe the lapses in automated controls or internal procedures: *

Part II: 10. Remediation

24-A M.R.S. § 2266(2)(K)

61

Please describe the efforts undertaken to remediate the situation that permitted the cybersecurity event to occur - or send the information separately to cybersecurity.boi@maine.gov (mailto:cybersecurity.boi@maine.gov)

Part II: 11. Investigation and Notification to Consumers

24-A M.R.S. § 2266(2)(L)

62

Does the Licensee have a written privacy policy? If yes, please forward a copy to **cybersecurity.boi@maine.gov (mailto:cybersecurity.boi@maine.gov)** *

- ◯ Yes
- ◯ No

63

If no, please explain why not below:

64

Please describe in the box below the steps the Licensee has taken or will take to investigate and notify customers of the cybersecurity event.

65

Is notice to affected Maine residents and/or entities required under state or federal law? *

- ◯ Yes
- ◯ No

66

If yes, please explain your plan and timeline for notification. *

Part III: Contact Information of Authorized Person

24-A M.R.S. § 2266(2)(M)

67

Pick one: *

- ◯ The authorized individual is identified in and has the same contact information as provided in Section 1.
- ◯ The authorized individual is not identified in Section 1, or has different contact information from that provided in Section 1. If this box is checked, fill in the information below.

68

Name: *

69

Business Name: *

70

Address Line 1: *

71

Address Line 2:

72

City: *

73

State: *

74

Zipcode: *

75

Telephone: *

76

Email Address: *

77

Relationship to Reporting Licensee: *

Part IV: Supporting Documentation

Please indicate below which documents have been provided to **cybersecurity.boi@maine.gov (mailto:cybersecurity.boi@maine.gov)**

78

These are Required Documents: *

- [ ] 1. The Licensee's privacy policy (24-A M.R.S. § 2266(2)(L)).
- [ ] 2. A statement outlining the steps the License has taken or will take to investigate and notify consumers affected by the cybersecurity event (24-A M.R.S. § 2266(2)(L)).
- [ ] 3. Any notice or notices sent to consumers (24-A M.R.S. § 2266(3)).
- [ ] 4. Any documents necessary to respond adequately to the questions in this form.

79

The Licensee is encouraged to submit any other information or documents relevant to the cybersecurity event, such as:

- [ ] 1. Any police report or notice sent to a regulatory, government, or law enforcement agency (24-A M.R.S. § 2266(2)(F)).
- [ ] 2. Any review identifying a lapse in automated controls or internal procedures or confirming that all automated controls and internal procedures were followed (24-A M.R.S. § 2266(2)(J)).
- [ ] 3. Other relevant information.

Part IV: Attestation

As the authorized representative, and on behalf, of the Licensee, I hereby:

- certify that I am authorized to submit this form on behalf of the Licensee, that this notification contains all information required to be submitted, and that this notification and its attachments are true and complete as of the date submitted to the Superintendent;

- acknowledge that the Licensee has a continuing obligation to update and supplement initial and subsequent notifications to the Superintendent concerning the cybersecurity event;

- understand and agree that 24-A M.R.S. § 2268 affords confidential treatment of certain information submitted to the Superintendent. However, I understand that under state or federal law, the Superintendent may be required to release statistical or aggregate information provided in this form;

- acknowledge that copies of consumer notices may also be made available, and the Superintendent may make available summary or other information related to cybersecurity events as permitted or required under state or federal law; and

- understand that Section 2268 also gives the Superintendent the authority to use the documents, materials, or other information furnished by the Licensee or someone acting on the Licensee's behalf in furtherance of regulatory or legal actions brought as a part of the Superintendent's duties and to share them on a confidential basis in accordance with 24-A M.R.S. § 216(5).

80

Name: *

81

Title: *

82

Date: *

Format: M/d/yyyy