## Appendix

National Educational Music Company's ("NEMC") vendor, CommerceV3, experienced a data security incident that involved Maine residents' information.

CommerceV3 provides an e-commerce platform that NEMC uses to process payment card information when an order is placed on NEMC's website. CommerceV3 learned that an unauthorized party accessed CommerceV3's systems between November 24, 2021 and December 14, 2022. Upon learning of this issue, CommerceV3 conducted a forensic investigation with third-party cybersecurity experts to assess whether cardholder data was involved in the incident. During this forensic investigation, CommerceV3 also worked alongside the major card brands and banks.

On May 3, 2023, CommerceV3 discovered that cardholder data it collected on NEMC's behalf was potentially accessed or acquired by an unauthorized party as a result of the incident. On June 7, 2023, CommerceV3 notified NEMC of this incident. CommerceV3 and NEMC worked to identify the individuals whose payment card information was involved in the incident and determined that it involved the name, email address, billing address, payment card number, card expiration date, and card verification code (CVV) for seven (7) Maine residents.

On August 2, 2023, NEMC mailed notification letters via United States Postal Service First-Class mail to the individuals whose information was involved, including the Maine residents. A copy of the notification is enclosed. NEMC has established a dedicated call center for individuals to call with questions about the incident.

NEMC understands that to help prevent a similar incident from occurring in the future, CommerceV3 has implemented additional security measures.

1110 Centennial Ave
STE 2
Piscataway, NJ 08854

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

August 2, 2023

Dear <<Name 1>> <<Name 2>>:

National Educational Music Company ("NEMC") is committed to ensuring the privacy and security of your personal information. We write to notify you of an incident that impacted our third-party e-commerce platform, CommerceV3, which may have involved some of your payment card information. This letter explains the incident, the measures we have taken, and the steps you can take to protect your personal information.

***What Happened?*** CommerceV3 provides the e-commerce platform NEMC uses to process payment card information when an order is placed on our website to purchase an instrument. This incident occurred at CommerceV3 and not at NEMC. CommerceV3 conducted a forensic investigation with the assistance of a cybersecurity firm and worked alongside the major card brands and banks during its investigation. CommerceV3 determined that an unauthorized party accessed its systems between November 24, 2021 and December 14, 2022. NEMC uses a different platform to process rental transactions related to its instrument rental program which was not involved.

***What Information Was Involved?*** On May 3, 2023, CommerceV3 determined that NEMC customer cardholder data was potentially accessed or acquired by the unauthorized party as a result of the incident. The information included your name, email address, billing address, payment card number, card expiration date, and the card verification code (CVV) for the card you used on NEMC's site between November 24, 2021 and December 14, 2022.

***What We Are Doing.*** NEMC worked with CommerceV3 to identify the individuals whose payment card information was involved. In response to the incident, CommerceV3 has implemented additional security measures designed to protect the privacy of our customers.

***What You Can Do.*** We encourage you to remain vigilant by reviewing your payment card account statement. If you see charges or activity you did not authorize, contact your payment card company immediately. The telephone number is on the back of your payment card. Please review the following pages for more information on ways to protect your information.

***For More Information.*** If you have any further questions regarding this incident, please contact 1-800-939-4170. This response line is available Monday through Friday, 9:00 am to 9:00 pm, Eastern Time.

Sincerely,

Kenneth P. Maehl
Chief Operations Officer, Vice President

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

**Fraud Alerts and Credit or Security Freezes:**
***Fraud Alerts:*** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

***Credit or Security Freezes:*** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

***Additional information for residents of the following states:***

**Connecticut:** You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

**District of Columbia:** You may contact and obtain information from your attorney general at: *Office of the Attorney General for the District of Columbia*, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

**Iowa**: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft at: *Office of the Attorney General of Iowa, Consumer Protection Division*, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

**Maryland:** You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

**New York:** You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

**Oregon**: You may obtain information about preventing identity theft from the Oregon Attorney General's Office at: *Oregon Department of Justice*, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active-duty military personnel have additional rights.