MICHIGAN STATE
UNIVERSITY

[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

RE: Important Security Notification
Please read this entire letter.

Dear [Insert customer name]:

We are writing to inform you of a data security incident that may have involved your personal information. Beginning on May 26, 2020, Michigan State University's (MSU) Physics and Astronomy departmental network was compromised by external attackers that enabled them to review and extract departmental files that may have enabled the theft of your personal information. The data types that were identified as having been exposed for you are:

[Data Type 1], [Data Type 2], [Data Type 3].

The vulnerability used by the criminals to access the departmental network has been deactivated and the affected systems have been removed or rebuilt to a defined security standard. The rebuilt network and systems have been reviewed and tested by our MSU Information Security team to ensure it is now secure and operational. MSU has been working in close cooperation with law enforcement partners and a third-party forensic audit firm on this matter and have carefully reviewed impacted data files to identify and notify affected persons. In addition to a technology security review, we are continually increasing our education and training across the MSU community to ensure the ongoing secure operations of our systems, networks, and data.

What we are doing to protect your information:
To protect your data from any further security breaches, MSU IT has migrated the affected department to centrally-managed and secured systems and networks, where enhanced security monitoring is implemented. MSU IT has also increased training and awareness on secure data storage and retention practices.

To help protect you from any negative impact of potential data disclosure, we are also offering a complimentary two-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity-theft detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

Information Technology Services

Office of the CISO

Computer Center
450 Auditorium Road
East Lansing, MI 48824

517-353-0722
tech.msu.edu

- Ensure that you **enroll by**: **[enrollment end date]** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [URL]
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [customer service number] by **[enrollment end date].** Be prepared to provide engagement number **[engagement #]** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR {24-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.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [customer service number]. 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 (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 this Identity Restoration support is available to you for two years 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. You will also find self-help tips and information about identity protection at this site.

In addition to the offered services from Experian ID Works, You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN

number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Security incidents reinforce the importance of everyday preventative measures all consumers should take to protect their personal information. MSU IT offers the following measures individuals can take to protect themselves when working and shopping online, including:

- Being aware of the possibility of phishing emails;
- Creating effective passwords;
- Using two-factor password authentication on devices and accounts whenever possible; and
- Deleting files and data when you are done using them.

We sincerely apologize for this incident and regret any inconvenience or concern it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact MSU at +1 517-432-6200.

Sincerely,

Thomas Siu
Chief Information Security Officer
Michigan State University

Philip Duxbury
Dean, College of Natural Science
Michigan State University

* Offline members will be eligible to call for additional reports quarterly after enrolling
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.