

June 1, 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: Our 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”). Pursuant to HRS § 487N-4 and HRS § 487J-4, we write to supplement our previous report dated February 15, 2023 to further inform you of the Incident, what information may have been compromised, and the steps that OHA has taken in response to the Incident.

1. Nature of 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. On January 31, 2023, OHA discovered that a breach of personal information may have occurred. After further investigations, on May 19, 2023, OHA

400 Poydras Street, Suite 2250 | New Orleans, LA 70130 | p 504.702.1710 | f 504.702.1715 | wilsonelser.com

Albany, NY | Atlanta, GA | Austin, TX | Baltimore, MD | Beaumont, TX | Birmingham, AL | Boston, MA | Charlotte, NC | Chicago, IL | Dallas, TX | Denver, CO
Detroit, MI | Edwardsville, IL | Garden City, NY | Hartford, CT | Houston, TX | Jackson, MS | Las Vegas, NV | London, England | Los Angeles, CA | Louisville, KY
Madison, NJ | McLean, VA | Merrillville, IN | Miami, FL | Milwaukee, WI | Nashville, TN | New Orleans, LA | New York, NY | Orlando, FL | Philadelphia, PA | Phoenix, AZ
Raleigh, NC | San Diego, CA | San Francisco, CA | Sarasota, FL | Seattle, WA | Stamford, CT | St. Louis, MO | Washington, DC | West Palm Beach, FL | White Plains, NY

identified individuals whose personally identifiable information may have been compromised.

2. What Information Was Involved?

OHA found no evidence that personal information has been misused; however, it is possible that the following information could have been accessed by an unauthorized third party: names and Social Security numbers and in very limited circumstances driver's license numbers and financial account numbers without information permitting access to the financial accounts.

3. Number of Individuals To Whom Notice Was Sent.

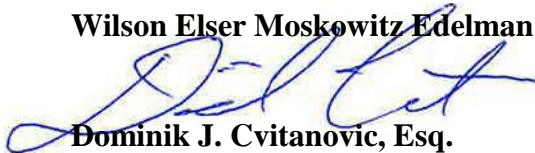
A total of seventy-four (74) individuals may have been potentially affected by this incident. Notification letters to these individuals were mailed on June 1, 2023, by first class mail. A sample copy of the notification letter is included with this letter under *Exhibit A*.

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.

Sincerely,

Wilson Elser Moskowitz Edelman & Dicker LLP


Dominik J. Cvitanovic, Esq.

Office of Hawaiian Affairs
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07491



[REDACTED]

Via First-Class Mail

June 1, 2023

Re: Notice of Cyber Incident

Dear [REDACTED],

The Office of Hawaiian Affairs (“OHA”) is writing to inform you of a recent data security incident that may have resulted in an unauthorized access to your sensitive personal information. 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. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On December 14, 2022, the Office of Hawaiian Affairs (“OHA”) noticed suspicious activity within its email environment. OHA immediately engaged a law firm specializing in cybersecurity and data privacy to investigate further. Additionally, OHA engaged third-party forensic specialists to assist OHA in its analysis of any unauthorized activity. The investigation identified a data set that may have been accessed by the unauthorized person. OHA then performed an extensive and comprehensive review of the data set and identified individuals whose personal information was in that data set. The investigation concluded on May 19, 2023.

What Information Was Involved?

Although OHA has no evidence that any sensitive information has been misused by third parties as a result of this incident, we are notifying you for purposes of full transparency. Based on the investigation, the types of information subject to unauthorized access varied by individuals, consisting of Social Security number.

What We Are Doing

Data privacy and security is among OHA’s highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon detecting this incident, OHA moved quickly to initiate a response, which included retaining a leading cybersecurity firm who assisted in conducting an investigation along with the assistance of leading IT specialists to confirm the security of OHA’s email environment. OHA has implemented additional security measures designed to prevent a recurrence of such an attack and to protect the privacy of OHA’s valued employees and vendors.

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twenty-four months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event

that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/oha> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

OHA sincerely regrets any concern or inconvenience this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,



Sylvia M. Hussey, Ed.D.
Ka Pouhana, Chief Executive Officer
Office of Hawaiian Affairs

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-800-349-9960	1-888-397-3742	1-888-909-8872
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, it is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer

Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

For Oregon residents, state law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For Rhode Island residents, this incident involves 0 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).