Mastery Schools

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

VIA U.S. MAIL

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>,

We are writing to inform you that Mastery Charter High School ("Mastery Schools" or "we") experienced a cybersecurity incident in September 2024 (the "Incident") that potentially involved your personal information ("Information"). This letter provides you with information about this Incident, our response, steps you can take, and if necessary, information on where to direct your questions. Additionally, although we are unaware of any identity theft or fraud in relation to the Incident, as a precaution we have also provided steps you can take to protect your Information, including the ability to enroll in credit monitoring services that we are offering free of charge for twenty-four (24) months.

What Happened?

As you may already be aware, on September 15, 2024, Mastery Schools detected suspicious activity attributed to an unauthorized actor that affected some of our systems. As soon as we discovered this suspicious activity, we immediately took steps to investigate, contain, and remediate the situation, including shutting down systems proactively, reporting the matter to federal law enforcement, and engaging experienced cybersecurity professionals to assist. Our investigation determined your Information was potentially affected. There is currently no evidence of identity theft or fraud in connection with the Incident.

What Information Was Involved?

There is a possibility that the following types of Information may have been impacted as a result of this Incident: name, Social Security number and/or taxpayer identification number, financial account information, and health insurance information. Note that this describes general categories of information identified as present within the affected systems during the Incident and includes categories that are not relevant to each individual whose Information may have been present.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further strengthen the security of our systems and practices, including expanding our current use of multifactor authentication and implementing additional endpoint detection and response monitoring. After determining the scope of unauthorized activity, we immediately began analyzing the information involved to confirm the identities of potentially affected individuals. We worked with leading privacy and security experts to aid in our investigation and response, and we are reporting this Incident to relevant government agencies.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twenty-four (24) months. While identity restoration assistance is immediately available to you, we also encourage you to activate the complimentary twenty-four (24) month membership to Experian IdentityWorks and its fraud detection tools. To start monitoring your personal information, please follow the steps below:

- You must **enroll by <<Enrollment Deadline>>** no later than 5:59 pm Central Time (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **<<Activation Code>>**.

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this Incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 931-7577 by <<Enrollment Deadline>>. Be prepared to provide the engagement number **<<Engagement Number>>** as proof of eligibility for the Identity Restoration services by Experian.

What Can You Do?

In addition to enrolling in credit monitoring services, it is always recommended that you remain vigilant, regularly monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of Information in our care seriously. If you have additional questions, you may call the toll-free assistance line for our dedicated call center at 888-458-9798 Monday through Friday from 9:00 a.m. to 9:00 p.m. (excluding U.S. holidays).

Sincerely,

Dr. Joel Boyd
CEO
Mastery Schools

Encl.

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Massachusetts residents: You may obtain one (1) or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. 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.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

For Massachusetts Residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. You have the right to obtain a police report if you are a victim of identity theft.