Appendix

On December 9, 2020, First State Bank concluded its investigation of a data security incident in which an unauthorized party accessed certain systems within First State Bank's computer network. Upon discovering this incident, First State Bank immediately secured its systems and launched an investigation with the assistance of a computer forensics firm. Through this investigation, First State Bank determined that the unauthorized access occurred between November 2, 2020 and November 9, 2020. First State Bank determined that certain files on its computer network may have been accessed by the unauthorized party. Those files contained the names, Social Security numbers, and/or financial account numbers of some of its customers and their beneficiaries.

Although the investigation was largely able to identify the systems and time frame involved or potentially involved, it was not able to identify the specific individuals potentially involved. Consequently, First State Bank is providing substitute notice today by issuing a press release, posting a statement on the First State Bank website and emailing its customers. Copies of the press release, website statement and the email are attached[1]. First State Bank is also offering one year of complimentary credit monitoring to individuals who are potentially affected by this incident. First State Bank has also provided a phone number for individuals to call if they have any questions regarding this incident.

To help prevent a similar incident from occurring in the future, First State Bank has implemented additional data security measures, such as installing new endpoint security monitoring software and providing employees with enhanced cybersecurity awareness training.

[1] This report does not waive First State Bank's objection that Maine lacks personal jurisdiction over it related to any claims that may arise from this incident.

First State Bank: Community Bank in Socorro, New Mexico Identifies and Addresses Data Security Incident

SOCORRO, N.M., Jan. 5, 2021 /PRNewswire/ -- Today, First State Bank, a Community Bank in Socorro and Catron counties, New Mexico, announced that it recently identified and addressed a data security incident.

On November 9, 2020, First State Bank became aware of a data security incident in which an unauthorized party accessed certain systems within First State Bank's computer network. Upon discovering this incident, First State Bank immediately secured its systems and launched an investigation with the assistance of a computer forensics firm. Through this investigation, First State Bank determined that the unauthorized access occurred between November 2, 2020 and November 9, 2020.

To help prevent a similar incident from occurring in the future, First State Bank has implemented additional data security measures, such as installing new endpoint security monitoring software and providing employees with enhanced cybersecurity awareness training.

First State Bank determined that certain files contained in the systems accessed by the unauthorized party included the names, Social Security numbers and/or financial account numbers of some of its customers and their beneficiaries. Although First State Bank is not aware of the misuse of any of the information maintained on its computer network, out of an abundance of caution, First State Bank encourages its customers to remain vigilant by reviewing their financial account statements for any unauthorized activity. As a precaution, First State Bank is offering complimentary credit monitoring to those individuals potentially affected by this incident. To enroll in credit monitoring, please contact First State Bank at 575-835-1550.

"First State Bank takes data security very seriously and understands the importance of protecting the information it maintains," said Cuatro Bursum, the President and Chief Operating Officer at First State Bank. "We have worked to address this issue and regret any inconvenience this may cause to our valued customers."

For more information about this incident, please visit https://www.socorrobanking.com/data-security-incident-notification or call First State Bank at 575-835-1550 Monday through Friday, from 9:00 a.m. to 5:00 p.m., Mountain Time.

NOTICE OF DATA SECURITY INCIDENT

Tuesday, January 5, 2021

Dear Valued Customer:

First State Bank takes data security very seriously and we understand the importance of protecting the information we maintain. We are writing to inform you about an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

WHAT HAPPENED?
On December 9, 2020, First State Bank concluded its investigation of a data security incident in which an unauthorized party accessed certain systems within First State Bank's computer network. Upon discovering this incident, First State Bank immediately secured its systems and launched an investigation with the assistance of a computer forensics firm. Through this investigation, First State Bank determined that the unauthorized access occurred between November 2, 2020 and November 9, 2020.

WHAT INFORMATION WAS INVOLVED?
First State Bank determined that certain files on its computer network may have been accessed by the unauthorized party. Those files contained the names, Social Security numbers, and/or financial account numbers of some of our customers and their beneficiaries.

WHAT YOU CAN DO.
To date, First State Bank is not aware of the misuse of any of the information maintained on its computer network. Out of an abundance of caution, we encourage you to remain vigilant by reviewing your financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, we suggest that you contact First State Bank immediately. As a precaution, we are offering complimentary credit monitoring to those individuals who believe that they might be affected by this incident. To enroll in credit monitoring, please contact First State Bank at 575-835-1550.

WHAT WE ARE DOING.
First State Bank regrets any inconvenience or concern this may cause. To help prevent a similar incident from occurring in the future, we have implemented additional data security measures, such as installing new endpoint security monitoring software and providing employees with enhanced cybersecurity awareness training.

FOR MORE INFORMATION.
If you have any questions regarding this incident, please call First State Bank at 575-835-1550 Monday through Friday, from 9:00 a.m. to 5:00 p.m., Mountain Time.

Sincerely,

Holm Bursum IV
President and Chief Executive Officer

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes

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

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

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

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

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

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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

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

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove

it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

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

Additional Information for Residents of the Following States

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

District of Columbia: You can contact First State Bank via U.S. mail at 103 Manzanares Ave E, Socorro, NM 87801 or via telephone at (575) 835-1550. You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: You can contact First State Bank via U.S. mail at 103 Manzanares Ave E, Socorro, NM 87801. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New York: You may contact and obtain information from these state agencies:

- New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection

- New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

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

Rhode Island: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as

agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

NOTICE OF DATA SECURITY INCIDENT

California Residents Please Click Here https://www.socorrobanking.com/data-security-incident-notification-california-residents.

First State Bank takes data security very seriously and we understand the importance of protecting the information we maintain. We are writing to inform you about an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

WHAT HAPPENED?

On December 9, 2020, First State Bank concluded its investigation of a data security incident in which an unauthorized party accessed certain systems within First State Bank's computer network. Upon discovering this incident, First State Bank immediately secured its systems and launched an investigation with the assistance of a computer forensics firm. Through this investigation, First State Bank determined that the unauthorized access occurred between November 2, 2020 and November 9, 2020.

WHAT INFORMATION WAS INVOLVED?

First State Bank determined that certain files on its computer network may have been accessed by the unauthorized party. Those files contained the names, Social Security numbers, and/or financial account numbers of some of our customers and their beneficiaries.

WHAT YOU CAN DO.

To date, First State Bank is not aware of the misuse of any of the information maintained on its computer network. Out of an abundance of caution, we encourage you to remain vigilant by reviewing your financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, we suggest that you contact First State Bank immediately. As a precaution, we are offering complimentary credit monitoring to those individuals who believe that they might be affected by this incident. To enroll in credit monitoring, please contact First State Bank at 575-835-1550.

WHAT WE ARE DOING.

First State Bank regrets any inconvenience or concern this may cause. To help prevent a similar incident from occurring in the future, we have implemented additional data security measures, such as installing new endpoint security monitoring software and providing employees with enhanced cybersecurity awareness training.

FOR MORE INFORMATION.

If you have any questions regarding this incident, please call First State Bank at 575-835-1550 Monday through Friday, from 9:00 a.m. to 5:00 p.m., Mountain Time.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes

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

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

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

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

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

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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

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

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

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

Additional Information for Residents of the Following States

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

District of Columbia: You can contact First State Bank via U.S. mail at 103 Manzanares Ave E, Socorro, NM 87801 or via telephone at (575) 835-1550. You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: You can contact First State Bank via U.S. mail at 103 Manzanares Ave E, Socorro, NM 87801. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New York: You may contact and obtain information from these state agencies:

- New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection

- New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

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

Rhode Island: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information

from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

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

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.