

&lt;&lt;Date&gt;&gt; (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

## &lt;&lt;b2b\_text\_4 (NOTICE OF DATA SECURITY INCIDENT / NOTICE OF DATA BREACH

Dear &lt;&lt;First\_Name&gt;&gt; &lt;&lt;Last\_Name&gt;&gt;,

Millyard Bank (the “Bank”) is writing to inform you of a recent incident involving a file transfer tool used by one of our third party vendors that may have involved some of your personal information. The Bank uses this vendor, a Fortune 500 company, for certain banking and payment technology solutions and your information was provided to the vendor to perform these services. According to the vendor, there is no evidence that any of your data has been made publicly available or otherwise published to any unauthorized websites. This letter includes information about the incident, details on how to enroll in our offer of free identity protection services, including credit monitoring, and additional measures you can take to help you protect your information should you feel it appropriate to do so.

**What Happened?**

On May 31, 2023, Progress Software, our vendor’s software service provider, disclosed a vulnerability in its MOVEit Transfer tool. Our vendor uses the MOVEit Transfer tool to transfer data files. According to our vendor, it took immediate steps to assess and respond to the situation, including swift patching of its production systems and heightened monitoring of the MOVEit Transfer environment. Our vendor also reported that it quickly activated its security response protocol and team, which includes a dedicated team of cybersecurity and forensics experts, alerted law enforcement, and began an investigation and review of potentially impacted data.

Our vendor stated that its investigation to date has identified unauthorized activity in the relevant MOVEit Transfer environment between May 27 to 31, 2023, which was before Progress Software publicly disclosed the existence of this vulnerability. During that time, unauthorized actors obtained files transferred via MOVEit Transfer that may have contained some of your personal information. The Bank does not use the MOVEit Transfer tool in its direct business operations and this incident did not have any impact on the Bank’s internal computer network.

**What Information Was Involved?**

The personal information that our vendor determined to have been potentially accessed may have included <<b2b\_text\_3 (your name, impacted data elements)>>.

**What We Are Doing.**

The Bank wanted to notify you of this incident, provide you the information regarding the incident that we’ve received from our vendor, and assure you that we are taking it seriously. To help prevent something like this happening again, our vendor represented that it has remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider’s guidelines, and also mobilized a technical response team to examine the relevant MOVEit Transfer systems and ensure that there were no further vulnerabilities.

**What You Can Do.**

We take the protection and proper use of personal information very seriously. To help protect your identity, we have arranged for you to receive a free identity monitoring service through Kroll for two years. 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, fraud consultation, and identity theft restoration. You must enroll in this identity monitoring service on your own as the Bank cannot do so on your behalf.

For more information on identity theft prevention, including instructions on how to activate your identity monitoring, as well as some additional steps you can take for your protection, please review Attachments A and B that follow this letter.

Regardless of whether you elect to activate the identity monitoring service, we strongly encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing and monitoring all of your credit history to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statements and notify us or any of your financial institutions if you suspect any unauthorized activity. Additional steps and resources are available in the accompanying **Attachment B – Additional Steps You Can Take**. We encourage you to read and follow these steps as well.

**For More Information.**

If you have any questions about this notice or the incident, please feel free to contact us directly at (866) 731-2256, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. We apologize for any concern or inconvenience this may cause you.

Sincerely,

<<b2b\_text\_1 (Data Owner Name)>>

## **ATTACHMENT A**

Visit <https://2023monitoring.kroll.com> to activate and take advantage of your identity monitoring services.

You have until *<<b2b\_text\_6 (Activation Deadline)>>* to activate your identity monitoring services.

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](http://info.krollmonitoring.com).



### **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services from Kroll:

#### **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 will be able to help you determine if it is an indicator of identity theft.

#### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

## **ATTACHMENT B**

### **ADDITIONAL STEPS YOU CAN TAKE**

To help protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your state's Attorney General, or the Federal Trade Commission.

#### **INFORMATION ON OBTAINING A FREE CREDIT REPORT**

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free (877) 322-8228.

#### **INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK**

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three consumer reporting agencies below:

##### **Equifax:**

Equifax Information Services LLC  
P.O. Box 105788  
Atlanta, GA 30348  
1-888-298-0045  
[www.equifax.com](http://www.equifax.com)

##### **Experian:**

Credit Fraud Center  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

##### **TransUnion:**

Fraud Victim Assistance Department  
P.O. Box 2000  
Chester, PA 19022-2000  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)

**Fraud Alert:** Consider contacting the three major consumer reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might help protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major consumer reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days but can be renewed.

**Credit Freeze:** A credit freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

Placing a credit freeze is free. To place a credit freeze, contact all three consumer reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

**Credit Lock:** Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three consumer reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to help protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-IDTHEFT; or [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above.

### ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

**District of Columbia Residents:** The Attorney General can be contacted at the Office of the Attorney General, 441 4th Street NW, Washington, DC 20001; (202) 727-3400; or <https://oag.dc.gov/>.

**Maryland Residents:** The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or <http://www.oag.state.md.us>.

**Massachusetts Residents:** Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**North Carolina Residents:** The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or <http://www.ncdoj.gov>.

**New Mexico Residents:** You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or [www.ftc.gov](http://www.ftc.gov).

**Rhode Island Residents:** The Attorney General can be contacted at (401) 274-4400 or <http://www.riag.ri.gov/>. You may also file a police report by contacting local or state law enforcement agencies.