UNIVERSITY of HAWAI'I®
Ke Kulanui o Hawai'i

Wendy F. Hensel
President

DEPT. COMM. NO. 358

February 27, 2026

The Honorable Ronald D. Kouchi,
President and Members of the Senate
Thirty-Third State Legislature
Honolulu, Hawai'i 96813

The Honorable Nadine K. Nakamura, Speaker
and Members of the House of Representatives
Thirty-Third State Legislature
Honolulu, Hawai'i 96813

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

For your information and consideration, the University of Hawai'i is transmitting a copy of the Amended Report on Data Exposure at the University of Hawai'i - Cancer Center (Section 487N-4, Hawai'i Revised Statutes) as requested by the Legislature.

In accordance with Section 93-16, Hawai'i Revised Statutes, this report may be viewed electronically at: https://www.hawaii.edu/govrel/docs/reports/2026/hrs487n-4_2026_cancer-center-exposure_amended-report.pdf.

Should you have any questions about this report, please do not hesitate to contact Stephanie Kim at (808) 956-4250, or via e-mail at scskim@hawaii.edu.

Sincerely,



Wendy F. Hensel
President

Enclosure

2444 Dole Street, Bachman Hall
Honolulu, Hawai'i 96822
Telephone: (808) 956-8207
Fax: (808) 956-5286
An Equal Opportunity Institution

UNIVERSITY OF HAWAIʻI SYSTEM REPORT

REPORT TO THE 2026 LEGISLATURE

Amended Report on Data Exposure at the
University of Hawaiʻi – Cancer Center

HRS 487N-4

February 2026

Subject: Amended Report to the Legislature on Data Exposure at the University of Hawai‘i – Cancer Center

Discovery of Data Exposure:	December 2025
Location of the Data Exposure:	University of Hawai‘i – Cancer Center – Research Operations
Nature of the Exposure:	Cyberattack on Certain Information Technology (IT) Systems in the Epidemiology Division of the Cancer Center

Incident Description and Response:

On or about August 31, 2025, the University of Hawai’i (UH) identified a cybersecurity incident isolated to specific systems that support its Epidemiology Division at the UH Cancer Center (UHCC). There has been no impact on the UHCC’s Clinical Trials operations or patient care at the UHCC, nor were the Basic Science or the Prevention Divisions at the UHCC impacted. There was no impact to UH student records. UH filed its initial Report to the Legislature on December 24, 2025. This amended report is based on currently available information and expands upon the initial Report. Please note that due diligence continues.

After UH identified that a threat actor (TA) had accessed the Epidemiology Division’s research files, UH promptly disconnected affected systems and took steps to terminate the TA’s unauthorized access and mitigate risk to data. Experts were immediately engaged to investigate and determine the nature and scope of the incident. Keeping law enforcement and external stakeholders informed, UH worked with an external team of cybersecurity experts to obtain a decryption tool and to secure and affirm destruction of any information the TA obtained illegally.

Due to the volume and complexity of data encrypted by the TA and the age of the studies and records, it took some time for UH to restore the affected systems and be in a position to assess the impact. Once the affected systems became accessible, UH promptly began identifying potentially impacted files and reviewed them for Personal Information.[1] During the course of the ongoing investigation, UH determined that the TA had access to and the opportunity to exfiltrate a subset of research files on certain servers supporting the Epidemiology Division.

Initally, the review identified a majority of the files related to the decades long Multi Ethnic Cohort (MEC) Study and primarily contained research data with no Personal Information about the research subjects. Between 1993 and 1996 the MEC Study recruited more than 215,000 residents of Hawai‘i and Los Angeles, California. A review of the affected files revealed the existence of a set of files containing Social Security numbers (SSNs), and/or Drivers’ License (DL) numbers for MEC Study participants.

[1] HRS §487N-1 defines “Personal Information” as including an individual’s first name or first initial and last name in combination with (1) Social security number or (2) Driver’s license number or Hawai‘i identification card number.

After making this discovery, UH submitted its initial report to the Legislature, and worked to compile the names and mailing addresses for potentially affected individuals. Notices regarding the data incident were mailed to 87,493 MEC Study participants on February 23, 2026; a sample of the notice is attached hereto (Attachment 1). The notice to affected individuals includes an offer of free credit monitoring and identity theft protection services.

UH continued its review of the remaining files for any additional sensitive information. Earlier this month, files were found containing names and Hawai'i State driver's license numbers (DLs) collected in the year 2000 from the State Department of Transportation, and voter registration (VR) information collected in the year 1998 from the City & County of Honolulu. In those days, SSNs were commonly used as driver's license and voter registration numbers, and government agencies freely provided said lists, which were used by researchers primarily to recruit study participants and for other research purposes. In addition, SSNs and health-related information obtained for other epidemiological studies of diet and cancer were uncovered.

The total number of potentially affected individuals is 1,153,527, not including the 87,493 MEC Study participants who are receiving written notification by mail. Because the total number of notifications exceeds 200,000, UH will be notifying the potentially impacted individuals in accordance with HRS §487N-2(e)(4):

> *(4) Substitute notice, if the business or government agency demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of subject persons to be notified exceeds two hundred thousand, or if the business or government agency does not have sufficient contact information or consent to satisfy paragraph (1), (2), or (3), for only those affected persons without sufficient contact information or consent, or if the business or government agency is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:*
>
> > *(A) Electronic mail notice when the business or government agency has an electronic mail address for the subject persons;*
> > *(B) Conspicuous posting of the notice on the website page of the business or government agency, if one is maintained; and*
> > *(C) Notification to major statewide media.*

UH has been able to locate email addresses for approximately 900,000 individuals who will be contacted via email by mid-March and provided with the attached sample "Notice of Data Incident" (Attachment 2). UH will post the "Notice of Data Incident" on UH websites, and notify major statewide media. Dedicated call centers will be available for individuals to inquire about the impact to them and to request credit monitoring services and insurance.

While review of the data continues, UH has high confidence that any other Personal Information (SSNs or DLs, in combination with names) found will be minimal (and if found, those individuals will receive separate notice), so UH is providing substitute notification now.

UH has taken the following steps to remediate the event and further bolster the security of the affected Epidemiology Division systems, including:

- Retaining third party experts to contain and remediate the event.
- Redesigning and hardening the network.
- Extending the deployment of modern endpoint protection with 24/7 monitoring.
- Migrating sensitive research servers to the secure UH Information Technology Services (ITS) data center.
- Upgrading hardware.
- Implementing stricter access controls for sensitive data.
- Rebuilding compromised systems to ensure that all malware has been eliminated and created new accounts/passwords to ensure that attackers no longer have access.
- Replacing existing firewall and rebuilding the network utilizing new firewall that includes additional security controls.
- Engaging independent third parties to assess and validate the security controls of the entire UHCC.
- Enforcing additional cybersecurity training for all Cancer Center employees.

An investigation team from the UH's Institutional Review Board is in the process of conducting a for-cause audit of impacted studies to ensure that the rights and welfare of participants are protected and to determine compliance with applicable federal, state, and institutional requirements.

In addition, to increase information security oversight and awareness across the entire system, UH has taken the following actions:

- Created a new Information Security Governance Council for Research (ISGC-R) responsible to coordinate research-related cybersecurity.
- Established a new Information Security Task Force responsible for updating policies, strengthening cyber roles and responsibilities, and recommending enterprise-level controls and investments.

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

UNIVERSITY OF HAWAI'I
CANCER CENTER

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

<<Date>> (Format: Month Day, Year)

<<b2b_text_1 (Re: Notice of Event Involving Your Personal Information/Notice of Data Breach)>>

Dear <<First_name>> <<Last_name>>,

On behalf of the University of Hawai'i Cancer Center ("UHCC"), I am writing to notify you of an event that may have involved your Social Security number and other research data. This letter provides you with details of the incident, our response, and resources available to help you protect your information, should you feel it necessary to do so. We had some of your personal information as detailed below in connection with a cancer research study, the Multiethnic Cohort Study (MEC Study), dating back to the early 1990s.

What happened. On or about August 31, 2025, we identified a cybersecurity incident isolated to specific servers that support the research arm of the UHCC's Research Operations. We promptly took affected systems offline and took steps to terminate the unauthorized access and mitigate risk to data. Experts were immediately engaged to investigate and determine the nature and scope of the incident. The affected data was contained in research files. There has been no impact on clinical operations or patient care at UHCC. The incident was also reported to law enforcement.

What information was involved. During the investigation, it was determined that an unauthorized third party gained access to and had the opportunity to exfiltrate a subset of research files on the servers supporting research operations. The impacted files may have contained your name, <<b2b_text_2 (Data Elements)>>, information you provided to the MEC Study, and certain information about you pulled from national and state cancer registries, which gather information from across the country to help doctors and researchers understand how to better prevent, find, and treat cancer. Programs like the Multiethnic Cohort (MEC) Study use this data to understand how lifestyle, diet, and genetics affect cancer risks for different groups of people.

What are we doing in response. In addition to launching a forensic investigation into this incident and notifying individuals, we reset passwords, implemented additional technical and organizational protection measures, and enhanced the security of our systems. Our security team and third-party cyber professionals continue to monitor our systems 24/7 for any unusual activity.

What can you do. To help protect yourself, we recommend remaining vigilant by reviewing and monitoring your financial account statements, and free credit reports for suspicious activity. We have included some additional steps that you can take to protect yourself, as you deem appropriate. While we have no evidence that any personal information has been used inappropriately, we recommend you take precautions, and **we are offering you 12 months of *free* credit monitoring and $1 million in identity theft insurance - to give you peace of mind. *You must activate the free product by the activation date in order for it to be effective. The activation instructions are included with this notification.***

Attachment 1

For more information, please call toll free (844) 443-0842 between 8:00 am – 5:30 pm Central Time, Monday - Friday (excluding holidays). We continue to take steps to enhance its security measures to help prevent something like this from happening in the future.

Sincerely,

Naoto T. Ueno

Director, University of Hawai‘i Cancer Center

STEPS YOU CAN TAKE

Below is information on steps you can take to help protect personal information, if you feel necessary.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** <<b2b_text_6 (activation deadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **<<Activation Code s_n>>**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by <<b2b_text_6 (activation deadline)>>. Be prepared to provide engagement number <<b2b_text_3 (Engagement Number)>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Additional Steps You May Wish to Take:

- **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your

credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

- **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

- **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD**. **CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. If your medical information was involved, it is also advisable to review the billing statements you receive from your healthcare providers. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 1-877-322-8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

  - *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
  - *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
  - *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

- **LAW ENFORCEMENT INVOLVEMENT:** Though law enforcement was notified of the incident, this notification has not been delayed as a result of a law enforcement investigation.

- **FAIR CREDIT REPORTING ACT (FCRA):** Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore/ or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. 1) You must be told if information in your file has been used against you. 2) You have the right to know what is in your file. 3) You have the right to ask for a credit score. 4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. 6) Consumer reporting agencies may not report outdated negative information. 7) Access to your file is limited. 8) You must give your consent for reports to be provided to employers. 9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. 10) You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. 11) You may seek damages from violators. 12) Identity theft victims and active-duty military personnel have additional rights.
- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT, FRAUD ALERTS, SECURITY FREEZES AND FCRA FROM THE FEDERAL TRADE COMMISSION.** Go to https://www.experian.com/fraud/center.html. Federal Trade Commission also provides information at https://consumer.ftc.gov/features/identity-theft FTC hotline is 1-877-438-4338; TTY: 1-866-653-4261 or write to the FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

UNIVERSITY OF HAWAI'I
CANCER CENTER

NOTICE OF DATA INCIDENT

This is notification by the University of Hawai'i Cancer Center ("UHCC") of an event that may have involved Social Security numbers (SSNs), driver's license (DL) numbers, names, addresses, and, in some cases research data for certain individuals defined below. This notification provides affected individuals details of the incident, our response, and resources available to help protect individuals' information, should it be necessary to do so. Individuals who participated in the Multiethnic Cohort Study (MEC Study) were mailed notifications on February 23, 2026, but all others whose SSNs and/or DL numbers may have been affected by this incident are being notified via email where an email address could be located and/or through publication.

What happened. On or about August 31, 2025, UHCC identified a cybersecurity incident isolated to several specific systems that support its Epidemiology Division. There has been no impact on clinical operations or patient care at UHCC. No student records were impacted.

After quickly identifying that a threat actor (TA) had accessed certain research files, UHCC promptly disconnected affected systems and took steps to terminate the TA's unauthorized access and mitigate risk to data. Experts were immediately engaged to investigate and determine the nature and scope of the incident. Keeping law enforcement and external stakeholders informed, UHCC worked with an external team of cybersecurity experts to obtain a means to unlock its systems and to secure and affirm the destruction of the data by the TA.

Due to the extensiveness of the encryption, it took some time to restore the affected systems and assess the impact to data. Once the affected systems became accessible, UHCC promptly began identifying potentially impacted files that may have contained personal information.

There is no evidence that the personal information was published, disseminated, or misused. Nonetheless, UHCC is notifying those whose information was in the impacted files so they may take steps to protect themselves, as necessary.

What information was involved. During the investigation, it was determined that an unauthorized third party gained access to and had the opportunity to exfiltrate a subset of research files used for certain epidemiology studies and recruitment efforts on the servers supporting epidemiology research operations at UHCC. This included the following files containing personal information (SSNs and/or DLs in combination with names):

1. Two files containing names in combination with SSNs: the first, containing DL numbers, was collected in the year 2000 from the State Department of Transportation; the second, containing voter registration information, was collected in the year 1998 from the City & County of Honolulu. At that time, DL numbers in Hawai'i were typically based on SSNs, and City and County of Honolulu voter registration information also often contained SSNs.
2. Files for study participants in the long-running Multi-Ethnic Cohort (MEC) Study (recruitment for participants in Hawai'i and Los Angeles, California from 1993-1996) and three other epidemiological studies of diet and cancer focusing on colorectal adenomas (recruitment for participants 1995-2007) and colon cancer (recruitment for participants 1994-2005), which also had SSNs and/or DL numbers in combination with names. They may also have contained questionnaires and other study information on participant health, as well as information pulled from national and state public health registries.
3. Two files that contain SSNs in combination with names collected from national and state public health registries as part of epidemiology research and study recruitment efforts. One file was closed to new names in 1999, and the other in the mid-2000s. The impacted files may also have contained research registry information about individuals' health.

What are we doing in response. In addition to launching a forensic investigation into this incident and notifying individuals, we enhanced existing security of our systems by resetting passwords and implementing additional technical and organizational protection measures. Our security team and third-party cyber professionals continue to monitor our systems for any unusual activity.

What can you do. If you believe you may have been affected by this incident, please contact (844) 443-0842 (hours below) for more information about resources we are offering to you. To help protect yourself, we recommend remaining vigilant by reviewing and monitoring your financial account statements, and free credit reports for suspicious activity. We have included below some additional steps that you can take to protect yourself, as you deem appropriate. While we have no evidence that any personal information has been used inappropriately, we recommend you take precautions. **If your information was involved, we are offering you 12 months of *free* credit monitoring and $1 million in identity theft insurance - to give you peace of mind. *You must activate the free product by the activation date in order for it to be effective. Please call the number above to learn how to enroll in the credit monitoring services.***

For more information about this incident, starting Monday, March 2, please call toll free (844) 443-0842 during the following hours.

- Monday to Friday, 8:30 a.m. to 9 p.m. Central Time (excluding holidays)
    - March 2-6, 2026, 4:30 a.m. to 5 p.m., Hawai‘i Standard Time
    - Starting March 9 (due to daylight savings time), 3:30 a.m. to 4 p.m. Hawai‘i Standard Time

We continue to take steps to enhance our security measures to help prevent something like this from happening in the future.

Sincerely,

Naoto T. Ueno
Director, University of Hawai‘i Cancer Center

STEPS YOU CAN TAKE

➢ **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

➢ **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

➢ **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. If your medical information was involved, it is also advisable to review the billing statements you receive from your healthcare providers. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

➢ **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 1-877-322-8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

➢ **LAW ENFORCEMENT INVOLVEMENT:** Though law enforcement was notified of the incident, this notification

has not been delayed as a result of a law enforcement investigation.

- **FAIR CREDIT REPORTING ACT (FCRA):** Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore/ or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. 1) You must be told if information in your file has been used against you. 2) You have the right to know what is in your file. 3) You have the right to ask for a credit score. 4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. 6) Consumer reporting agencies may not report outdated negative information. 7) Access to your file is limited. 8) You must give your consent for reports to be provided to employers. 9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. 10) You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. 11) You may seek damages from violators. 12) Identity theft victims and active-duty military personnel have additional rights.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT, FRAUD ALERTS, SECURITY FREEZES AND FCRA FROM THE FEDERAL TRADE COMMISSION.** Go to https://www.experian.com/fraud/center.html. Federal Trade Commission also provides information at https://consumer.ftc.gov/features/identity-theft FTC hotline is 1-877-438-4338; TTY: 1-866-653-4261 or write to the FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.