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)

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.