



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>>

Dear <<Name 1>>:

Veritex Holdings, Inc. (“Veritex”) is writing to inform you of an incident that could affect the security of some of your information. While we are unaware of any actual or attempted misuse of your information, we take this incident very seriously and we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

**What Happened?** Earlier this year, Veritex became aware of unusual activity involving certain employee email accounts and immediately began an investigation with the assistance of third-party forensic investigators. On May 8, 2020, the investigation determined that certain employee email accounts were accessed without authorization at varying times between April 2, 2020 and April 27, 2020. Unfortunately, the available evidence did not allow us to determine what, if any, emails and attachments were viewed while the accounts were subject to unauthorized access.

Therefore, the forensic investigator reviewed the email accounts to identify any personal information that was located in the email accounts at the time of the unauthorized access and could have been accessible. On September 25, 2020, we determined that some personal information was present in one or more of the email accounts at the time of the incident. We reviewed this information and our internal records to identify the individuals associated with this information and their address for purposes of providing notice. Through this process we determined that some of your personal information was contained in one or more of the impacted email accounts.

**What Information Was Involved?** Our investigation determined that at the time of the incident the email accounts contained information including your name, <<Data Elements>>. To date, we are unaware of any actual or attempted misuse of your personal information as a result of this incident.

**What We Are Doing.** We take this incident and the security of personal information in our care very seriously. Upon learning of this incident, we promptly began an investigation using external digital forensic specialists, changed email account credentials, and investigated to confirm the security of our email network. We are also working to enhance our existing security processes and protocols.

As an added precaution, we are also offering you access to 12 months of identity monitoring services through TransUnion Interactive, a subsidiary of TransUnion,<sup>®</sup> one of the three nationwide credit reporting companies at no cost to you. These services include credit monitoring and identity theft restoration. If you wish to activate these identity monitoring services, you may follow the instructions included in the “Steps You Can Take to Protect Your Information.”

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Please review the enclosed “Steps You Can Take to Protect Your Information.” You can also enroll to receive the free credit monitoring and identity theft protection services we are offering.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 855-940-5298 between 9 am and 9 pm Eastern Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

Veritex Community Bank

## Steps You Can Take to Protect Your Information

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

### **How to Enroll:** You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at **[www.MyTrueIdentity.com](http://www.MyTrueIdentity.com)** and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

### **ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

### **Monitor Accounts**

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

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

#### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

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, provide 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

**Experian**

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

**TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338). 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 Maryland residents*, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 1-888-743-0023; [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer).

*For North Carolina residents*, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; [www.ncdoj.gov](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

*For Rhode Island residents*, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; [www.riag.ri.gov](http://www.riag.ri.gov); 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 7 Rhode Island residents impacted by this incident.

*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 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 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 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](http://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.

*Oregon Residents*, Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/); 877-877-9392.

*Kentucky Residents*, Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov/](http://www.ag.ky.gov/); 1-502-696-5300.

*For District of Columbia residents*, the Office of the District of Columbia Attorney General can be contacted at 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; Phone (202) 442-9828; Fax: (202) 347-8922; TTY: (202) 727-3400; Email: [oag@dc.gov](mailto:oag@dc.gov); or you may visit the website of the Office of the District of Columbia Attorney General at <https://oag.dc.gov/>.