October 28, 2020

Good afternoon,

As a follow up to our previous breach notifications, attached is the letter templates we will be individualizing and sending to affected consumer customers today, October 28, 2020. At present, 4 additional Washington-based customers were identified as having data involved in the breach.

On July 30, 2020, a local office computer server containing client information was physically stolen from our corporate office in Ontario, CA. The server contained information on commercial loans and the associated individuals tied to those loans, which included current, former and prospect accounts. Since the event, we have been focused on identifying who was impacted and working with authorities to recover the stolen server. Additional files containing personal information were discovered through additional investigation.

Organization: U.S. Bank, N.A., 425 Walnut Street, Cincinnati, OH 45202
Primary Contact: Jeff Roby 612.303.2398 jeffrey.roby@usbank.com
Types of Information: Customer Name, Address, Account Number, SSN, Driver's License Number
Date of Security Breach: July 30th, 2020
Date of additional Consumer Notification: October 28, 2020

Thanks,

Micheal L Goodman
Assistant Vice President | Privacy – Technology Risk Oversight
p. 612.852.1600 | **c.** 612.430.0024 | micheal.goodman@usbank.com
U.S. Bank
MN-U.S. Bank Plaza Minneapolis
200 S 6th St, Minneapolis, MN 55402 | EP-MN-L06C | www.usbank.com

<<Street Address>>
<<City>>, <<State>> <<Zip>>

<<Month Date, Year>>

<<Customer Name>>
<<Address>>
<<City>>, <<State>> <<Zip>>
<<Barcode>>

Dear [Customer Name]:

At U.S. Bank, we value your confidence in us and place the privacy and security of your information as a top priority. We are writing to let you know about an event that occurred at a U.S. Bank location, which included some of your personal information.

What happened:
On July 30, 2020, a computer server containing your information was physically stolen from one of our corporate offices. Since the event, we have been focused on identifying who may have been impacted and working with authorities to recover the stolen server.

What information was involved:
The information on the server included personally identifiable information including your name, account number, Social Security number, and driver's license number. At this time, we are not aware of the information being used fraudulently against you or your account.

What are we doing:
We apologize for any inconvenience this has caused. As a precautionary measure, if you would like to receive a new account number, you can do so by calling our Fraud Liaison Center at 877.595.6256 between 8 a.m. to 9 p.m. CT, Monday through Sunday. We can help you close and reopen your account with a new account number at no charge.

We also want to inform you of some steps we have taken to protect you and some additional steps you can take to help protect yourself.

Free credit monitoring and identity restoration services
To help you protect your identity, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at **mytrueidentity.com** and in the space referenced as "Enter Activation Code," enter the following 12-letter Activation Code and follow the three steps to receive your credit monitoring service online within minutes.

Unique activation code: **<< TU Code>>**

Once you are enrolled, you will be able to obtain an initial 3-in-1 credit report and credit scores along with two years of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at

TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes dark web internet identity monitoring, the ability to lock and unlock your TransUnion credit report, access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Certain policy limitations and exclusions may apply.)

If you believe you may be a victim of identity theft, please call the TransUnion Fraud Response Services toll-free hotline at 855.288.5422**.** When prompted, enter the following 6-digit telephone pass code 698500 to speak to a TransUnion representative about your identity theft issue.

You can sign up for the *my*TrueIdentity online credit monitoring anytime between now and **December 15, 2020.** 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, Experian and Equifax or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

What you can do:

Free fraud alert information

Whether or not you enroll in credit monitoring, we recommend that you place a "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
equifax.com	transunion.com/fraud	experian.com/fraud
800.525.6285	800.680.7289	888.397.3742

Free credit report information

Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 877.322.8228 or make a request online at annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) at identitytheft.gov or at 877.ID.THEFT (877.438.4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. Also visit the FTC's website at ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "*Identity Theft - A Recovery Plan.*"

Free credit-security freeze information

You can request a free Security Freeze (aka "Credit Freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a credit freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A credit freeze can make it more difficult for someone to

get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

Equifax Security Freeze	TransUnion Security Freeze	Experian Security Freeze
PO Box 105788	PO Box 2000	PO Box 9554
Atlanta, GA 30348	Chester, PA 19016	Allen, TX 75013
equifax.com	transunion.com/freeze	experian.com/freeze
800.685.1111	888.909.8872	888.397.3742

Finally, I want to thank you on behalf of U.S. Bank for your business, as well as the confidence you place in us. We take that trust seriously and are sorry that this situation has occurred. Please reach out to us with any questions or concerns at U.S. Bank 24-Hour banking at 800.USBANKS (872.2657).

Sincerely,

Timothy J. Nagle
Senior Vice President
Chief Privacy Officer

<<Street Address>>
<<City>>, <<State>> <<Zip>>

<<Month Date, Year>>

<<Customer Name>>
<<Address>>
<<City>>, <<State>> <<Zip>>
<<Barcode>>

Re: Information regarding your account ending in XXXX.

Dear [Customer Name]:

At U.S. Bank, we value your confidence in us and place the privacy and security of your information as a top priority. We are writing to let you know about an event that occurred at a U.S. Bank location, which included some of your personal information.

What happened:
On July 30, 2020, a computer server containing your information was physically stolen from one of our corporate offices. Since the event, we have been focused on identifying who may have been impacted and working with authorities to recover the stolen server.

What information was involved:
The information on the server included personally identifiable information including your name and account number. At this time, we are not aware of the information being used fraudulently against you or your account.

What are we doing:
We apologize for any inconvenience this has caused. As a precautionary measure, if you would like to receive a new account number, you can do so by calling our Fraud Liaison Center at 877.595.6256 between 8 a.m. to 9 p.m. CT, Monday through Sunday. We can help you close and reopen your account with a new account number at no charge.

What you can do:
Free fraud alert information
We recommend that you place a “Fraud Alert” on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
equifax.com	transunion.com/fraud	experian.com/fraud
800.525.6285	800.680.7289	888.397.3742

Free credit report information
Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 877.322.8228 or make a request online at annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) at identitytheft.gov or at 877.ID.THEFT (877.438.4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. Also visit the FTC's website at ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "*Identity Theft - A Recovery Plan.*"

Free credit-security freeze information
You can request a free Security Freeze (aka "Credit Freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a credit freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A credit freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

Equifax Security Freeze	TransUnion Security Freeze	Experian Security Freeze
PO Box 105788	PO Box 2000	PO Box 9554
Atlanta, GA 30348	Chester, PA 19016	Allen, TX 75013
equifax.com	transunion.com/freeze	experian.com/freeze
800.685.1111	888.909.8872	888.397.3742

Finally, I want to thank you on behalf of U.S. Bank for your business, as well as the confidence you place in us. We take that trust seriously and are sorry that this situation has occurred. Please reach out to us with any questions or concerns at U.S. Bank 24-Hour banking at 800.USBANKS (872.2657).

Sincerely,

Timothy J. Nagle
Senior Vice President
Chief Privacy Officer