BANK OF THE WEST
BNP PARIBAS

June 23, 2022

Customer Name
Street Address
City, State Zip

LS 0622-096

Dear Customer Name:

As you are likely aware, your Bank of the West debit card(s) may have been compromised as a result of fraudulent activities involving an ATM. We regret this unfortunate incident.

What Happened?
On November 10, 2021, our security teams identified instances of unauthorized account withdrawal attempts at several ATMs. We promptly contacted law enforcement and began taking steps to review our ATM network. Our review found that a device known as an "ATM skimming device" had been installed on several of our ATMs. This investigation and discovery period occurred between November 10, 2021 and April 18, 2022.

What Information Was Involved?
The ATM skimming device that was installed interfered with the normal debit card transaction and allowed the theft of your card number, the PIN number associated with your card, and possibly your name and address. This stolen information may have been used to create fake debit cards and attempt cash withdrawals.

What We Are Doing
We take this matter very seriously. Promptly upon our discovery of a potential ATM skimming device, we took steps to stop the continued fraudulent use of stolen card information. We also moved quickly to protect you and your information by actively monitoring your account(s) for suspicious activity, taking the ATM machines in question out of service, and inspecting them for evidence of tampering, and working closely with law enforcement. If our monitoring found suspicious or fraudulent activity on your account, your account was blocked and we sent you a new debit card with instructions for creating a new PIN.

Remember, in general, if you become aware of unauthorized transactions on your account and promptly report those transactions to us, you will not be responsible for unauthorized withdrawals, transfers, or purchases made using your debit card. Finally, and as a further precaution, we are offering you a year of free credit monitoring and identity theft protection services. See the ***Other Important Information*** section of this letter for information about how to enroll.

What You Can Do
We recommend closely reviewing all of your account statements for suspicious activity. If you find anything suspicious or fraudulent, you should call the Bank at the number listed on your account statement.

If you have not already done so, you may wish to request new debit or credit cards. If you feel this step is appropriate, please call the telephone number on your account statement.

You have the right to obtain a copy of your credit report for free once a year from each credit reporting agency. You can obtain a free credit report by visiting www.annualcreditreport.com, by calling (877) 322-8228, or by completing the Annual Credit Request Form and mailing it to: Annual Credit Report Request

Please see reverse for additional information

Service, P.O. Box 105281 Atlanta, GA 30348-5281. We suggest you remain vigilant over the next 12 to 24 months by checking your account statements monthly and requesting your free credit report from one bureau at a time every four months If you have questions regarding the information appearing on your credit report, please call the credit agency at the telephone number on the credit report.

If you do find suspicious activity on your credit report, call your local police or sheriff's office and file a report of identity theft. Get a copy of the police report, as you may need to give copies of the police report to creditors to clear up your records. It is also recommended that you report any incidents of identity theft to Bank of the West as well as to the Federal Trade Commission (FTC).

The Federal Trade Commission (FTC) also provides information about identify theft. You can visit www.identitytheft.gov, or you may also contact the FTC directly: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington DC, 20580, 1-877-FTC-HELP (1-877-382-4357).

In addition to reviewing your credit report, you have the right to place an initial "fraud alert" on your credit file. You can do this by calling any one of the three credit reporting agencies at the numbers below. Doing so will let you automatically place fraud alerts with all three agencies, and you will be sent information on how you can order a free credit report from each of the agencies. The "fraud alert" will stay on your credit report for 90 days. After that, you can renew the alert for additional 90-day periods by calling any one of the three agencies:

Equifax	Experian	TransUnion
(888) 766-0008	(888) 397-3742	(800) 680-7289
P.O. Box 740241	P.O. Box 9532	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

If you want to learn more about the steps you can take to avoid identity theft, visit the Federal Trade Commission's website. The FTC runs the U.S. government's identity theft information website, at www.identitytheft.gov. You can also contact the FTC via telephone at (877) ID-THEFT (877-438-4338). The FTC and the consumer reporting agencies can also provide you with additional information about using fraud alerts and security freezes to protect your information.

Additional state-specific notifications are included at the end of this letter.

Other Important Information

COMPLIMENTARY SERVICE OFFER

At our expense, we would like to offer you a free one year subscription to Identity Guard® Total, a credit monitoring and identity theft protection service. Aura Identity Guard Total provides essential monitoring and protection of not only credit data, but also monitors the Dark Web and alerts you if your Social Security number, credit cards, and bank account numbers are found in unsecure online locations.

Identity Guard® TOTAL features include:

- Dark Web Monitoring
- High Risk Transaction Alerts
- US Based Identity Theft Recovery Assistance
- 3-Bureau Credit Monitoring
- $1 Million Identity Theft Insurance*
- Bank Account Monitoring
- Account Access via Mobile App
- Anti-Phishing App/Safe Browser Extension

If you wish to take advantage of this monitoring service, you must enroll by August 23, 2022.

ENROLLMENT PROCEDURE

To activate this coverage please visit the Website listed below and enter the activation code. The activation code is required for enrollment and can only be used one time by the individual addressed.

Website: https://app.identityguard.com/activate/btw

Activation Code: [Activation Code]

In order to enroll, you will need to provide your: mailing address, telephone number, Social Security number, date of birth, email address, as well as your redemption code.

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel. We apologize for any inconvenience and urge you to enroll today.

For More Information

If you have any questions, please call our Contact Center at (800) 488-2265 (for TTY use: 800-659-5495) Monday - Friday, 6:00 a.m. to Midnight, and Saturday, Sunday, and most holidays, 7:00 a.m. to Midnight, Central Time.

We deeply regret the exposure of your personal information and are committed to supporting you through this situation.

Sincerely,

Randy Miskanic

Randy Miskanic
Senior Vice President
Bank of the West

AURA
IDENTITY GUARD

Identity Guard® Total Service

➢ **$1,000,000 Identity Theft Insurance* ($0 Deductible)** is provided to all members for certain fraud related expenses such as but not limited to:

- Unauthorized Loss of Funds Reimbursement
- Lost Wages: up to $2,000 per week, for 5 weeks maximum
- Travel Expenses: up to $1,000 per policy period
- Elder Care, Spousal Care, and Child Care: up to $2,000
- Costs for re-filing loan applications, grants or other credit instruments
- Attorney fees incurred (with prior consent from insurer)

➢ **Credit Monitoring (3 Bureau) Equifax®, Experian®, TransUnion® -** Every day a member's Equifax, Experian, and TransUnion credit files are monitored for certain changes such as an address change, new accounts, inquiries, accounts in collections, bankruptcy filings, new public records, and public record changes that could indicate identity theft.

➢ **Dark Web Monitoring –** Members are alerted when we detect their SSN, credit card numbers, financial account numbers, health insurance number, passport number and more are found on the Dark Web – places such as thousands of black-market websites, secret chat rooms, and underground forums.

➢ **Bank Account Monitoring –** Members are alerted when new bank accounts are opened in their name, personal information is changed on an existing account, or a new account holder is added to their account. Alerts also are sent when changes such as a member's name, address, or email address are made.

➢ **High Risk Transaction Monitoring/Authentication Alerts –** Notifies members when their identity is used for noncredit transactions like payday loans, wire transfers, and account openings.

➢ **Identity Guard's Alerts and Restoration Services –** Members are assigned a specially trained Dedicated Case Manager for a minimum of 90 days who monitors the customer's account and acts as the customer's primary point of contact for any potentially fraudulent activities.

➢ **Risk Assessment –** A score that assesses how likely members are to become a victim of identity theft based on behavioral and demographic data.

➢ **Internet Toolkit (Anti-Phishing & Safe Browsing) –** Protects members from phishing, malware delivered through ads, and Flash as well as providing an easy way to analyze and improve a member's social media privacy settings.

➢ **Mobile App –** Members can access their Identity Guard membership on their iOS or Android phone.

**Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

Note to California residents: Even if you do not find any signs of fraud on your reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. The law allows you to order a free credit report from each agency every 12 months. You may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period to monitor the accuracy and completeness of the information in your reports. Just call one of the numbers above to order your report and keep the "fraud alert" in place. For more information on identity theft, you may visit the California Office of Privacy Protection website at www.oag.ca.gov/privacy or call them toll-free at (866) 785-9663.

Note to Massachusetts residents: Residents of Massachusetts can obtain a copy of a police report, if filed. Massachusetts consumers also have the right to obtain a security freeze. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to Massachusetts law. The security freeze will prohibit a consumer-reporting agency from releasing any information in your credit report without your express authorization or approval. There is no charge for requesting a security freeze.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer-reporting agency and provide all of the following: (1) The unique personal identification number or password provided by the consumer-reporting agency; (2) Proper identification to verify your identity; and (3) The period of time for which the report shall be available to users of the credit report.

A consumer-reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request. A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit. You have the right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer-reporting agency.

Note to Maryland residents: Residents of Maryland can receive additional information by contacting the Office of Attorney General, 200 St. Paul Pl, Baltimore, MD 21202 phone (888-743-0023) www.oag.state.md.us/idtheft.

Note to North Carolina Residents: The North Carolina Attorney General's office is a good source of information about preventing identity theft. You can visit www.ncdoj.gov/Protect-Yourself/2-4-3-Protect-Your-Identity/Protect-Yourself.aspx, contact them at Consumer Protection Division, NC Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001 or call (919) 716-6000 (toll free in NC: (877) 566-7226).

Note to New York residents: The New York Attorney General's office is a good source of information about data breaches and preventing identity theft. You can visit https://ag.ny.gov/internet/data-breach and https://ag.ny.gov/internet/privacy-and-identity-theft or contact them at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, or call 1-800-771-7755, TTY 1-800-788-9898 or the New York Department of Financial Services at https://www.dfs.ny.gov/consumers/scams_schemes_frauds/identity_theft and https://www.dfs.ny.gov/consumers/scams_schemes_frauds/security_breach or call 1-800-342-3736.

Note to Rhode Island Residents: The Rhode Island Attorney General's office is a good source of information about preventing identity theft. You can visit www.riag.ri.gov/ConsumerProtection/About.php# , contact them at 150 South Main Street, Providence, RI 02903 or call (401) 274-4400.

Rhode Island consumers also have the right to obtain a security freeze. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to Rhode Island law. The security freeze will prohibit a consumer-reporting agency from releasing any information in your credit report without your express authorization or approval. Fees may be required to be paid to the consumer reporting agencies.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer-reporting agency and provide all of the following: (1) The unique personal identification number or password provided by the consumer-reporting agency; (2) Proper identification to verify your identity; and (3) The period of time for which the report shall be available to users of the credit report.

A consumer-reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request. A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit. You have the right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer-reporting agency.

Note to West Virginia Residents: West Virginia consumers also have the right to obtain a security freeze. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to West Virginia law. The security freeze will prohibit a consumer-reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer-reporting agency and provide all of the following: (1) The unique personal identification number or password provided by the consumer-reporting agency; (2) Proper identification to verify your identity; and (3) The period of time for which the report shall be available to users of the credit report.

A consumer-reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request. A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit. You have the right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer-reporting agency.