

February 15, 2023

Dominik Cvitanovic

(504) 702-1710

Dominik.Cvitanovic@wilsonelser.com

Via Legislature Report Submission Portal:

Hawai'i State Legislature

Hawai'i State Capital

Room 401

415 South Beretania St.

Honolulu, HI 96813

| | | | |
|------------|----------------------------|----------|---|
| Re: | Client | : | Office of Hawaiian Affairs |
| | Matter | : | Notice of Data Security Incident |
| | Wilson Elser File # | : | 16516.02055 |

Dear Sir or Madam:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents the Office of Hawaiian Affairs (“OHA”) with respect to a recent data security incident (hereinafter, the “Incident”). OHA takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

Pursuant to HRS § 487N-4 and HRS § 487J-4, this report will serve to inform you of the nature of the Incident, what information may have been compromised, and the steps that OHA has taken in response to the Incident.

1. Nature of the Security Incident

On December 14, 2022, OHA noticed suspicious activity within its email environment. OHA’s CFO received a request for a wire transfer from the email account of OHA’s CEO. The request had a dollar amount, routing information, and signature. This was flagged as a suspicious transfer request. The CFO called the CEO, who confirmed that the email was not legitimate. OHA immediately took responsive action, including (1) multiple global password resets; (2) a review of all suspicious logins with OHA’s email tenant; (3) the suspension of all CEO authorizations to financial transactions; and (4) implementation of temporary cross-functional authorization actions with OHA’s COO, CFO, and Treasury Director, with notice to the CEO.

OHA also immediately initiated an investigation into the incident and an assessment of its email security protocols by a third-party vendor. This investigation continues, but on January 31, 2023, OHA discovered that a breach of personal information may have occurred.

2. What Information Was Involved?

OHA is currently performing a review of all potentially impacted information to determine what information may have been exposed as a result of this incident. OHA is providing this preliminary notice out of an abundance of caution. As of this writing, OHA has not received any reports of related identity theft since the date of the incident.

3. Number of Individuals To Whom Notice Was Sent.

OHA's investigation is ongoing, but once completed, OHA will notify any individuals whose data may have been subject to unauthorized acquisition. OHA will supplement this notice upon completion of its investigation and notification of potentially impacted persons.

4. Other Important Information

OHA remains dedicated to protecting the sensitive information in its control. As noted above, OHA has reviewed, and continues to review, all suspicious logins within its email tenant, performed multiple global password resets, and has had its email security protocols assessed by a third-party vendor. OHA continues to work with the originating financial institution of the unauthorized transfer to enhance financial and electronic protections. OHA has also initiated agency-wide cybersecurity training of its employees and staff regarding potential cybersecurity risks. If you have any questions or need additional information, please do not hesitate to contact me at Dominik.Cvitanovic@WilsonElser.com or (504) 372-6698.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Dominik J. Cvitanovic, Esq.