

MICHIGAN STATE UNIVERSITY

Via Email

August 13, 2020

Consumer Protection Bureau
New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110
DOJ-CPB@doj.nh.gov

To Whom It May Concern:

We represent Michigan State University, and with this letter, we are providing notice pursuant to N.H. Rev. Stat. Ann. § 359-C:20 regarding a recent data security incident. On June 24, 2020, Michigan State University was notified that an unauthorized party gained access to its online store, shop.msu.edu, and placed malicious code that was used to expose credit card numbers of shoppers between October 19, 2019 and June 24, 2020. Below is more information regarding this incident.

1. Name and contact information of person reporting the breach.

Jim Gallagher
Assistant General Counsel
Michigan State University
Gallagh3@msu.edu
(517) 353-3530

2. Name and address of business that experienced the breach, and the type of business.

Name: shop.msu.edu
Type of Business: Online business selling collegiate merchandise
Web address: <https://shop.msu.edu/>
Physical Address:
Angell Building
Michigan State University
166 Service Rd.
East Lansing, MI 48824

3. A general description of the breach, including the date(s) of the breach, when and how the breach was discovered, and any remedial steps taken in response to the breach.

As noted above, Michigan State University was notified on June 24, 2020, that an unauthorized party gained access to the University's online store, shop.msu.edu, and placed malicious code that was used to expose credit card numbers of shoppers between October 19, 2019 and June 24, 2020.

The unauthorized intrusion was a result of a configuration issue related to an administrative user's account. Once it became aware of the breach, the University's information security team took prompt action to correct the vulnerability that enabled the data to be exploited. An initial investigation determined the exposed information included names, addresses and credit cards from about 2,600 credit card holders. Importantly, no social security numbers were compromised and Michigan State University is working with law enforcement on this matter.



OFFICE OF THE
GENERAL COUNSEL

Michigan State University
Hannah Administration Building
426 Auditorium Road, Room 494
East Lansing, MI 48824
517/353-3530
Fax: 517/432-3950

- 4. The number of New Hampshire residents affected by the breach.**
There were four (4) New Hampshire residents affected by this breach.
- 5. A detailed list of the categories of personal information subject of the breach.**
The information that was exposed included the following: (i) first name; (ii) last name; (iii) physical address; and (iv) credit card number, CVV and expiration date.
- 6. The date(s) that notification was/will be sent to the affected New Hampshire residents.**
August 14, 2020.
- 7. A template copy of the notification sent to the affected New Hampshire residents.**
Attached is the Notification Letter template issue by Experian on behalf of Michigan State University.
- 8. Whether credit monitoring or identity theft protection services has been or will be offered to affected New Hampshire residents, as well as a description and length of such services.**
Yes. See attached Notification Letter for details.
- 9. Reason for any Delay in Sending Notification**
Notice to individuals and regulatory officials was delayed due to a comprehensive forensic audit performed by Michigan State University's IT Team, with coordination from local law enforcement and the FBI.

If you have any questions regarding this matter, please refer them to the undersigned at the contact number listed in Item 1 of this letter.

Sincerely,



Jim Gallagher
Assistant General Counsel
Michigan State University

Attachment: Experian Notice

August 14, 2020



F7124-L01-0000001 T00001 *****OEL LINE

SAMPLE A SAMPLE - L01

APT #123

123 ANY ST

ANYTOWN, US 12345-6789



RE: Important Security Notification
Please read this entire letter.

Dear Sample A Sample:

We are writing to inform you of a data security incident that may have involved your personal information. Between October 19, 2019 and June 26, 2020, shop.msu.edu was compromised by external attackers that inserted malicious code which may have enabled the theft of name, address and credit card information, including the card number, expiration date and CVV code, used to purchase goods through the site.

The malicious code has been removed and the system has been reviewed by our IT Security team to ensure it is now secure and operational. Michigan State University has been working in close cooperation with our processing banks and law enforcement partners on this matter. 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.

What we are doing to protect your information:

To protect your data from any further security breaches, in addition to the mandatory security training already in place, MSU IT will be requiring advanced training for the website administrators who manage the affected site to ensure they are adhering to all appropriate security measures.

We are also offering a complimentary two-year membership of Experian's® IdentityWorksSM. 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:

- Ensure that you **enroll by: November 30th, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **<https://www.experianidworks.com/3bcredit>**
- Provide your **activation code:** [REDACTED]

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 (833) 281-4829 by **November 30th, 2020**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

0000001



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 (833) 281-4829. 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.

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 +1 517-355-1855.

Sincerely,



Daniel Ayala
Interim Chief Information Security Officer
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.