JacksonLewis

Jackson Lewis P.C.
666 Third Avenue
29th Floor
New York, NY 10017
(212) 545-4063
www.jacksonlewis.com

Damon W. Silver
Direct: (212) 545-4063
damon.silver@jacksonlewis.com

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

Re: Data Incident Notification[1]

April 5, 2024

Dear Sir or Madam:

We are writing to notify your office that Tiegerman ("the School") was the subject of a criminal cyberattack (the "Incident") on September 25, 2023. The School immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope and the identities of those the Incident may have affected.

Through its extensive investigation, the School determined that the Incident resulted in the encryption of certain files stored on the School's information systems. Although the School found no indications that the protected health information ("PHI") and/or personally identifiable information ("PII") stored in the encrypted files was subject to unauthorized access or acquisition, it nevertheless undertook the time- and resource-intensive steps of identifying that information and the individuals to whom it relates.

On or about January 4, 2024, the School determined that files containing PII related to three (3) Maryland residents may have been accessed by the bad actor. Out of an abundance of caution, and in accordance with applicable law, the School will provide notice on a rolling basis to the affected Maryland residents, in the form enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused.

As set forth in the enclosed letter, the School took a number of steps to mitigate the risk that the Incident would result in harm and to further bolster the School's data security program. Those steps include: isolating the affected systems and taking them offline; severing VPN connectivity to all remote locations; recovering impacted data from backups (after confirming integrity and cleanliness) to avoid disruption to student services and other business operations; restoring and rebuilding impacted servers; deploying a round-the-clock endpoint detection and response solution; conducting dark web

[1] Please note that Tiegerman does not, by providing this letter, agree to the jurisdiction of the State of Maryland, nor waive its right to challenge jurisdiction in any subsequent actions.

monitoring; conducting round-the-clock DMARC monitoring; and conducting automated recurring PEN and PII scans. The School also upgraded its on-premises server's active directory to utilize DUO MFA.

We will continue to monitor this situation and will update you on any significant developments. If you require any additional information on this matter, please contact me.

Sincerely,

JACKSON LEWIS, P.C.

/s/ Damon W. Silver

Damon W. Silver

cc: Melissa Pascualini (Jackson Lewis P.C.)

4853-8421-8016, v. 3

EXHIBIT A

TIEGERMAN

TEACHING THE EXTRAORDINARY

EXPERTS IN LANGUAGE AND COMMUNICATION DEVELOPMENT

To Enroll, Please Visit:
https://members.excelsiorenroll.com/TS/

March 1, 2024

Notice of Data Breach

To Whom It May Concern:

What Happened

We are writing to notify you that Tiegerman ("the School") was the subject of a criminal cyberattack ("the Incident") on September 25, 2023. The School immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope and the identities of those the Incident may have affected.

Through its extensive investigation, the School determined that the Incident resulted in the encryption of certain files stored on the School's information systems. Although the School found no indications that the protected health information ("PHI") and/or personally identifiable information ("PII") stored in the encrypted files was subject to unauthorized access or acquisition, it nevertheless undertook the time- and resource-intensive steps of identifying that information and the individuals to whom it relates. We completed this process on or about January 4, 2024.

What Information May Have Been Involved

The impacted files may have contained your name, along with your address, date of birth, social security number, driver's license number, government ID number, financial account information, health insurance information, medical information, biometric information, email address, or username/password information.

What We Are Doing

Out of an abundance of caution, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we are offering identify theft protection services through Norton LifeLock Benefit Solutions for six months.

We encourage you to contact Norton LifeLock Benefit Solutions with any questions and to enroll in the free identity protection services by going to https://members.excelsiorenroll.com/TS/ and following the instructions to complete the online enrollment. A comprehensive overview of this benefit can be viewed at the following website: https://www.gendigital.com/us/en/partner/employee-benefits/essential-plan/

Please note that the deadline to enroll is **May 31, 2024.**

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. In addition to those described above, the School took a number of steps to mitigate the risk that the Incident would result in harm and to further

bolster the School's data security program. Those steps include: isolating the affected systems and taking them offline; severing VPN connectivity to all remote locations; recovering impacted data from backups (after confirming integrity and cleanliness) to avoid disruption to student services and other business operations; restoring and rebuilding impacted servers; deploying a round-the-clock endpoint detection and response solution; conducting dark web monitoring; conducting round-the-clock DMARC monitoring; and conducting automated recurring PEN and PII scans. The School also upgraded its on-premises server's active directory to utilize DUO MFA.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

We apologize for any inconvenience this Incident may cause you. If you have additional questions, please call our dedicated assistance line at 1-888-541-2426, Monday through Friday from 9:00 a.m. to 9:00 p.m.

Sincerely,

Dr. E Tiegerman

Dr. Ellenmorris Tiegerman
CEO
Tiegerman

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

TIEGERMAN

TEACHING THE EXTRAORDINARY

EXPERTS IN LANGUAGE AND COMMUNICATION DEVELOPMENT

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

   - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
   - You can also receive information from these agencies about avoiding identity theft, such as by placing a "security freeze" on your credit accounts.
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
Consumer Fraud Division	Experian Security Assistance	Consumer Relations & Fraud
P.O. Box 740256	P.O. Box 9554	Victim Assistance
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 2000
800-525-6285	888-397-3742	Chester, PA 19016
securitymonitoring@equifax.com	businessrecordsvictimassistance@experian.com	800-372-8391
		databreach@Transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a "security freeze" on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

   Federal Trade Commission
   Consumer Response Center 600
   Pennsylvania Avenue NW
   Washington, DC 20580

4. *For 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.

5. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the

Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

6. *For New York Residents*: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

TIEGERMAN

TEACHING THE EXTRAORDINARY

EXPERTS IN LANGUAGE AND COMMUNICATION DEVELOPMENT

To Enroll, Please Visit:
https://members.excelsiorenroll.com/TS/

March 1, 2024

Notice of Data Breach

To Whom It May Concern:

What Happened

We are writing to notify you that Tiegerman ("the School") was the subject of a criminal cyberattack ("the Incident") on September 25, 2023. The School immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope and the identities of those the Incident may have affected.

Through its extensive investigation, the School determined that the Incident resulted in the encryption of certain files stored on the School's information systems. Although the School found no indications that the protected health information ("PHI") and/or personally identifiable information ("PII") stored in the encrypted files was subject to unauthorized access or acquisition, it nevertheless undertook the time- and resource-intensive steps of identifying that information and the individuals to whom it relates. We completed this process on or about January 4, 2024. We have not found any evidence that your information was misused as a result of the Incident.

What Information Was Involved

The impacted files may have contained your name, along with your address, date of birth, social security number, health insurance information, or medical information.

What We Are Doing

Out of an abundance of caution, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we are offering identify theft protection services through Norton LifeLock Benefit Solutions for six months.

We encourage you to contact Norton LifeLock Benefit Solutions with any questions and to enroll in the free identity protection services by going to https://members.excelsiorenroll.com/TS/ and following the instructions to complete the online enrollment. A comprehensive overview of this benefit can be viewed at the following website: https://www.gendigital.com/us/en/partner/employee-benefits/essential-plan/.

Please note that the deadline to enroll is **May 31, 2024.**

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. In addition to those described above, the School took a number of steps to mitigate the risk that the Incident would result in harm and to further bolster the School's data security program. Those steps include: isolating the affected systems and taking them offline; severing VPN connectivity to all remote locations; recovering impacted data from backups (after confirming integrity and cleanliness) to avoid

disruption to student services and other business operations; restoring and rebuilding impacted servers; deploying a round-the-clock endpoint detection and response solution; conducting dark web monitoring; conducting round-the-clock DMARC monitoring; and conducting automated recurring PEN and PII scans. The School also upgraded its on-premises server's active directory to utilize DUO MFA.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

We apologize for any inconvenience this Incident may cause you. If you have additional questions, please call our dedicated assistance line at 1-888-541-2426, Monday through Friday from 9:00 a.m. to 9:00 p.m.

Sincerely,

Dr. E Tiegerman

Dr. Ellenmorris Tiegerman
CEO
Tiegerman

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

TIEGERMAN

TEACHING THE EXTRAORDINARY

EXPERTS IN LANGUAGE AND COMMUNICATION DEVELOPMENT

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

   - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
   - You can also receive information from these agencies about avoiding identity theft, such as by placing a "security freeze" on your credit accounts.
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
Consumer Fraud Division	Experian Security Assistance	Consumer Relations & Fraud
P.O. Box 740256	P.O. Box 9554	Victim Assistance
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 2000
800-525-6285	888-397-3742	Chester, PA 19016
securitymonitoring@equifax.com	businessrecordsvictimassistance@experian.com	800-372-8391
		databreach@Transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a "security freeze" on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

   Federal Trade Commission
   Consumer Response Center 600
   Pennsylvania Avenue NW
   Washington, DC 20580

4. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

5. *For New York Residents*: You may also contact the following state agencies for information regarding security breach

response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

TIEGERMAN

TEACHING THE EXTRAORDINARY

EXPERTS IN LANGUAGE AND COMMUNICATION DEVELOPMENT

To Enroll, Please Visit:
https://members.excelsiorenroll.com/TS/

March 1, 2024

Notice of Data Breach

To Whom It May Concern:

What Happened

We are writing to notify you that Tiegerman ("the School") was the subject of a criminal cyberattack ("the Incident") on September 25, 2023. The School immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope and the identities of those the Incident may have affected.

Through its extensive investigation, the School determined that the Incident resulted in the encryption of certain files stored on the School's information systems. Although the School found no indications that the protected health information ("PHI") and/or personally identifiable information ("PII") stored in the encrypted files was subject to unauthorized access or acquisition, it nevertheless undertook the time- and resource-intensive steps of identifying that information and the individuals to whom it relates. We completed this process on or about January 4, 2024. We have not found any evidence that your information was misused as a result of the Incident.

What Information Was Involved

The impacted files may have contained your name, along with your address, date of birth, social security number, health insurance information, or email address.

What We Are Doing

Out of an abundance of caution, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we are offering identify theft protection services through Norton LifeLock Benefit Solutions for six months.

We encourage you to contact Norton LifeLock Benefit Solutions with any questions and to enroll in the free identity protection services by going to https://members.excelsiorenroll.com/TS/ and following the instructions to complete the online enrollment. A comprehensive overview of this benefit can be viewed at the following website: https://www.gendigital.com/us/en/partner/employee-benefits/essential-plan/

Please note that the deadline to enroll is **May 31, 2024.**

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. In addition to those described above, the School took a number of steps to mitigate the risk that the Incident would result in harm and to further bolster the School's data security program. Those steps include: isolating the affected systems and taking them offline; severing VPN connectivity to all remote locations; recovering impacted data from backups (after confirming integrity and cleanliness) to avoid

disruption to student services and other business operations; restoring and rebuilding impacted servers; deploying a round-the-clock endpoint detection and response solution; conducting dark web monitoring; conducting round-the-clock DMARC monitoring; and conducting automated recurring PEN and PII scans. The School also upgraded its on-premises server's active directory to utilize DUO MFA.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

We apologize for any inconvenience this Incident may cause you. If you have additional questions, please call our dedicated assistance line at 1-888-541-2426, Monday through Friday from 9:00 a.m. to 9:00 p.m.

Sincerely,

Dr. E Tiegerman

Dr. Ellenmorris Tiegerman
CEO
Tiegerman

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

   - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
   - You can also receive information from these agencies about avoiding identity theft, such as by placing a "security freeze" on your credit accounts.
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
Consumer Fraud Division	Experian Security Assistance	Consumer Relations & Fraud
P.O. Box 740256	P.O. Box 9554	Victim Assistance
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 2000
800-525-6285	888-397-3742	Chester, PA 19016
securitymonitoring@equifax.com	businessrecordsvictimassistance@experian.com	800-372-8391
		databreach@Transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a "security freeze" on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

   Federal Trade Commission
   Consumer Response Center 600
   Pennsylvania Avenue NW
   Washington, DC 20580

4. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

5. *For New York Residents*: You may also contact the following state agencies for information regarding security breach

response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.