



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Colin D. Scanlon
Office: (267) 930-4259
Fax: (267) 930-4771
Email: cscanlon@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

September 8, 2023

VIA E-MAIL

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

Re: Notice of Data Event

To Whom it May Concern:

We represent Northfield Bank located at 581 Main Street, Suite 810, Woodbridge, NJ 07095 and are writing to notify your office of a third-party event that may affect the security of certain personal information relating to two (2) Maryland residents. This notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Northfield Bank does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On August 4, 2023, Northfield Bank was initially notified by a third-party vendor of an incident related to vulnerabilities discovered in the vendor's MOVEit Transfer application. The vendor uses MOVEit software to support services being provided to the bank. Northfield Bank understands the third-party vendor's MOVEit Transfer application was exploited between May 27 to May 31, 2023 and that certain Northfield Bank customer information being stored within the application was subject to unauthorized access or acquisition. On August 8, 2023, the third-party vendor provided Northfield Bank with files containing a list of potentially affected individuals, the types of data associated with each individual, and the documents that were subject to unauthorized access. Upon receiving the same, Northfield Bank commenced a detailed review of the files to confirm the information reported by the third-party vendor. This review concluded by Northfield Bank on August 28, 2023 (subject to change of address and deduplication processes) and the information that could have been subject to unauthorized access includes name, address, account number, Social Security number and/or online banking username. On August 30, 2023, the third-party vendor provided Northfield Bank with

additional files that include a list of potentially affected individuals, the types of data associated with each individual, and the documents that were subject to unauthorized access. This review is ongoing.

Notice to Maryland Residents

On September 7, 2023, Northfield Bank began providing written notice of this event to two (2) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Northfield Bank continues to review the data impacted and may supplement this notice if additional residents of Maryland are determined to be impacted.

Other Steps Taken and To Be Taken

Upon being notified of the incident, Northfield Bank moved quickly to investigate, gather as much information from the vendor as possible and notify potentially affected individuals. Northfield Bank, through the third-party vendor, is providing individuals whose personal information was potentially impacted by this event access to credit monitoring services for two (2) years through Kroll at no cost to the individuals.

Additionally, Northfield Bank is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to Northfield Bank or any other of their financial institutions. Northfield Bank is providing individuals with information on how to place fraud alerts, credit freezes, and credit lock on their credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Northfield Bank is also providing notice of this incident to relevant state and federal regulators.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4259.

Very truly yours,

Colin D. Scanlon of
MULLEN COUGHLIN LLC

CDS/cob

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (NOTICE OF [DATA SECURITY EVENT / DATA BREACH])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are contacting you to provide important information regarding a data security event which occurred at a third-party vendor whom Northfield Bank utilizes to provide certain products and services to you. Please note that the event had no impact on Northfield Bank's systems and is not the result of any activities at Northfield Bank.

What Happened?

On August 4, 2023, we were notified by our vendor of an incident which occurred during the period May 27 to May 31, 2023, related to vulnerabilities discovered in the MOVEit Transfer application. The application is offered by Progress Software Corporation and is a commonly used Managed File Transfer (MFT) software supporting file transfer activities of thousands of organizations around the world. The MOVEit software was used by our vendor to support its services to Northfield Bank. Upon notification from our vendor of the event, Northfield Bank began an investigation to evaluate the scope and nature of the event.

Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about it, our response, and additional measures you can take to help protect your information.

What Information Was Involved?

We conducted a review of the contents of files provided by our vendor, and determined one or more of the files contained the following information related to you: your name, account number, Social Security number and/or online banking username. Please note that **no** password information was present.

What We Are Doing

Upon learning of this incident, we began working with our vendor to monitor their investigation and remediation, and identify customers affected. Our vendor mobilized a technical response team to examine the relevant MOVEit Transfer systems to ensure that there were no further vulnerabilities. Our vendor has advised us that they have also remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider's guidelines. We have engaged cyber security specialists to assist us in monitoring their investigation and remediation.

What You Can Do

Our vendor is offering for a period of two years complimentary identity monitoring and restoration services through Kroll, a global leader in risk mitigation and response.

For more information on identity theft protection, including instructions on how to activate the monitoring and restoration services, please review Attachments A and B that follow this letter.

We recommend that you remain vigilant and regularly review and monitor all of your credit history to guard against any unauthorized transactions or activities. We also recommend that you monitor your account statements and notify us or any other of your financial institutions if you suspect any unauthorized activity.

For More Information

If you have any questions about this notice or the event, please feel free to contact Kroll at [\[TFN\]](#), Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Northfield Bank

ATTACHMENT A

Visit <https://enroll.krollmonitoring.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.

Membership Number: <<Membership Number (s_n)>>

For more information about Kroll and your Identity Monitoring services, you can visit 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.

\$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 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 or call toll-free (877) 322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

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

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
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 1-877-382-4357; or www.consumer.gov/idtheft.

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.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or <https://www.marylandattorneygeneral.gov/>.

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 276999001; (919) 716-6400; or <http://www.ncdoj.gov>.

New York Residents: The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Colin Scanlon
Office: (267) 930-4259
Fax: (267) 930-4771
Email: cscanlon@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

October 2, 2023

VIA E-MAIL

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

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Northfield Bank located at 581 Main Street, Suite 810, Woodbridge, NJ 07095. We are writing to supplement our September 7, 2023 notification to your office of a third party event that may affect the security of certain personal information relating to an additional four (4) Maryland residents on behalf of Northfield Bank. Our previous notification to your office is attached as ***Exhibit AA***. By providing this notice, Northfield Bank does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On August 4, 2023, Northfield Bank was initially notified by a third-party vendor of an incident related to vulnerabilities discovered in the vendor's MOVEit Transfer application. The vendor uses MOVEit software to support services being provided to the bank. Northfield Bank understands the third-party vendor's MOVEit Transfer application was exploited between May 27 to May 31, 2023 and that certain Northfield Bank customer information being stored within the application was subject to unauthorized access or acquisition. On August 8, 2023, the third-party vendor provided Northfield Bank with files containing a list of potentially affected individuals, the types of data associated with each individual, and the documents that were subject to unauthorized access. Upon receiving the same, Northfield Bank commenced a detailed review of the files to confirm the information reported by the third-party vendor. This review concluded by Northfield Bank on August 28, 2023 (subject to change of address and deduplication processes) and the information that could have been subject to unauthorized access includes name, address, account number, Social Security number and/or online banking username. On August 30, 2023, the third-party vendor provided Northfield Bank with additional files containing a list of potentially affected individuals, the types of data associated with each individual, and the documents that were subject to unauthorized access. Northfield Bank continued to review the impacted data to determine if there were any additional individuals impacted by this event. Northfield Bank completed this review on September 14, 2023 (subject to change

of address and deduplication processes), and determined that additional residents of Maryland may have been impacted. The information that could have been subject to unauthorized access is same as noted above.

Notice to Maryland Residents

As previously indicated, Northfield Bank began mailing notice letters to potentially affected individuals on September 7, 2023. On September 25, 2023, Northfield Bank mailed notice letters to an additional four (4) Maryland residents. To date, Northfield Bank provided written notice to a total of six (6) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit BB***. Northfield Bank does not intend to issue additional notices in relation to this event.

Other Steps Taken and To Be Taken

Upon being notified of the incident, Northfield Bank moved quickly to investigate, gather as much information from the vendor as possible and notify potentially affected individuals. Northfield Bank, through the third-party vendor, is providing individuals whose personal information was potentially impacted by this event access to credit monitoring services for two (2) years through Kroll at no cost to the individuals.

Additionally, Northfield Bank is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to Northfield Bank or any other of their financial institutions. Northfield Bank is providing individuals with information on how to place fraud alerts, credit freezes, and credit lock on their credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Northfield Bank is also providing notice of this incident to relevant state and federal regulators.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4259.

Very truly yours,

Colin Scanlon of
MULLEN COUGHLIN LLC

CDS/bld
Enclosure

EXHIBIT AA

Dorothy Petry

From: Courtney Malloy
Sent: Friday, September 8, 2023 3:39 PM
To: idtheft@oag.state.md.us
Cc: Colin Scanlon; Christy O'Brian; Kelsey Hutchinson; Dorothy Petry; Courtney Malloy
Subject: Northfield Bank – Notice of Data Event – MD
Attachments: Northfield Bank - Notice of Data Event - MD.pdf

To Whom It May Concern,

Please see the attached for notice of data event.

Thank you,

Courtney Malloy

Attorney

Mullen Coughlin LLC

426 W. Lancaster Avenue, Suite 200

Devon, PA 19333

(267) 930-6738 - Office

(610) 389-7558 - Mobile

cmalloy@mullen.law

<https://www.mullen.law/>

This email may be an attorney-client communication or otherwise confidential and privileged. If you are not the intended recipient, or received it in error, do not review or copy. Please immediately notify the sender and permanently delete/destroy the email and attachments.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Colin D. Scanlon
Office: (267) 930-4259
Fax: (267) 930-4771
Email: cscanlon@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

September 8, 2023

VIA E-MAIL

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

Re: Notice of Data Event

To Whom it May Concern:

We represent Northfield Bank located at 581 Main Street, Suite 810, Woodbridge, NJ 07095 and are writing to notify your office of a third-party event that may affect the security of certain personal information relating to two (2) Maryland residents. This notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Northfield Bank does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On August 4, 2023, Northfield Bank was initially notified by a third-party vendor of an incident related to vulnerabilities discovered in the vendor's MOVEit Transfer application. The vendor uses MOVEit software to support services being provided to the bank. Northfield Bank understands the third-party vendor's MOVEit Transfer application was exploited between May 27 to May 31, 2023 and that certain Northfield Bank customer information being stored within the application was subject to unauthorized access or acquisition. On August 8, 2023, the third-party vendor provided Northfield Bank with files containing a list of potentially affected individuals, the types of data associated with each individual, and the documents that were subject to unauthorized access. Upon receiving the same, Northfield Bank commenced a detailed review of the files to confirm the information reported by the third-party vendor. This review concluded by Northfield Bank on August 28, 2023 (subject to change of address and deduplication processes) and the information that could have been subject to unauthorized access includes name, address, account number, Social Security number and/or online banking username. On August 30, 2023, the third-party vendor provided Northfield Bank with

additional files that include a list of potentially affected individuals, the types of data associated with each individual, and the documents that were subject to unauthorized access. This review is ongoing.

Notice to Maryland Residents

On September 7, 2023, Northfield Bank began providing written notice of this event to two (2) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Northfield Bank continues to review the data impacted and may supplement this notice if additional residents of Maryland are determined to be impacted.

Other Steps Taken and To Be Taken

Upon being notified of the incident, Northfield Bank moved quickly to investigate, gather as much information from the vendor as possible and notify potentially affected individuals. Northfield Bank, through the third-party vendor, is providing individuals whose personal information was potentially impacted by this event access to credit monitoring services for two (2) years through Kroll at no cost to the individuals.

Additionally, Northfield Bank is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to Northfield Bank or any other of their financial institutions. Northfield Bank is providing individuals with information on how to place fraud alerts, credit freezes, and credit lock on their credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Northfield Bank is also providing notice of this incident to relevant state and federal regulators.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4259.

Very truly yours,

Colin D. Scanlon of
MULLEN COUGHLIN LLC

CDS/cob

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (NOTICE OF [DATA SECURITY EVENT / DATA BREACH])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are contacting you to provide important information regarding a data security event which occurred at a third-party vendor whom Northfield Bank utilizes to provide certain products and services to you. Please note that the event had no impact on Northfield Bank's systems and is not the result of any activities at Northfield Bank.

What Happened?

On August 4, 2023, we were notified by our vendor of an incident which occurred during the period May 27 to May 31, 2023, related to vulnerabilities discovered in the MOVEit Transfer application. The application is offered by Progress Software Corporation and is a commonly used Managed File Transfer (MFT) software supporting file transfer activities of thousands of organizations around the world. The MOVEit software was used by our vendor to support its services to Northfield Bank. Upon notification from our vendor of the event, Northfield Bank began an investigation to evaluate the scope and nature of the event.

Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about it, our response, and additional measures you can take to help protect your information.

What Information Was Involved?

We conducted a review of the contents of files provided by our vendor, and determined one or more of the files contained the following information related to you: your name, account number, Social Security number and/or online banking username. Please note that **no** password information was present.

What We Are Doing

Upon learning of this incident, we began working with our vendor to monitor their investigation and remediation, and identify customers affected. Our vendor mobilized a technical response team to examine the relevant MOVEit Transfer systems to ensure that there were no further vulnerabilities. Our vendor has advised us that they have also remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider's guidelines. We have engaged cyber security specialists to assist us in monitoring their investigation and remediation.

What You Can Do

Our vendor is offering for a period of two years complimentary identity monitoring and restoration services through Kroll, a global leader in risk mitigation and response.

For more information on identity theft protection, including instructions on how to activate the monitoring and restoration services, please review Attachments A and B that follow this letter.

We recommend that you remain vigilant and regularly review and monitor all of your credit history to guard against any unauthorized transactions or activities. We also recommend that you monitor your account statements and notify us or any other of your financial institutions if you suspect any unauthorized activity.

For More Information

If you have any questions about this notice or the event, please feel free to contact Kroll at [\[TFN\]](#), Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Northfield Bank

ATTACHMENT A

Visit <https://enroll.krollmonitoring.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.

Membership Number: <<Membership Number (s_n)>>

For more information about Kroll and your Identity Monitoring services, you can visit 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.

\$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 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 or call toll-free (877) 322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

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

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
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 1-877-382-4357; or www.consumer.gov/idtheft.

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.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or <https://www.marylandattorneygeneral.gov/>.

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 276999001; (919) 716-6400; or <http://www.ncdoj.gov>.

New York Residents: The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

EXHIBIT BB



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (NOTICE OF [SECURITY INCIDENT / DATA BREACH])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are contacting you to provide important information regarding a data security event which occurred at a third-party vendor whom Northfield Bank utilizes to provide certain products and services to you. Please note that the event had no impact on Northfield Bank's systems and is not the result of any activities at Northfield Bank.

What Happened?

On August 4, 2023, we were notified by our vendor of an incident which occurred during the period May 27 to May 31, 2023, related to vulnerabilities discovered in the MOVEit Transfer application. The application is offered by Progress Software Corporation and is a commonly used Managed File Transfer (MFT) software supporting file transfer activities of thousands of organizations around the world. The MOVEit software was used by our vendor to support its services to Northfield Bank. Upon notification from our vendor of the event, Northfield Bank began an investigation to evaluate the scope and nature of the event.

Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about it, our response, and additional measures you can take to help protect your information.

What Information Was Involved?

We conducted a review of the contents of files provided by our vendor, and determined one or more of the files contained the following information related to you: your name, account number, Social Security number, Employer Identification number and/or online banking username. Please note that **no** password information was present.

What We Are Doing

Upon learning of this incident, we began working with our vendor to monitor their investigation and remediation, and identify customers affected. Our vendor mobilized a technical response team to examine the relevant MOVEit Transfer systems to ensure that there were no further vulnerabilities. Our vendor has advised us that they have also remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider's guidelines. We have engaged cyber security specialists to assist us in monitoring their investigation and remediation.

What You Can Do

Our vendor is offering for a period of two years complimentary identity monitoring and restoration services through Kroll, a global leader in risk mitigation and response.

For more information on identity theft protection, including instructions on how to activate the monitoring and restoration services, please review Attachments A and B that follow this letter.

We recommend that you remain vigilant and regularly review and monitor all of your credit history to guard against any unauthorized transactions or activities. We also recommend that you monitor your account statements and notify us or any other of your financial institutions if you suspect any unauthorized activity.

For More Information

If you have any questions about this notice or the event, please feel free to contact Kroll at [\[TFN\]](#), Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Northfield Bank

ATTACHMENT A

Visit <https://enroll.krollmonitoring.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.

Membership Number: <<Membership Number (s_n)>>

For more information about Kroll and your Identity Monitoring services, you can visit 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.

\$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 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 or call toll-free (877) 322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

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

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
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 1-877-382-4357; or www.consumer.gov/idtheft.

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 <https://www.marylandattorneygeneral.gov/>.

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 276999001; (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.

New York Residents: The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.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. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. [There are approximately \[##\] Rhode Island residents that may be impacted by this event.](#)