OSBORN MALEDON
ATTORNEYS AT LAW

Danielle D. Janitch
Direct: 602-640-9381
Office: 602-640-9000
djanitch@omlaw.com

2929 North Central Avenue
Suite 2000
Phoenix, Arizona 85012
omlaw.com

August 9, 2024

VIA EMAIL (Idtheft@oag.state.md.us)
AND US MAIL

Anthony G. Brown
Maryland Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice pursuant to The Personal Information Protection ACT (PIPA), Md. Code Ann., Com. Law § 14-3504

To Whom it May Concern,

We are writing as counsel for East Valley Institute of Technology ("EVIT") to formally notify the Office of the Attorney General of a security breach pursuant to Md. Code Ann. Comm. Law 14-3504. EVIT is providing written notice in connection with the data security incident it experienced on January 9, 2024, which involved unauthorized access to EVIT's servers and computer systems by a threat actor associated with the LockBit ransomware group.

Details Regarding Impacted Maryland Citizens

EVIT learned on August 7, 2024, that the January 9, 2024 breach impacted 32 Maryland citizens. We attached an example of the written notice that will be provided to Maryland citizens as **Exhibit 1.** This notice will be mailed on or about August 13, 2024, to the 32 recently identified as impacted Maryland citizens. The following data elements, including "Personal information" elements under Md. Code Ann., Com. Law § 14-3501(e) (bolded), were impacted in the breach: **IEP/504 Plan**, **SSN, Driver's License or State ID**, Financial Aid Information, **TIN, Tribal ID Number**, Account Number, Routing Number, **Health Insurance Information, Medical Information**, Financial Aid Account Number, **Health/Allergy Information, Diagnosis, Patient ID Number, Health Insurance Policy Number or Subscriber Number or Policy Number**, **US Alien Registration Number, Medical Record Number, Treatment Location**, Payment Card Number, **Mental or Physical Condition, Treatment Type, Prescription Information, Passport Number, Treatment Information**, Username with Password Pin or Login Information, **Patient Account Number, Biometric Data, Mental or Physical Treatment, Diagnosis Code**, Payment Card Type, **Military ID Number**. EVIT was overinclusive in identifying data elements beyond the scope of Maryland's "Personal information" definition. EVIT used search criteria broader than

the notification requirements of many state laws in order to make a broad disclosure to potentially impacted individuals. Particular data elements impacted vary by individual and state; not all data elements were impacted for each individual or in each state.

Description of Security Breach

On January 9, 2024, the East Valley Institute of Technology (EVIT) experienced a cyber-incident involving unauthorized access to its servers and computer systems. The initial investigation revealed that the cyber-incident was carried out by a threat actor associated with the LockBit ransomware group, using compromised credentials to access the EVIT VPN remotely. The virtualized server infrastructure, which stores all server data, was impacted by the ransomware. VMware does not appear to have been impacted. The breach had a limited operational impact. EVIT was able to continue to operate after the incident and cloud-based systems remained operational, but there was potential exposure of sensitive information belonging to current and former students, faculty, and parents.

Immediate actions taken included corrective steps to investigate and secure systems, reporting the incident to law enforcement and relevant authorities, and engaging a third party to review potentially impacted files. Notification efforts involved informing impacted individuals and offering tools to minimize harm, as well as continuous monitoring for the publication of data.

Measures implemented to address the incident included enhanced security protocols and systems, engagement of cybersecurity experts for investigation and response, offering credit monitoring services to affected individuals, and providing regular updates and notifications to potentially impacted individuals.

Remediation Status and Steps Taken

EVIT contacted state, local, and federal law enforcement, locked down VPN Access, deployed EDR software, has 24x7 monitoring for the incident, privileged user access has been revoked, service account passwords have all been changed, all user passwords have been changed, domain trust has been revoked, some domain cleanup has taken place, and all nineteen virtual servers were rebuilt or replaced, so that none of the prior impacted servers were brought back onto the network. The three largest credit reporting agencies--Equifax, Experian, and TransUnion--were notified of this breach on June 14, 2024

EVIT's Notification Efforts

As part of EVIT's efforts to notify affected persons as promptly as possible, preliminary notification was provided to all current and former students, parents and faculty at their most current email address on file. These notifications were sent on January 12, January 24 and March 5, respectively. Copies of these notifications are included with our submission as **Exhibit 2**. These notices were sent to everyone with an email address on file at EVIT, while the investigation to identify affected individuals proceeded as quickly as possible. On June 18, 2024, EVIT conspicuously posted an additional notice of the breach (https://www.evit.edu/about-evit/district-departments/information-systems/notice-of-january-breach) on its website (https://www.evit.edu/), where it will remain for at least 45 days and be updated as necessary. This

notice constituted substitute notice under Arizona Statute. A copy of this notification is included with our submission as **Exhibit 3**.

EVIT engaged a third party to review potentially impacted files to identify the individuals by name whose data may have been compromised in the incident. Due to the large number of files to be reviewed, potentially impacted individuals were not identified by name until June 4. EVIT had physical addresses on file for approximately half of these identified individuals. But the physical addresses are from when the impacted individuals last attended EVIT and have never been updated. Counsel, on behalf of EVIT, engaged a notification vendor to verify and, if possible, locate additional physical addresses for identified impacted individuals. Of those addresses EVIT had on file, the notification vendor explained that only about 39,000 addresses were current enough for reliable NCOA address search and verification. So, as part of the address verification process, EVIT authorized the notification vendor to conduct an advanced address search for individuals who received no prior email notice and had Personal Information (as defined by state law) impacted. This physical address identification process was completed on August 7, 2024. Notification letters will be sent promptly, on or about August 13, 2024, to all individuals with identified physical addresses, offering credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. In addition, anyone impacted by the incident will also be eligible to receive the same credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. Additional email notifications of these services, as well as an update to the online website notice, will occur on or about August 13, 2024.

Reason for Delay in Notifying the OAG and Maryland Citizens

As outlined above, EVIT acted promptly to respond to the cyber-incident, immediately reporting the incident to law enforcement and engaging counsel to conduct an investigation. Email notification was sent out promptly following the incident to all potentially impacted individuals with email addresses on file with EVIT. Subsequently, an online notification was prominently posted on EVIT's website. Finally, notification to physical addresses is anticipated to on or about August 13, 2024, promptly after receiving updated physical address information from the notification vendor that EVIT contracted with to notify impacted individuals.

A full investigation of the incident required engagement of a data-mining consultant and a notification vendor. These vendors were necessary measures to determine the scope of the breach, including identification of the individuals impacted and data elements involved. Until the notification vendor completed its physical address search on August 7, 2024, EVIT did not have the necessary information to determine where impacted individuals resided or where to send physical notifications. Consequently, EVIT also did not have information necessary to make individual state notices. EVIT learned on August 7, 2024, that 32 Maryland citizens were impacted, and thus is now providing notice to Maryland's Office of the Attorney General. Additionally, written notice will be mailed to impacted Maryland citizens on or about August 13, 2024, using the address information provided by EVIT's notification service provider on August 7.

Commitment to Continued Efforts

EVIT remains committed to protecting the personal information of its students, faculty, and associated individuals.

We appreciate your attention to this matter and are available to provide any additional information or clarification as needed.

Sincerely,

Danielle D. Janitch

Enclosures:

- Exhibit 1: Data Breach Form of Notification Letter
- Exhibit 2: Previous Email Notifications (January 12, January 24, and March 5)
- Exhibit 3: EVIT Substitute Notification Posted to EVIT's Website

Exhibit 1

022594

evit
COLLEGE AND CAREER

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

72 022594

Parent or Guardian of
[redacted]

Enrollment Code: MTCV94EMTN
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/EVIT

August 13, 2024

Notice of Data Breach

Dear Parent or Guardian of [redacted],

What Happened

On January 9, 2024, the East Valley Institute of Technology ("EVIT") was the target of a cyber-incident that involved unauthorized access to the network. The records of 208,717 individuals were potentially affected. This attack had a limited impact on our operations. We promptly took corrective steps to investigate the incident, secure our systems, report the incident to the three largest nationwide consumer reporting agencies and appropriate authorities, contain and remediate the threat, and notify potentially impacted individuals. To date, EVIT has not discovered any publication of EVIT data that contained sensitive information. However, given the possibility that sensitive information may have been compromised, EVIT engaged a third party to conduct a thorough review of all potentially impacted files. This review concluded recently and identified your child as potentially impacted by the cyber-incident.

What Information Was Involved

For impacted individuals, the categories of impacted personal information may include Class List, Student ID Number, Date of Birth, Race/Ethnicity, Grades, Course Schedule, Home Phone Number, Email Address, Home Address, Parent/Guardian Name, Transcript, IEP/504 Plan, SSN, Driver's License or State ID, Financial Aid Information, Class Rank, Place of Birth, TIN, Tribal ID Number, Account Number, Routing Number, Health Insurance Information, Account Type, Disciplinary File, Medical Information, Absence Reason, Financial Aid Account Number, Health/Allergy Information, Diagnosis, Patient ID Number, Institution Name, Health Insurance Policy Number or Subscriber Number or Policy Number, US Alien Registration Number, Medical Record Number, Treatment Location, Payment Card Number, Mental or Physical Condition, Treatment Type, Prescription Information, Passport Number, Treatment Information, Username with Password Pin or Login Information, Patient Account Number, Biometric Data, Mental or Physical Treatment, Diagnosis Code, Payment Card Type, and Military ID Number. However, the potentially compromised information varies by individual, and for most individuals, not all of this data was potentially compromised.

What We Are Doing

EVIT is working tirelessly to improve security and mitigate risk. To date, EVIT has contacted the appropriate authorities, locked down VPN Access, deployed EDR software, has 24x7 monitoring for the incident, revoked

privileged user access, changed all service account passwords, changed all user passwords, revoked domain trust, performed domain cleanup, and rebuilt or replaced nineteen virtual servers so that none of the prior impacted servers were brought back onto the network. EVIT engaged a third party specializing in network security to help EVIT with adding these and other computer security protections and protocols to harden its network infrastructure and offer improved protections of sensitive data from unauthorized access.

Further, immediately following detection of the incident, EVIT provided email notification to all current and former students, staff, faculty, and parents with email addresses on file with EVIT. These notices were sent out of an abundance of caution, as EVIT investigated to determine by name potentially impacted individuals.

Promptly following completion of the impacted file investigation, EVIT posted alternative website notice for impacted individuals online at www.evit.edu/about-evit/district-departments/information-systems/notice-of-january-breach, as it simultaneously diligently worked to find current mailing addresses and send individual notice to anyone identified as potentially impacted by the breach.

You are eligible to receive identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 12 months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-457-8842, going to https://response.idx.us/EVIT, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 a.m. - 9 p.m. Eastern Time. Please note the deadline to enroll is November 13, 2024.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. For more on how to protect your information, please see the enclosed Recommended Steps document.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on online, so please do not discard this letter.

Please call 1-888-457-8842 or go to https://response.idx.us/EVIT for assistance or for any additional questions you may have.

Sincerely,

Superintendent Dr. Chad Wilson
East Valley Institute of Technology (EVIT)

(Enclosure)

022594

IDX
A ZEROFOX COMPANY

Recommended Steps To Help Protect Your Information

1. **Website and Enrollment.** Scan the QR image or go to https://response.idx.us/EVIT and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Telephone. Contact IDX at 1-888-457-8842 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

3. Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. If your minor has a credit report:

A. Review your minor's credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

B. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

It is necessary to contact only one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

5. **Security Freeze.** You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact each of the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your child's credit files.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Arizona Residents: Office of Attorney General of Arizona may be contacted at: 2005 N. Central Avenue, Phoenix, AZ 85004; 1-602-542-5025. The Arizona Attorney General provides additional information on protection against identify theft and data privacy and data breach reporting online at: www.azag.gov/consumer/data-breach.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, Telephone: 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

015441

evit
COLLEGE AND CAREER

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

51 015441

[redacted]

Enrollment Code: AAAAAAAAAAAAAA
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/EVIT

August 13, 2024

Notice of Data Breach

Dear [redacted],

What Happened

You previously received an email from EVIT concerning a data breach that occurred earlier this year. This is a follow-up letter to provide you with further details and steps you can take to protect your information. On January 9, 2024, the East Valley Institute of Technology ("EVIT") was the target of a cyber-incident that involved unauthorized access to the network. The records of 208,717 individuals were potentially affected. This attack had a limited impact on our operations. We promptly took corrective steps to investigate the incident, secure our systems, report the incident to the three largest nationwide consumer reporting agencies and appropriate authorities, contain and remediate the threat, and notify potentially impacted individuals. To date, EVIT has not discovered any publication of EVIT data that contained sensitive information. However, given the possibility that sensitive information may have been compromised, EVIT engaged a third party to conduct a thorough review of all potentially impacted files. This review concluded recently and identified you as potentially impacted by the cyber-incident.

What Information Was Involved

For impacted individuals, the categories of impacted personal information may include Class List, Student ID Number, Date of Birth, Race/Ethnicity, Grades, Course Schedule, Home Phone Number, Email Address, Home Address, Parent/Guardian Name, Transcript, IEP/504 Plan, SSN, Driver's License or State ID, Financial Aid Information, Class Rank, Place of Birth, TIN, Tribal ID Number, Account Number, Routing Number, Health Insurance Information, Account Type, Disciplinary File, Medical Information, Absence Reason, Financial Aid Account Number, Health/Allergy Information, Diagnosis, Patient ID Number, Institution Name, Health Insurance Policy Number or Subscriber Number or Policy Number, US Alien Registration Number, Medical Record Number, Treatment Location, Payment Card Number, Mental or Physical Condition, Treatment Type, Prescription Information, Passport Number, Treatment Information, Username with Password Pin or Login Information, Patient Account Number, Biometric Data, Mental or Physical Treatment, Diagnosis Code, Payment Card Type, and Military ID Number. However, the potentially compromised information varies by individual, and for most individuals, not all of this data was potentially compromised.

What We Are Doing

EVIT is working tirelessly to improve security and mitigate risk. To date, EVIT has contacted the appropriate authorities, locked down VPN Access, deployed EDR software, has 24x7 monitoring for the incident, revoked

privileged user access, changed all service account passwords, changed all user passwords, revoked domain trust, performed domain cleanup, and rebuilt or replaced nineteen virtual servers so that none of the prior impacted servers were brought back onto the network. EVIT engaged a third party specializing in network security to help EVIT with adding these and other computer security protections and protocols to harden its network infrastructure and offer improved protections of sensitive data from unauthorized access.

Further, immediately following detection of the incident, EVIT provided email notification to all current and former students, staff, faculty, and parents with email addresses on file with EVIT. These notices were sent out of an abundance of caution, as EVIT investigated to determine by name potentially impacted individuals.

Promptly following completion of the impacted file investigation, EVIT posted alternative website notice for impacted individuals online at www.evit.edu/about-evit/district-departments/information-systems/notice-of-january-breach, as it simultaneously diligently worked to find current mailing addresses and send individual notice to anyone identified as potentially impacted by the breach.

You are eligible to receive identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-457-8842, going to https://response.idx.us/EVIT, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 a.m. - 9 p.m. Eastern Time. Please note the deadline to enroll is November 13, 2024.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. For more on how to protect your information, please see the enclosed Recommended Steps document.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-888-457-8842 or go to https://response.idx.us/EVIT for assistance or for any additional questions you may have.

Sincerely,

Superintendent Dr. Chad Wilson
East Valley Institute of Technology (EVIT)

(Enclosure)

015441

IDX
A ZEROFOX COMPANY

Recommended Steps To Help Protect Your Information

1. **Website and Enrollment.** Scan the QR image or go to https://response.idx.us/EVIT and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-457-8842 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact each of the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Arizona Residents: Office of Attorney General of Arizona may be contacted at: 2005 N. Central Avenue, Phoenix, AZ 85004; 1-602-542-5025. The Arizona Attorney General provides additional information on protection against identify theft and data privacy and data breach reporting online at: www.azag.gov/consumer/data-breach.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, Telephone: 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Exhibit 2

Jan. 12, 2024

Dear EVIT faculty, staff, parents and students,

On Jan. 9, EVIT was the target of a cyber-incident that involved unauthorized access to certain servers and other computer systems. This attack has had a limited impact on our operations. We immediately took corrective steps to investigate the incident, secure our systems, report the incident to law enforcement, and to remediate any impacts to our systems.

We are working to determine what, if any, faculty, staff, student, or parent information was compromised. But as a precaution, we will be working with faculty and students in the coming days to reset passwords for their accounts at EVIT. Please be on the lookout for communication over the weekend on how we will proceed resetting passwords.

Our investigation into this cyber incident is ongoing. At this point, we are not aware of any misuse or external disclosure of your personal information. However, we are notifying you so that if you desire, you can take action, in addition to our efforts, to minimize or eliminate potential harm. These steps include:

1. Closely monitor your financial accounts. If your financial institutions permit you to notify them of a potential theft of your personal information, please do so.

2. Place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

Equifax	Experian	TransUnionCorp
800-685-1111	888-397-3742	800-680-7289

Please note there is no cost to place a fraud alert on your credit file, however, the credit bureaus may offer you additional products for a fee.

3. File an identity theft report with the FTC at IdentityTheft.gov. Details regarding this program are available at: https://www.ftc.gov/news-events/topics/identity-theft/report-identity-theft.

4. Even if you do not find any suspicious activity on your initial credit reports or accounts, the Federal Trade Commission (FTC) recommends checking your credit reports periodically. Reports may be obtained by visiting www.annualcreditreport.com or calling 877-322-8228. Checking your credit reports periodically can help you spot problems and address them quickly. Get a copy of the credit report; many creditors want the information to absolve you of fraudulent charges. Additional information about identity theft is available on the FTC's website at www.ftc.gov/idtheft.

EVIT is a family, and we take the importance of the information our family entrusts to us very seriously. We will work closely with our insurance carrier as they investigate the event and we are already

reviewing our processes and implementing additional safeguards to protect your information.

Please don't hesitate to contact me with any questions or concerns at cwilson@evit.edu.

Sincerely,
Superintendent Dr. Chad Wilson

Dear EVIT faculty, staff, parents, and students,

I am writing to provide you with an update to my earlier letter regarding the cyber incident that targeted EVIT on Jan. 9. As part of that investigation, we have become aware of unverified social media posts stating that EVIT was the target of a ransomware attack and that stolen files may be published. Since we learned of the cyber incident, we have been working tirelessly to investigate what, if any, faculty, staff, student, or parent information may have been compromised.

That investigation is ongoing. Again, we encourage you to take the steps we outlined in our prior letter to minimize or eliminate potential harm from the cyber incident:

1. Closely monitor your financial accounts. If your financial institutions permit you to notify them of a potential theft of your personal information, please do so.

2. Place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

Equifax	Experian	TransUnionCorp
800-685-1111	888-397-3742	800-680-7289

Please note there is no cost to place a fraud alert on your credit file, however, the credit bureaus may offer you additional products for a fee.

3. File an identity theft report with the FTC at IdentityTheft.gov. Details regarding this program are available at: https://www.ftc.gov/news-events/topics/identity-theft/report-identity-theft.

4. Even if you do not find any suspicious activity on your initial credit reports or accounts, the Federal Trade Commission (FTC) recommends checking your credit reports periodically. Reports may be obtained by visiting www.annualcreditreport.com or calling 877-322-8228. Checking your credit reports periodically can help you spot problems and address them quickly. Get a copy of the credit report; many creditors want the information to absolve you of fraudulent charges. Additional information about identity theft is available on the FTC's website at www.ftc.gov/idtheft.

Please feel free to reach out to me with any questions or concerns at cwilson@evit.edu.

Sincerely,

Superintendent Dr. Chad Wilson

Dear former EVIT faculty, staff, parents, and students,

On Jan. 9, EVIT was the target of a cyber-incident that involved unauthorized access to certain servers and other computer systems. This attack has had a limited impact on our operations. We immediately took corrective steps to investigate the incident, secure our systems, report the incident to law enforcement, and to remediate any impacts to our systems.

I am writing to you now because while we originally believed the breach to be narrower in scope, our investigation of the attack is ongoing, and we want to provide former faculty, staff, parents, and students with the tools to minimize or eliminate any potential harm resulting from the cyber attack.

As part of our investigation, we have become aware of unverified social media posts stating that EVIT was the target of a ransomware attack and that stolen files may be published. Since we learned of the cyber incident, we have been working tirelessly to investigate what, if any, current or former faculty, staff, student, or parent information may have been compromised. To date, no publication of data has included any sensitive data.

That investigation is ongoing. Out of an abundance of caution, we encourage you to take the steps to minimize or eliminate potential harm from the cyber incident:

1. Closely monitor your financial accounts. If your financial institutions permit you to notify them of a potential theft of your personal information, please do so.

2. Place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

Equifax	Experian	TransUnionCorp
800-685-1111	888-397-3742	800-680-7289

Please note there is no cost to place a fraud alert on your credit file, however, the credit bureaus may offer you additional products for a fee.

3. File an identity theft report with the FTC at IdentityTheft.gov. Details regarding this program are available at: https://www.ftc.gov/news-events/topics/identity-theft/report-identity-theft.

4. Even if you do not find any suspicious activity on your initial credit reports or accounts, the Federal Trade Commission (FTC) recommends checking your credit reports periodically. Reports may be obtained by visiting www.annualcreditreport.com or calling 877-322-8228. Checking your credit reports periodically can help you spot problems and address them quickly. Get a copy of the credit report; many creditors want the information to absolve you of fraudulent charges. Additional information about identity theft is available on the FTC's website at www.ftc.gov/idtheft.

EVIT is a family, and we take the importance of the information our family entrusts to us very seriously. We will work closely with our insurance carrier as they investigate the event and we are already

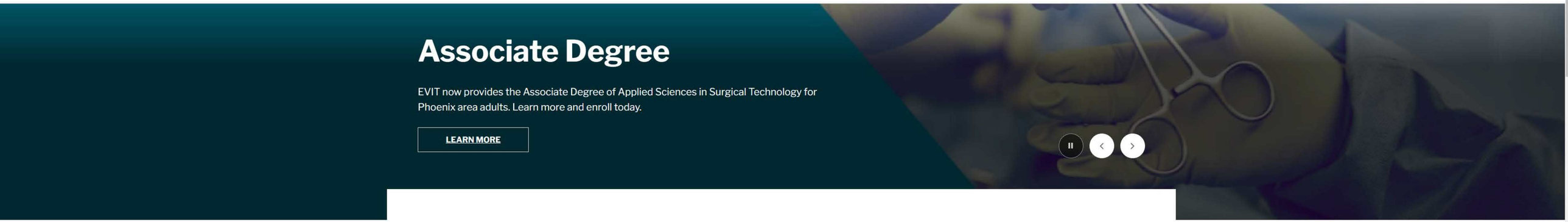
reviewing our processes and implementing additional safeguards to protect your information.

Please feel free to reach out to me with any questions or concerns at evit-notifications@evit.edu.

Sincerely,

Superintendent Dr. Chad Wilson

Exhibit 3



Associate Degree

EVIT now provides the Associate Degree of Applied Sciences in Surgical Technology for Phoenix area adults. Learn more and enroll today.

LEARN MORE

PROGRAMS | ASSOCIATE DEGREES | COURSE CATALOG | CALENDAR | SCHEDULE CAMPUS TOUR | MAKE ONLINE PAYMENTS | ADMISSIONS | WORK AT EVIT

Notice of January 2024 Data Breach

Mission Statement

To change lives by loving our students and serving our communities with a career and college preparatory training experience that produces a qualified workforce, meeting the market-driven needs of business and industry.

Notice of January 2024 Data Breach

The following contains important information about a recent cyber incident that potentially impacted the personal information of current and former students, faculty and parents of the East Valley Institute of Technology ("EVIT"). EVIT is a family, and we take the importance of the information our family entrusts to us very seriously. We are investigating the event, and we are reviewing and implementing additional safeguards to protect your information.

What Happened

On January 9, 2024, EVIT was the target of a cyber incident that involved unauthorized access to the network. This attack had a limited impact on our operations. We immediately took corrective steps to investigate the incident, secure our systems, report the incident to law enforcement, contain and remediate the threat, and notify potentially impacted individuals. To date, EVIT has not discovered any publication of EVIT data that contained sensitive information. However, given the possibility that sensitive information may have been compromised, EVIT engaged a third party to conduct a thorough review of all potentially impacted files. Given the number of potentially impacted files, this investigation concluded on June 4.

What Information was Involved

For individuals who may have been impacted by the breach, the categories of impacted personal information may include date of birth, social security number, student ID number, race/ethnicity, parent/guardian name, home phone number, email address, IEP/504 plan, grade, class lists, and course schedule. However, not all this data was potentially compromised for most individuals.

What are We Doing

We have implemented several measures to ensure that your information is protected from future unauthorized disclosures. EVIT has notified appropriate authorities, as well as provided email notification to all current and former students, staff, faculty, and parents.

Now that the impacted file investigation is completed, and potentially impacted individuals have been identified by name, EVIT is posting this website notice as it simultaneously diligently works to send individual notice to anyone identified as potentially impacted by the breach. All potentially impacted individuals are eligible to receive credit monitoring and other related services. Finally, EVIT engaged a third party to help EVIT with adding computer security protections and protocols to harden its network infrastructure and offer improved protections of your sensitive data from unauthorized access.

What You Can Do

To help protect your identity, we recommend that impacted individuals take immediate steps to protect themselves from further potential harm:

- Closely monitor your financial accounts. If your financial institutions permit you to notify them of a potential theft of your personal information, please do so.

- Place a credit freeze and/or fraud alert on your credit file. A fraud alert is a basic type of alert available to any consumer that tells creditors to contact you before they open any new accounts or change your existing accounts. A credit freeze, also knowns as a security freeze, helps restrict access to your credit report, which then makes it more difficult for other people to fraudulently open new accounts in your name. Call any one of the three major credit bureaus to request a credit freeze and/or fraud alert. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. But, for a credit freeze, you will need to notify each credit bureau individually.
- Equifax 800-685-1111
- Experian 888-397-3742
- TransUnionCorp 800-680-7289

  Please note there is no cost to place a credit freeze or fraud alert on your credit file, however, the credit bureaus may offer you additional products for a fee. If you elect to set up a credit freeze, you will be required to select a PIN to use when you are ready to un-freeze your credit or submit a legitimate application. More information about credit freezes and fraud alerts is available from the FTC at https://consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts (https://consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts)

Skip To Main Content

- File an identity theft report with the FTC at IdentityTheft.gov. Details regarding this program are available at: https://www.ftc.gov/news-events/topics/identity-theft/report-identity-theft (https://www.ftc.gov/news-events/topics/identity-theft/report-identity-theft).

- Even if you do not find any suspicious activity on your initial credit reports or accounts, the Federal Trade Commission (FTC) recommends checking your credit reports periodically. Reports may be obtained by visiting www.annualcreditreport.com or calling 877-322-8228. Checking your credit reports periodically can help you spot problems and address them quickly. Get a copy of the credit report; many creditors want the information to absolve you of fraudulent charges. Additional information about identity theft is available on the FTC's website at https://www.ftc.gov/idtheft (https://www.ftc.gov/idtheft).

For More Information For more information or if you have any questions about this incident, please contact us at evit-notifications@evit.edu (mailto:evit-notifications@evit.edu)