Office of the Administrative Director of the Courts – THE JUDICIARY • STATE OF HAWAIʻI
417 SOUTH KING STREET • ALIʻIŌLANI HALE • HONOLULU, HAWAIʻI 96813 • TELEPHONE (808) 539-4900 • FAX (808) 539-4855

Rodney A. Maile
ADMINISTRATIVE DIRECTOR

Daylin-Rose H. Heather
DEPUTY ADMINISTRATIVE DIRECTOR

October 18, 2024

The Honorable Ronald D. Kouchi
President of the Senate
State Capitol, Room 409
415 South Beretania Street
Honolulu, Hawaiʻi 96813

The Honorable Scott K. Saiki
Speaker of the House of Representatives
State Capitol, Room 431
415 South Beretania Street
Honolulu, Hawaiʻi 96813

Dear President Kouchi, Speaker Saiki, and Members of the Legislature:

Re: Report of Security Breach by Hawaiʻi State Judiciary

On October 4, 2024, the Hawaiʻi State Judiciary discovered that Judiciary employees' personal data had been breached. This occurred after a Judiciary staff member fell victim to a phishing email communication. That staff person's email inbox contained payroll documents that included Judiciary employees' names, addresses, birthdates and social security numbers. Bank account information was not breached. The breach was contained right away and immediate measures were taken to ensure no further security breach to this confidential information by use of the method used. Moreover, Judiciary employees were immediately notified and provided information as to recommended action, such as placing fraud alerts with the three available credit bureaus.

Pursuant to Hawaiʻi Revised Statutes Section 487N-4, I am submitting the enclosed written report explaining the incident, persons impacted, and action taken by the Hawaii State Judiciary. Please do not hesitate to call if you have questions or would like further information.

Sincerely,

Rodney A. Maile
Administrative Director of the Courts

Enclosures

Hawai‘i State Judiciary
Report of Security Breach

– Access to Judiciary Employee Personal Data –
Submitted Pursuant to HRS § 487N-4 (2006)

I. Breach Event, Discovery and Action Taken:

On October 4, 2024, the Hawai‘i Judiciary discovered that Judiciary employees' personal data had been breached. Upon investigation, it appeared that a Judiciary staff person was victimized by a phishing email communication. That employee's email inbox contained payroll documents that included Judiciary employees' names, addresses, birthdates and social security numbers. Bank account information was not breached. The breach was contained as soon as it was discovered and immediate measures were taken to ensure no further security breaches of confidential information by the method used. Upon discovery of the breach, Judiciary employees were immediately notified and provided information as to recommended action, such as placing fraud alerts with the three available credit bureaus.

II. Timeframe:

It appears that the Hawai‘i Judiciary's employee data was breached on October 2, 2024 at 10:01 am. The breach was contained on October 3, 2024 at 8:33 am. Judiciary administration learned about this breach on October 4, 2024 at 4:29 pm. On Oct. 4, 2024 at 9:19 pm, a text wire alert was sent to all Judiciary employees informing them of the breach and recommending steps to ensure financial safety. That alert was followed by an email message to all current Judiciary employees at 9:38 pm. A letter to impacted former Judiciary employees was sent by the Administrative Director of the Courts on October 8, 2024. Copies of these messages and correspondence are attached hereto.

III. Impacted Persons and Judiciary's Response/Alerts to Impacted Judiciary Employees:

We believe that personal data from June, 2021 to the present may have been improperly accessed, thus impacting approximately 2600 individuals (i.e., about 1700 current employees and 900 former employees).

At **9:19 pm,** October 4, the Judiciary sent a text wire alert to all Judiciary employees. The text alert stated:

> URGENT! An electronic file with employee names, social security numbers, addresses and birth dates was improperly accessed. IT and security vendor are working to assess and respond appropriately. Recommended action: Report fraud alerts with the 3 major credit bureaus: Equifax, Experian and TransUnion. URLS to follow.

At **9:38 pm,** October 4, an email was sent to all Judiciary employees. The email stated:

> This evening (Friday) our IT security system detected a breach of an employee's email inbox containing files with personal information for all Judiciary employees that is used for payroll processing. There was no bank account information in these files. At this time, we believe that employee names, addresses, social security numbers, and birthdates were improperly accessed. We recommend that you request fraud alerts with the three major credit bureaus. . . (Links to those credit bureaus were provided in the email message.)

At **5:14 pm,** October 5, the Judiciary sent a text wire alert to all Judiciary employees. The text alert stated:

> From CCR Office (Communications & Community Rel): Update on breach and tips on fraud alerts have been sent via email.

At **5:13 pm,** October 5, an email was sent to all Judiciary employees. The email stated:

> **Update:**
> While the investigation into the breach continues, all emails with file share requests, including Dropbox links, should be verified as legitimate with the person sending you the file(s). Do so by calling or emailing the person before taking any further action.
>
> **Your Personal Information**
> As a follow up to last night's email regarding the data breach, here are some tips when registering with Equifax, Experian, and/or TransUnion:
>
> - If you are having trouble doing so from your mobile phone, try using a desktop computer, laptop, or tablet.
> - If you are having difficulty accessing one of the sites or the performance is glitchy or slow, try using another browser.
> - **Equifax and TransUnion**: Set up an online log-in account first, then sign up.
> - **Experian:** Experian allows for sign up through two methods: Experian credit report number or personal information. If you don't have a credit report, then scroll down for the personal information option.
> - According to the Federal Trade Commission (FTC), as soon as one credit bureau confirms your fraud alert, the others will be notified to place fraud alerts.
>
> **Here's some additional information from the FTC:**
>
> Ask each credit bureau to send you a free credit report after it places a **fraud alert** on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit

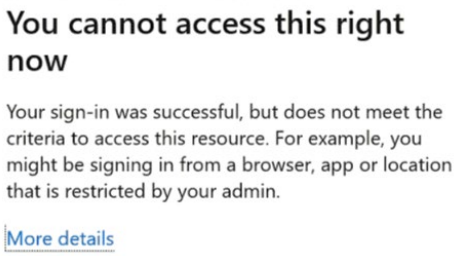
reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free **credit freeze**. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

Here is a link to the FTC's website, IdentityTheft.gov/databreach, about steps you can take to help protect yourself from identity theft. The steps are based on the types of information exposed in this breach.

At **9:23 am,** October 7, an email was sent to all Judiciary employees. The email stated:

Due to the recent security incident which -- was triggered by a phishing email — we are now blocking logins to Judiciary email from approximately 115 international countries. Anyone logging in from one of these countries, you will see the following message:



If have any questions or you plan to travel outside the United States and anticipate needing to email any Judiciary addresses, please notify the ITSD Help Desk at x5812.

IV. Action Taken to Prevent Further Security Breaches:

Upon discovery of this breach and to prevent this type of incident from recurring, the breached account password was reset and enhanced restrictions were set to block access from countries/regions where we believe access would be particularly risky.

V. Further Remediation and Continued Response to Cybersecurity Issues:

The Hawai‘i Judiciary recognizes the importance of cybersecurity safeguards. To this end, steps we have recently taken and actions planned for the very near future are as follows:

A. Mandatory Cybersecurity Training

Mandatory Training on cybersecurity issues was launched for all Judiciary employees, including judges, on October 1, 2023. The Judiciary's cybersecurity program's goal is to ensure the confidentiality, integrity and availability of the court's information, data and IT services. It also provides the policy, solutions and messaging services to protect and promote a safe and more secure internet environment for all Judiciary courts.

The Cybersecurity Training program consists of two courses — Avoiding Phishing Scams (8 minutes) and Cybersecurity at Work (60 minutes). The course reviews best practices for cybersecurity that includes how to recognize and report phishing. After completing the mandatory initial training, all Judiciary employees are required to take an online education program every four years.

In addition to the mandatory training, newsletters have been posted on the Judiciary's intranet with security tips and recent security alerts.

Additional phishing trainings will be added to the program for Judiciary employees who handle sensitive data.

B. Cybersecurity and Disaster Recovery Workshop

Several Judiciary employees attended a workshop entitled "Cybersecurity and Disaster Recover Workshop" sponsored by the National Center of State Courts, in September, 2024. At that workshop, representatives from various courts throughout the country discussed concerns, strategies and best practices going forward. A review was provided of some of the cybersecurity events that have occurred throughout the federal, state and local court levels and discussions were held as to how best to prevent such events and what to do in the event of their occurrence.

Following the workshop, information was disseminated to Judiciary personnel and follow up plans for cybersecurity awareness were discussed.

C. Tabletop exercises – Preparing for Appropriate Responses in the Event of Cybersecurity Attacks

The Judiciary has been involved with "tabletop exercises" which involves persons from different offices working together through sample hypothetical situations to determine appropriate responses in the event such occurrences actually take place. This will heighten awareness, require review of best practices and ensure that appropriate measures are taken in a timely manner in the event of cybersecurity threats or attacks.

D. Cybersecurity Information Officer

With funding from the legislature this past session, the Judiciary will soon be hiring a cybersecurity information officer. One of the primary assignments for this officer will be to review present measures, recommend improvements and assist with further training for Judiciary employees as to how to keep data safe and promote cybersecurity.

E. Microsoft Subscription Upgrade to G5

The Judiciary will request funding in the next legislative session to upgrade its current subscription with minimum security features to M365 G5 which includes a full suite of advanced threat and information protection and device management. One feature that would be included is an M365 monitoring tool that allows automatic user account lockout when risky behaviors are detected.

Office of the Administrative Director of the Courts – THE JUDICIARY • STATE OF HAWAIʻI
417 SOUTH KING STREET • ALIʻIŌLANI HALE • HONOLULU, HAWAIʻI 96813 • TELEPHONE (808) 539-4900 • FAX (808) 539-4855

Rodney A. Maile
ADMINISTRATIVE DIRECTOR

Daylin-Rose H. Heather
DEPUTY ADMINISTRATIVE DIRECTOR

October 8, 2024

[redacted]

Dear [redacted]:

We are writing to inform you that last Friday evening, October 4, the Judiciary's IT security system detected a breach of an employee's email inbox containing files with personal information for all Judiciary employees that is used for payroll processing. This employee was authorized to have this information.

At this time, we believe that employee names, addresses, social security numbers, and birth dates were improperly accessed. This includes those who were employed by the Judiciary as of **June 2021**. Our records indicate you are among the group of former employees potentially affected by this breach.

There was no bank account information in these files.

We understand it is concerning and want to assure you that our IT team and security vendor immediately began investigating the breach and took appropriate action. The investigation and response is ongoing.

Your Personal Information

We recommend that you request fraud alerts with the three major credit bureaus: Equifax, Experian, and/or TransUnion. Here are some helpful tips when registering:

- If you are having trouble doing so from your mobile phone, try using a desktop computer, laptop, or tablet.
- If you are having difficulty accessing one of the sites or the performance is glitchy or slow, try using a different browser.
- **Equifax and TransUnion**: Set up an online log-in account first, then sign up.
- **Experian:** Experian allows for sign up through two methods: Experian credit report number or personal information. If you don't have a credit report, then scroll down for the personal information option.
- According to the Federal Trade Commission (FTC), as soon as one credit bureau confirms your fraud alert, the others will be notified to place fraud alerts.

Some additional information from the FTC:

Ask each credit bureau to send you a free credit report after it places a **fraud alert** on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free **credit freeze**. A credit freeze means potential creditors cannot get your credit report and makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

Go to the FTC's web page, IdentityTheft.gov/databreach, to learn what you can do to help protect yourself from identity theft. The steps are based on the types of information exposed in this breach.

Any questions may be sent via email to: PAO@courts.hawaii.gov.

Sincerely,

Rodney A. Maile
Administrative Director of the Courts