

August 11, 2021

[Address]

Dear [Name],

I am writing to provide you notice of a data security event that we believe affected the security of some of your personal information. On July 20, 2021, we provided preliminary notice of this event to current employees, parents, and alumnae whose current email addresses are on file with us.

### **What Happened?**

On July 12, 2021, hackers illegally accessed Emma Willard's computer network as part of a ransomware attack. We took immediate steps to respond to this attack and reduce the threat to your personal information. Steps we have taken include disabling the device used by the attackers to access our network, as well as hiring cybersecurity experts to scan our systems to ensure that the attackers were fully expelled from our network. We also are working to make improvements and enhancements to our security systems to reduce the risk of a similar attack in the future.

### **What Information Was Involved?**

On July 14, 2021, we determined the hackers were able to steal some information before they were expelled from our network. We have reason to believe that documents containing your name, address, social security number and other personal information were among the documents accessed and stolen by the hackers during the attack.

### **What Can You Do?**

Although we believe the hackers' goal was to encrypt Emma Willard's computer systems as part of a ransomware attack, we cannot rule out the possibility that the hackers may use or disclose your personal information. To help protect you, we are offering twelve (12) months of credit monitoring and identity theft protection services through Kroll, free of charge.

The attached information packet includes information on how you can take advantage of the free credit monitoring and identity theft protection offer. The attached information packet also contains information on other resources and steps you can take to protect yourself.

We understand this situation is frustrating and that you may have questions regarding this incident, including questions about what specific personal information of yours may have been accessed or copied. Should you have any questions or concerns, please do not hesitate to contact our Data Protection Officer, Judith Curry, at [dpo@emmawillard.com](mailto:dpo@emmawillard.com) or (518) 833-1316 at your earliest convenience.

Sincerely,

Jenny Rao, Head of School

## Credit Monitoring and Identity Theft Services

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.<sup>1</sup>

### How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by <DATE>. Your Activation Code will not work after this date.
2. Visit [Enroll.krollmonitoring.com/redeem](https://enroll.krollmonitoring.com/redeem) to activate your identity monitoring services.
3. Provide Your Activation Code: <<Enter Activation Code>> and Your Verification ID: <ID>

### Take Advantage of Your Identity Monitoring Services

**Single Bureau Credit Monitoring.** You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

**Web Watcher.** Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

**Public Persona.** Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

**Quick Cash Scan.** Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

**\$1 Million Identity Fraud Loss Reimbursement.** Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

**Fraud Consultation.** You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Identity Theft Restoration.** If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

---

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file

## **Steps You Can Take to Protect Your Personal Information**

When dealing with a data security incident, you should remain vigilant by reviewing your account statements and credit reports. If you detect suspicious activity, you should promptly notify the financial institution or company that maintains the account. You also should promptly report any fraudulent activity or suspected identity theft to proper law enforcement authorities, your state's attorney general, and/or the Federal Trade Commission.

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting: <https://www.annualcreditreport.com>, calling toll-free 1-877-322-8228, or by mailing an annual credit report request form to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can find a copy of the request form at: <https://www.annualcreditreport.com>.

You may also wish to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three major reporting agencies: TransUnion, by visiting <https://www.transunion.com/fraud-alerts>, calling 1-800-680-7289, or mailing to P.O. Box 2000, Chester, PA 19016; Experian, by visiting <https://www.experian.com/fraud/center.html>, calling 1-888-397-3742, or mailing to P.O. Box 9554, Allen, TX 75013; and Equifax, by visiting <https://www.equifax.com/personal/credit-report-services/>, calling 1-800-525-6285, or mailing to P.O. Box 105069, Atlanta, GA 30374. Ask the company to put a fraud alert on your credit line and confirm that the company you called will contact the other two. Additional information is available at: <https://www.annualcreditreport.com>.

You also have a right to place a freeze on your credit file, which will prohibit a consumer credit reporting agency from accessing or releasing information in your credit report without your express consent. It will also prevent new credit from being opened in your name without the use of a PIN number that is issued to you. However, using a credit freeze may delay or interfere with your ability to obtain credit. Credit freezes are free of charge and will last until temporary lifted or permanently removed. To place a credit freeze, please contact each major reporting agency listed above. Additional information is available at: <https://www.consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts>.

For additional information on how to avoid identity theft, the Federal Trade Commission provides a comprehensive guide to help you guard against, identify, and respond to identity theft, a copy of which may be found at: [https://www.consumer.ftc.gov/articles/pdf-0009\\_identitytheft\\_a\\_recovery\\_plan.pdf](https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf). For more information, please visit <https://www.identitytheft.gov> or call 1-877-ID-THEFT (1-877-438-4338).

If you are a New York resident, you may also wish to review information provided by the New York Attorney General at <https://ag.ny.gov/consumer-frauds-bureau/identity-theft> or by calling 1-800-771-7755