



Rodney A. Malle
ADMINISTRATIVE DIRECTOR

Brandon M. Kimura
DEPUTY ADMINISTRATIVE DIRECTOR

April 26, 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: Report of Unauthorized Access to Personal Information -- HRS § 487N-4

On April 11, 2023, the Hawaii State Judiciary was forwarded a letter alleging unauthorized access to personal information belonging to [REDACTED]. After conducting an investigation, we determined that the author of the letter was able to obtain [REDACTED] personal information after gaining unauthorized access to an internal feature on the Judiciary Electronic Filing and Service System.

Upon learning of the unauthorized access to [REDACTED] personal information, the Judiciary took immediate measures to ensure that there could be no further unauthorized access to confidential information by use of the method described in the forwarded letter.

The Judiciary is investigating whether anyone else accessed confidential information after receiving the same letter from the unauthorized user and, if so, which information was accessed and by whom. This will help us determine if persons other than [REDACTED] should be notified of the potential unauthorized access to their personal information.

Pursuant to Hawaii Revised Statutes § 487N-4, I am submitting the enclosed written report of the incident. This letter and the enclosed report serves as a preliminary notification and will be updated as soon as we have further information from which we can determine the extent of the problem and how best to protect against further problems. Further updated reports to the Legislature will include the number of individuals affected by the unauthorized access, a copy of any notice of unauthorized access (aside from the letter sent to [REDACTED] issued, the number of individuals to whom notice was sent, and all procedures taken to ensure that further instances of unauthorized access will not recur.

The Honorable Ronald D. Kouchi
April 26, 2023
Page 2

The Judiciary informed [REDACTED] about its initial investigation and response to the incident by letter dated April 14, 2023, a copy of which is enclosed with our report.

Sincerely,



Rodney A. Maile
Administrative Director of the Courts

Enclosure

Hawai'i State Judiciary
Report of Unauthorized Access to Personal Information – April 2023

The Judiciary submits this report 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 personal information maintained on an internal component of the Judiciary Electronic Filing and Service System (JEFS). The following is an account of the incident:

On April 11, 2023, the [REDACTED] for [REDACTED] forwarded to the Judiciary a letter dated April 10, 2023 from John Parker, Esq., addressed to the Maui News. In that letter, Mr. Parker alleged that, because of deficiencies in the Judiciary's data management system, he was able to use his JEFS subscription to access [REDACTED] social security number. Mr. Parker attached a screenshot of [REDACTED] 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.

Upon receipt of this letter, the Judiciary immediately shut down JEFS and investigated Mr. Parker's claim. The initial results of this investigation indicate that Mr. Parker was only able to obtain the personal information through unauthorized access to the data management system.

Mr. Parker's contention that "[a]ll a member of the public must do to access this confidential information is purchase an access pass for \$125" is inaccurate. To access this information, a JEFS subscriber would need to log into the system and then enter the specific URL, or internet address, that provides a higher level of system access to retrieve the information via a webpage tab. That URL is made available only to certain entities, upon login, primarily criminal justice partner agencies that are signatories to memoranda of understanding that protect the confidentiality of information and allow limited access and use for authorized purposes. Mr. Parker was not authorized to access the URL address he used.

Upon learning of the unauthorized access to [REDACTED] personal information, the Judiciary immediately took action to prevent further unauthorized access to confidential information utilizing the method Mr. Parker described. We have added another access control verification to the webpage tab in addition to replacing the URL used by Mr. Parker with a new address. If Mr. Parker, a JEFS subscriber, or anyone from the public were to discover the new address, the access control verification would still deny them access to the webpage tab.

Hawai'i State Judiciary
Report of Unauthorized Access to Personal Information – April 2023

Based on Mr. Parker's letter, the process he used to access personal information may have been shared with others. The letter includes an email drafted on April 7, 2023 with steps to access the webpage tab that appears to have been addressed to himself but does not show who could also have been copied. As of April 11, 2023, there were 266 active JEFS document subscribers. From April 7 to 11, 2023, the Judiciary identified 17 new or renewed subscriptions. Of these 17 subscribers, only three are not associated with a law firm or a self-represented litigant with an active case.

Currently, [REDACTED] is the only individual who we can confirm may have been affected by the incident. On April 14, 2023 we wrote to [REDACTED] informing [REDACTED] of our initial investigation and response. A copy of that letter is attached hereto.

The Judiciary is continuing to investigate whether other people accessed confidential information after receiving the April 7 email from Mr. Parker. We have retained forensic consultants to help us ascertain whether anyone else used this method to access information and, if so, which information was accessed and by whom. This will help us determine if persons other than [REDACTED] should be notified of the potential unauthorized access to their personal information. If additional personal information was compromised, we will take immediate corrective action, as statutorily specified.

The Judiciary has been actively working with the Department of the Attorney General and the Department of Accounting and General Services' Risk Management Office on this matter. We will continue our investigation to determine how Mr. Parker was able to obtain the URL to access personal information, whether any other JEFS subscribers may have used the same method as Mr. Parker to access the information from our internal system, and whether additional individuals were affected by the incident. We will submit updated reports to the Legislature regarding any new information from our investigation.

Enclosure: Letter to [REDACTED]



Rodney A. Maile

ADM N S RA VE D REC OR

Brandon M. Kimura

DEPU Y ADM N S RA VE D REC OR

April 14, 2023



Honolulu, Hawai‘i 96813

Dear [REDACTED]

I am writing to inform you about action taken by the Judiciary following the incident reported to me on April 11, 2023 concerning the compromise of your personal information. On that date, [REDACTED], forwarded a letter dated April 10, 2023 from John Parker, Esq., addressed to the Maui News. Mr. Parker’s letter alleges that, because of deficiencies in the Judiciary’s data management system, he was able to access your social security number through his Judiciary Electronic Filing System (JEFS) subscription. He attached a screenshot of your social security number to support his claim.

Upon receipt of this letter, the Judiciary immediately shut down JEFS and began an investigation to determine whether Mr. Parker’s claims were accurate. Based on this investigation, we believe that Mr. Parker was only able to locate this information through **unauthorized access** to our data management system.

Mr. Parker’s contention that “[a]ll a member of the public must do to access this confidential information is to purchase an access pass for \$125” is incorrect. The process he used is not one that can be discovered by any JEFS subscriber because one would have to log in using credentials of a subscriber and also know the specific sequence of characters that makes the URL, the internet address. That URL is available only to certain entities, primarily criminal justice partner agencies with MOUs that protect the confidentiality of information and access and use for limited purposes.

It was only by knowing and using the URL internet address provided by Mr. Parker that a JEFS subscriber would be able to access the information. Thus, one would have to know the unauthorized technique of using JEFS subscriber credentials to log in to the system and then switching the URL to obtain a higher level of access to access the information. The tab selected, “Violator History” is not available through a JEFS subscription account.

Based on Mr. Parker’s letter, the process for accessing personal information may have been shared with others. The letter includes an email drafted on April 7, 2023 with steps to access the Violator History tab that appears to have been addressed to himself but does not show who could also have been copied. As of April 11, 2023, there were

