



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Carolyn Purwin Ryan
Office: (267) 930-6836
Fax: (267) 930-4771
Email: CPurwinRyan@mullen.law

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

May 18, 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: Triad Business Bank - Preliminary Notice of Data Event

To Whom It May Concern:

We represent Triad Business Bank (“the Bank”) located at 1501 Highwoods Boulevard, Suite 103, Greensboro, NC 27410, and are writing to notify your office of an incident that may affect the security of certain personal information relating to fifty-two (52) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this preliminary notice, the 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.

On or about January 27, 2023, the Bank became aware of suspicious activity relating to an employee’s email account. The Bank immediately took steps to secure all email accounts and launched an investigation with assistance from qualified professionals, including legal counsel and forensic specialist to determine the nature and scope of the activity. The investigation revealed that there was unauthorized access to a single employee’s email account for a limited period of time between January 24, 2023, to January 27, 2023.

Although the investigation was unable to confirm whether the unknown actor viewed any emails or attachments while in the account, we could not rule out the possibility that some information contained within the account may have been impacted. Therefore, in an abundance of caution, the Bank undertook a comprehensive and resource-intensive review of the contents of the email account again with assistance from outside professionals, to determine whether sensitive information was present in the emails at the time of the incident. That process was recently completed, and it was determined that certain information was present in the impacted email

Office of the Attorney General

May 18, 2023

Page 2

account. The information that could have been subject to unauthorized access includes name and Social Security number. The Bank will be notifying affected individuals and will update your Office when such notice occurs.

Upon discovering the incident, the Bank moved quickly to investigate and respond to the incident, assess the security of the Bank systems, and identify potentially affected individuals. Further, the Bank notified federal law enforcement regarding the incident. The Bank is also working to implement additional safeguards and training to its employees.

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-6836.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Carolyn Ryan".

Carolyn Purwin Ryan of
MULLEN COUGHLIN LLC

CPR/tty

TRIADBUSINESSBANK

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

NOTICE OF <<VARIABLE HEADER>>

Dear <<Name 1>>:

Triad Business Bank (“the Bank”) is writing to inform you of an event that may involve some of your information. Although there is no indication that your information has been misused in relation to this event, we are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On or about January 27, 2023, the Bank became aware of suspicious activity relating to an employee’s email account. The Bank immediately took steps to secure all email accounts and launched an investigation with assistance from qualified professionals to determine the nature and scope of the activity. The investigation revealed that there was unauthorized access to a single employee’s email account for a limited period of time between January 24, 2023, to January 27, 2023.

Although the investigation was unable to confirm whether the unknown actor viewed any emails or attachments while in the account, we could not rule out the possibility that some information contained within the account may have been impacted. Therefore, in an abundance of caution, the Bank undertook a comprehensive and resource-intensive review of the contents of the email account to determine whether sensitive information was present in the emails at the time of the incident. That process was recently completed. The Bank then worked to identify contact information for the potentially impacted individuals. We are notifying you because that investigation determined certain information related to you was present in an impacted email account.

What Information Was Involved? The information that may have been impacted by this incident includes your <<Breached Elements>>, and name. To date, we have not received any reports of fraudulent misuse of any information as a result of this incident.

What We Are Doing. Data privacy and security are among our highest priorities, and we have security measures in place to protect information in our care. Upon learning of the activity, the Bank immediately took steps to further secure our systems and investigate the event. We will also notify applicable federal and state regulators, as necessary.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity over the next twelve (12) to twenty-four (24) months. You may also review the enclosed *Steps You Can Take to Help Protect Personal Information* to learn helpful tips to protect your information, should you feel it appropriate to do so.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call our dedicated assistance line at 1-888-981-5733, 9:00 a.m. to 9:00 p.m. Eastern Time, except holidays. You can also write to the Bank at 1501 Highwoods Boulevard, Suite 103, Greensboro, NC 27410. We apologize for any inconvenience or concern this incident may cause.

Sincerely,

Julie Compton
Regional Operations Manager
Triad Business Bank

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	1 (800) 916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

<<For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.>>

<<For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [https://www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov).>>

<<For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.>>

<<For 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/>.>>

<<For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.>>

<<For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<RI #>> Rhode Island residents impacted by this incident.>>



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Carolyn Purwin Ryan
Office: (267) 930-6836
Fax: (267) 930-4771
Email: CPurwinRyan@mullen.law

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

May 24, 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: Triad Business Bank - Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Triad Business Bank (“the Bank”) located at 1501 Highwoods Boulevard, Suite 103, Greensboro, NC 27410, and are writing to supplement our notification on May 18, 2023 and provide additional information to your office of an incident that may affect the security of certain personal information relating to fifty (50) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this supplemental notice, the 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 or about January 27, 2023, the Bank became aware of suspicious activity relating to an employee’s email account. The Bank immediately took steps to secure all email accounts and launched an investigation with assistance from qualified professionals, including legal counsel and forensic specialist to determine the nature and scope of the activity. The investigation revealed that there was unauthorized access to a single employee’s email account for a limited period of time between January 24, 2023, to January 27, 2023.

Although the investigation was unable to confirm whether the unknown actor viewed any emails or attachments while in the account, we could not rule out the possibility that some information contained within the account may have been impacted. Therefore, in an abundance of caution, the Bank undertook a comprehensive and resource-intensive review of the contents of the email account again with assistance from outside professionals, to determine whether sensitive information was present in the emails at the time of the incident. That process was recently completed. The Bank then worked to identify contact information for the impacted individuals. We are notifying you because that investigation determined certain information related to fifty (50) residents of your state was present in an impacted email account.

Mullen.law

The information that could have been subject to unauthorized access includes name, payment card number, date of birth, and Social Security number.

Notice to Maryland Residents

On or about May 24, 2023, the Bank provided written notice of this incident to fifty (50) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit A**.

Other Steps Taken and To Be Taken

Upon discovering the event, the Bank moved quickly to investigate and respond to the incident, assess the security of Bank systems, and identify potentially affected individuals. Further, the Bank notified the Federal Deposit Insurance Corporation and the North Carolina Commissioner of Banking. The Bank is also working to implement additional safeguards and training to its employees.

Additionally, the 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 their credit card company and/or bank. The Bank is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

The Bank is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-6836.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Carolyn Ryan".

Carolyn Purwin Ryan of
MULLEN COUGHLIN LLC

CPR/kzm
Enclosure

EXHIBIT A

TRIADBUSINESSBANK

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

NOTICE OF <<VARIABLE HEADER>>

Dear <<Name 1>>:

Triad Business Bank (“the Bank”) is writing to inform you of an event that may involve some of your information. Although there is no indication that your information has been misused in relation to this event, we are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On or about January 27, 2023, the Bank became aware of suspicious activity relating to an employee’s email account. The Bank immediately took steps to secure all email accounts and launched an investigation with assistance from qualified professionals to determine the nature and scope of the activity. The investigation revealed that there was unauthorized access to a single employee’s email account for a limited period of time between January 24, 2023, to January 27, 2023.

Although the investigation was unable to confirm whether the unknown actor viewed any emails or attachments while in the account, we could not rule out the possibility that some information contained within the account may have been impacted. Therefore, in an abundance of caution, the Bank undertook a comprehensive and resource-intensive review of the contents of the email account to determine whether sensitive information was present in the emails at the time of the incident. That process was recently completed. The Bank then worked to identify contact information for the potentially impacted individuals. We are notifying you because that investigation determined certain information related to you was present in an impacted email account.

What Information Was Involved? The information that may have been impacted by this incident includes your <<Breached Elements>>, and name. To date, we have not received any reports of fraudulent misuse of any information as a result of this incident.

What We Are Doing. Data privacy and security are among our highest priorities, and we have security measures in place to protect information in our care. Upon learning of the activity, the Bank immediately took steps to further secure our systems and investigate the event. We will also notify applicable federal and state regulators, as necessary.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity over the next twelve (12) to twenty-four (24) months. You may also review the enclosed *Steps You Can Take to Help Protect Personal Information* to learn helpful tips to protect your information, should you feel it appropriate to do so.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call our dedicated assistance line at 1-888-981-5733, 9:00 a.m. to 9:00 p.m. Eastern Time, except holidays. You can also write to the Bank at 1501 Highwoods Boulevard, Suite 103, Greensboro, NC 27410. We apologize for any inconvenience or concern this incident may cause.

Sincerely,

Julie Compton
Regional Operations Manager
Triad Business Bank

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	1 (800) 916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

<<For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.>>

<<For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [https://www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov).>>

<<For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.>>

<<*For 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/>.>>

<<*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.>>

<<*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<RI #>> Rhode Island residents impacted by this incident.>>