



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: ljensen@mullen.law

3 Allied Drive, Suite 303
Dedham, MA 02026

October 30, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Saint Xavier University (“SXU”) located at 3700 W. 103rd St, Chicago, IL 60655, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one hundred thirty-six (136) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SXU does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 21, 2023, SXU became aware of potential suspicious activity within certain computer systems. Accordingly, SXU quickly took steps to contain the suspicious activity, confirm the security its systems, and with the assistance of external cybersecurity specialists, initiated a comprehensive investigation to determine the full nature, scope, and impact of the activity. The investigation determined that an unauthorized actor downloaded certain files stored on limited SXU systems between June 29 and July 18, 2023. In light of this unauthorized access, SXU conducted a thorough and time-consuming review of the identified data to determine what information was present and to whom it related for purposes of assessing potential notification obligations. Once the preliminary results of this review were identified, significant efforts were required to enrich necessary address information and reconcile the records to further the notification assessment and process. SXU worked diligently to complete these efforts, and on August 26, 2024, all such efforts were completed. Thereafter SXU continued its diligent efforts, working to notify identified individuals as quickly as possible.

The information that could have been subject to unauthorized access varies by individual and includes name, Social Security number, driver's license or state identification number, financial account information, health insurance information, and medical information.

Notice to Maryland Residents

On or about October 30, 2024, SXU began providing written notice of this incident to affected individuals, which includes one hundred thirty-six (136) Maryland residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning the event, SXU moved quickly to investigate and respond to the incident, assess and confirm the security of SXU systems, and identify potentially affected individuals. SXU also promptly notified federal law enforcement regarding the matter. Additionally, SXU continues to review and, where necessary, enhance its existing policies and procedures relating to data protection and security, and has implement additional technical and administrative safeguards and training to its employees. Further, as an added measure, SXU is also providing access to credit monitoring services for twelve (12) months, through IDX, a ZeroFox company, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, SXU is providing impacted individuals with guidance on how to better protect against identity theft and fraud. SXU is also providing notified individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. SXU is also notifying relevant regulatory authorities, as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data event, please contact us at (267) 930-2303.

Very truly yours,

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/laf
Enclosure

EXHIBIT A



3700 West 103rd Street
Chicago, IL 60655
844-468-6798
(844-GOTO-SXU)
www.sxu.edu

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/SaintXavierUniversity>

October 30, 2024

RE: Notice of Data <<Breach/Incident>>

Dear <<First Name>> <<Last Name>>:

Saint Xavier University ("SXU") writes to inform you of an incident that may impact the privacy of some of your information. You are receiving this letter because you are a current or former SXU student or employee, a dependent, spouse, or beneficiary of a current or former employee, a parent or guardian of a current or former SXU student, or you previously applied for admission. This notice provides you with information about the matter, our response, and steps you can take to help protect your personal information, should you feel it appropriate to do so.

What Happened? In July 2023, we became aware of potential suspicious activity within our computer systems. Accordingly, we quickly took steps to contain the activity, confirm the security of our systems, and begin a comprehensive investigation to determine the full nature, scope, and impact of the activity. The investigation determined that an unauthorized actor downloaded certain files stored on limited SXU systems between June 29 and July 18, 2023. In light of this unauthorized access, we conducted a thorough and time-consuming review of the identified data to determine what information was present and to whom it related for purposes of assessing potential notification obligations. Once the preliminary results of this review were identified, significant efforts were required to enrich necessary address information to further the notification assessment and process. These efforts recently concluded, and you are receiving this notification because our investigation identified that your information was present in the relevant data.

What Information Was Involved? The investigation determined that the files involved in this matter included your name, <<data elements>>.

What We Are Doing. We take this matter and the security of information in our care seriously. Upon first learning of the activity, we quickly responded, and have been working diligently to provide you with an accurate and complete notice. We also promptly notified federal law enforcement, and we also provided relevant updates to the SXU community as we worked to respond to this matter. Further, as part of our ongoing commitment to the privacy and security of personal information in our care, we continue to review and, where necessary, enhance our existing policies and procedures relating to data protection and security. We have also implemented additional security measures to mitigate risk associated with this incident and to help minimize the reoccurrence of a similar future incident. We are also providing notice of this incident to potentially impacted individuals and to relevant regulatory authorities, as required.

As an added measure, we are providing you with <<CM length>> months of complimentary access to credit monitoring services through IDX, a ZeroFox company, as well as guidance on how to better protect your information, should you feel it is appropriate to do so. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself.

What You Can Do. As a general best practice, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You may also review and consider the information in the enclosed *Steps You Can Take to Help Protect Personal Information*. There you will find additional information about the complimentary credit monitoring services we are offering and how to enroll.

For More Information. If you have additional questions about this incident, please call our dedicated assistance line at: 1-877-225-2116, which is available Monday to Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time. You may also write to SXU at 3700 W 103rd St, Chicago, IL 60655.

Sincerely,

Saint Xavier University

Steps You Can Take To Help Protect Personal Information

Enroll in Monitoring Services

Scan the QR image or go to <https://response.idx.us/SaintXavierUniversity> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is January 30, 2025.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud.

Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Saint Xavier University is located at 3700 W 103rd St, Chicago, IL 60655.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 24 Rhode Island residents that may be impacted by this event.