



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

Rodney A. Maile
ADMINISTRATIVE DIRECTOR

Brandon M. Kimura
DEPUTY ADMINISTRATIVE DIRECTOR

July 25, 2023

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

Dear Mr. President and Members of the Senate:

Re: Final Report of Unauthorized Access to Personal Information -- HRS §487N-4

Please find enclosed a final written update to the Judiciary's April 2023 report to the Legislature, submitted in accordance with Hawaii Revised Statutes §487N-4, which requires government agencies to submit a report following the discovery of unauthorized access to personal information. The unauthorized access involved confidential personal information maintained on an internal component of the Judiciary Electronic Filing System (JEFS).

This final report of the incident provides further information on the procedures taken to ensure against further instances of unauthorized access to JEFS. In addition, our investigation did not find any additional individuals who were affected by this incident.

Sincerely,

A handwritten signature in blue ink that reads "Rodney A. Maile".

Rodney A. Maile
Administrative Director of the Courts



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

Rodney A. Maile
ADMINISTRATIVE DIRECTOR

Brandon M. Kimura
DEPUTY ADMINISTRATIVE DIRECTOR

July 25, 2023

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

Dear Mr. Speaker and Members of the House of Representatives:

Re: Final Report of Unauthorized Access to Personal Information -- HRS §487N-4

Please find enclosed a final written update to the Judiciary's April 2023 report to the Legislature, submitted in accordance with Hawaii Revised Statutes §487N-4, which requires government agencies to submit a report following the discovery of unauthorized access to personal information. The unauthorized access involved confidential personal information maintained on an internal component of the Judiciary Electronic Filing System (JEFS).

This final report of the incident provides further information on the procedures taken to ensure against further instances of unauthorized access to JEFS. In addition, our investigation did not find any additional individuals who were affected by this incident.

Sincerely,

A handwritten signature in blue ink that reads "Rodney A. Maile".

Rodney A. Maile
Administrative Director of the Courts

Hawai`i State Judiciary Final Report of Unauthorized Access to Personal Information – July 2023

This is an update to the Judiciary's April 2023 report to the Legislature submitted in accordance with Hawai`i Revised Statutes §487N-4. The unauthorized access involved confidential personal information maintained on an internal component of the Judiciary Electronic Filing System (JEFS).

JEFS enables eligible and registered attorneys and pro se parties to electronically file documents for court cases. Within JEFS is an internal system that is not available to the general public (internal JEFS), which includes confidential case information. The internal JEFS is only accessible to authorized individuals who are required to keep the information confidential.

The Nature of Unauthorized Access

The Judiciary first learned of the incident on April 11, 2023, when a letter from John F. Parker addressed to the Maui News, dated April 10, 2023, was forwarded to the Judiciary. In his April 10, 2023 letter, Mr. Parker alleged that because of security deficiencies in JEFS, he was able to use his JEFS document subscription to access an individual's social security number without authorization. Mr. Parker attached a screenshot of the social security number to support his claim, along with an explanation as to how such personal records could be obtained through the use of a URL address.

The process used by Mr. Parker to access personal information may have been shared with others. The April 10, 2023 letter included a copy of an email sent on April 7, 2023 with instructions explaining Mr. Parker's method of unauthorized access. Mr. Parker appeared to have addressed the email to himself, but it is unclear whether others may have been copied on the email. At a minimum, the instructions were shared with at least one other party when it was included in the letter addressed to the Maui News.

Upon receipt of the letter, the Judiciary immediately shut down JEFS and suspended Mr. Parker's access to JEFS while it investigated Mr. Parker's claim that any member of the public could access confidential information in internal JEFS by purchasing a JEFS document subscription.

Procedures Implemented to Prevent Further Unauthorized Access

The Judiciary shut down all access to the entire JEFS system on April 11, 2023, the same day the Judiciary learned of the unauthorized access to the affected individual's personal information. The Judiciary brought the JEFS system back online on April 12, 2023 only after taking immediate action to prevent future occurrences of the type of unauthorized JEFS access that Mr. Parker committed. Having taken this immediate action to prevent further unauthorized access to confidential information, and following the completion of our investigation into the incident, on July 18, 2023, Mr. Parker's access to JEFS was reinstated and he was informed of his reinstatement.

Investigative Findings and Determination of the Number of Affected Individuals

The Judiciary looked into whether other parties may have received the instructions in Mr. Parker's April 7 email and used them to access confidential information on internal JEFS prior to the Judiciary's response to the incident. After consulting with the Department of the Attorney General, and the Department of Accounting and General Services' Risk Management Office, the Judiciary retained counsel with information technology expertise. Forensic consultants helped ascertain whether anyone else used

Mr. Parker's method to access information from internal JEFS and, if so, what information was accessed and by whom. The conclusions from this investigation were:

(a) Mr. Parker's claim that any member of the public could access confidential information in internal JEFS by purchasing a JEFS document subscription, is false. In order to access internal JEFS, a JEFS subscriber is required to log into JEFS and then enter the specific URL, or internet address, for internal JEFS that provides a higher level of system access to retrieve the information via a webpage tab. Mr. Parker did not have authorized access to internal JEFS and was only able to obtain access by using the URL address without authorization.

(b) No additional persons were identified as being affected by the incident and thus no notifications of potential unauthorized access to personal information were issued. Consequently, there is only one confirmed individual who has been affected by the incident. By letter dated April 14, 2023, the Judiciary informed the affected individual of the unauthorized access and the Judiciary's initial investigation and response.

(c) The forensic consultant found no evidence of data scraping, or the mass extraction of information from a website, from the incident.

After investigating the incident and reviewing documentation provided by Mr. Parker and his counsel, the Judiciary determined that Mr. Parker:

- (1) obtained unauthorized access to internal JEFS;
- (2) used a means of unauthorized access to gain confidential personal information for which he should have known that he had no authority to access; and
- (3) disseminated the confidential personal information to at least one other party, along with written instructions on how to replicate his method of unauthorized access, without permission and without appropriate regard for the affected individual's privacy and safety and that of other individuals whose personal information is maintained on JEFS.

This is the final report of the Judiciary on this matter.