28541

OLD POINT NATIONAL BANK

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Old Point National Bank ("Old Point"), like many organizations across the country, has unfortunately been the victim of a cybersecurity incident involving a business email account at the Bank. We are writing to you to share with you how this may have affected your personal information and, as a precaution, to provide steps you can take to help protect your information. Old Point takes the privacy and security of your personal information very seriously, and we sincerely regret any concern this incident may cause you.

What Happened

We were the victim of a cybersecurity incident involving an Old Point business email account being accessed by an unauthorized user. The incident occurred on or about September 2, 2022, when an unauthorized user gained access to the Old Point business email account remotely. We engaged leading outside cybersecurity experts who confirmed that the unauthorized user's access was limited only to the web-based email platform and that no other systems at the Bank were impacted. While the unauthorized user was only able to gain access to this one email account for a brief period of time, the email account contained certain personal information of Old Point customers who were transacting business with the Bank.

It is unknown whether the unauthorized user was able to discover or access this customer personal information. We have no evidence that the unauthorized user was able to use any of the personal information the email account contained to cause any harm to customers of Old Point or that your information was used for any malicious purpose. However, out of an abundance of caution, we are notifying you of this event and are asking you to stay vigilant regarding your personal information.

What Information Was Involved

The personal information involved was related to a loan or similar transaction, which may have included your name, a copy of your driver's license, Social Security number, and Old Point account numbers and loan balances. Old Point has retained industry-leading outside security experts to conduct a thorough internal investigation into this incident and believes that your account or information at Old Point has **not** been fraudulently accessed. However, we want to alert you to this issue so that you can remain alert to any potential issues in the future.

What We Are Doing

Old Point immediately reported the incident to the appropriate law enforcement authorities including the Virginia State Police High Tech Crimes Unit, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, and the FBI Cyber Crimes Division. Old Point is cooperating in the investigation of these incidents by law enforcement to help bring the attackers to justice. Old Point also took immediate steps to make sure that this information could not be utilized to cause damage to your account at Old Point by putting in place extra procedures and protocols to help protect your information. We also engaged leading cybersecurity experts to assist us in our investigation and the hardening of our environment. We are working to remain vigilant to the ever-changing cyberthreat landscape and encourage you to do the same.

Additionally, to help prevent similar types of incidents from occurring in the future, we have implemented further security protocols designed to further protect our network, email environment, systems, and customer personal information.

What You Can Do

Please review the enclosed "Information About Identity Theft Protection" reference guide, which describes additional steps you may take to help protect your information. We recommend that you change your passwords for all your financial accounts and stay vigilant regarding issues around identity fraud for the next twelve to twenty-four months. Carefully review your monthly checking, savings and investment statements and use the provided identity monitoring service to ensure that no new cards, loans or mortgages have been taken out in your name.

To help relieve concerns and restore confidence following this incident, 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, Fraud Consultation, and Identity Theft Restoration.

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.

Additional information describing your services is included with this letter.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information

The security of your personal information is extremely important to us and we sincerely regret that this incident occurred. If you have questions, please call (855) 504-2882, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Robert F. Shuford, Jr.

Chairman, President & CEO
Old Point National Bank

ADDITIONAL RESOURCES

Contact information for the three 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 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three 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 Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one 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 Alerts. There are two types of 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 at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three 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 him/her 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 5 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 minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

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

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

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 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.