



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Maria Monastra
Office: (267) 930-4602
Fax: (267) 930-4771
Email: MMonastra@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

November 4, 2022

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

Dear Sir or Madam:

We represent Seminole State College of Florida (“the College”) located at 100 Weldon Blvd., Sanford, FL 32773. We are writing to notify your office of an incident experienced by one of the College’s third-party vendors, Omnigo, that may affect the security of certain personal information relating to one (1) Maryland residents (the “Omnigo Incident”). Omnigo assists the College with collecting and storing incident reports created by the College’s Department of Campus Safety & Security. This notice may be supplemented with any new significant facts learned after its submission. By providing this notice, the College 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 September 2, 2022, Omnigo informed the College of a gap in Omnigo’s data retention controls which allowed some customer information to remain on a server that was being used to facilitate the transfer of the data to a new location. This was the first time the College learned of any potential issue. Omnigo’s review of the issue revealed that the customer information involved could have been accessed by an unauthorized third party during four separate instances on August 3, 2021, November 3, 2021, February 3, 2022, and May 8, 2022.

Upon learning of the Omnigo Incident, the College immediately moved to determine what, if any, sensitive information relating to the College was involved. The investigation to date has included working diligently to gather additional information from Omnigo to understand the scope of the incident and nature of the data affected, including whether such data was rendered unusable

through encryption during the periods of potential unauthorized access. On September 26, 2022, the College received additional incident details from Omnigo, including the types of data pertaining to the College that could have been accessed or acquired by an unauthorized third party. Since that date, the College has undertaken efforts to locate address information for the individuals whose personal information was present on the Omnigo server at the time of the incident and provide notice of the incident.

The information that could have been subject to unauthorized access includes the following types of data related to Maryland resident: name and driver's license number.

Notice to Maryland Resident

On November 4, 2022, the College provided written notice of this incident to one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter included herewith as *Exhibit A*.

Other Steps Taken and To Be Taken

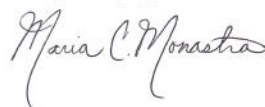
Upon learning of the Omnigo Incident, the College moved quickly to investigate and respond, gather additional details from Omnigo, and identify potentially affected individuals. Further, the College is coordinating with Omnigo to confirm its implementation of additional security controls since the incident to protect against a similar incident in the future. As an added precaution, the College is providing individuals potentially affected by the Omnigo Incident with access to complimentary credit monitoring services for one (1) year through Experian.

Additionally, the College is providing potentially affected individuals with guidance on how to protect against identity theft and fraud. The College is also providing individuals with guidance 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event it describes, please contact us at (267) 930-4602.

Very truly yours,



Maria Monastra of
MULLEN COUGHLIN LLC

MCM/nad
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

i5529-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



November 4, 2022

NOTICE OF [Extra3]

Dear Sample A. Sample:

Seminole State College of Florida (“We” or “the College”) is writing to notify you of an incident that one of our third-party vendors, Omnigo, experienced and recently reported to us (the “Omnigo Incident”). The Omnigo Incident may affect the privacy of some of your information.

We contract with Omnigo for assistance with collecting and storing the College’s incident reports created by Campus Safety & Security. We take the Omnigo Incident very seriously and sincerely regret any concern it may cause you.

What Happened? On September 2, 2022, Omnigo informed the College of a gap in Omnigo’s data retention controls which allowed some customer information to remain on a server that was being used to facilitate the transfer of the data to a new location. This was the first time the College learned of any potential issue. Omnigo’s review of the issue revealed that the customer information involved could have been accessed by an unauthorized third party during four separate instances on August 3, 2021, November 3, 2021, February 3, 2022, and May 8, 2022.

Upon learning of the Omnigo Incident, we immediately moved to determine what, if any, sensitive information relating to the College was involved. Our investigation to date has included working diligently to gather additional information from Omnigo to understand the scope of the incident and nature of the data affected, including whether such data was rendered unusable through encryption during the periods of potential unauthorized access. On September 26, 2022, the College received additional incident details from Omnigo, including the types of data pertaining to the College that could have been accessed or acquired by an unauthorized third party. Since that date, the College has undertaken efforts to locate address information for the individuals whose personal information was present on the Omnigo server at the time of the incident and begin providing notice of the incident.

What Information Was Involved? The College understands from Omnigo that the potentially impacted incident reports may have contained a combination of the following: your name and [Extra2]. **Please note that your Social Security number was not impacted by the Omnigo Incident.** Please further note that as of the date of this letter, Omnigo has reported to the College that there is no evidence of information misuse as a result of the incident.

ENGAGE#

0000001



i5529-L01

What We Are Doing. Protecting the privacy and security of information entrusted to us is among our highest priorities. We continue to work closely with Omnigo to respond to the incident and determine the impact to the College's data as a result. We are also coordinating with Omnigo to confirm its implementation of additional security controls since the incident to protect against a similar incident in the future. To date, Omnigo has confirmed that it fully addressed the underlying gap in data retention controls and implemented additional data access requirements. If our ongoing efforts to investigate the Omnigo Incident reveal details that significantly alter any details included in this letter, we will update you accordingly.

As an added precaution, we are offering you access to complimentary credit monitoring and identity protection services for 12 months through Experian. These services, which include fraud consultation and identity restoration, are being offered to you free of cost, but due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included in the enclosure to this letter.

What You Can Do. 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 and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*. There, you will also find more information on the complimentary credit monitoring services we are making available to you.

For More Information. We understand that you may have questions about the Omnigo Incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (877) 644-1116, Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). Be prepared to provide engagement number **ENGAGE#**. You may also write to us at Seminole State College of Florida, c/o Risk Management, 100 Weldon Blvd., Sanford, FL 32773.

We apologize for any inconvenience or concern this incident may cause you.

Sincerely,

Dick T. Hamann

Dick T. Hamann
VP, Information and Technology Resources/CIO

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration Services

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity 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: January 31st, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

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 (877) 644-1116 by **January 31st, 2023**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your [Extra4]-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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** 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 (877) 644-1116. 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 [Extra4] 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. You will also find self-help tips and information about identity protection at this site.

* 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.

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 your free credit report, visit

ENGAGE#

0000001



www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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
888-298-0045	1-888-397-3742	833-395-6938
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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 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, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.

