LifeMark
Securities Corp.

C/O ID Experts
PO Box 4600
Everett WA 98204

ENDORSE
NAME
ADDRESS1
ADDRESS2
CSZ
BREAK
SEQ
CODE 2D
Ver 1GE
COUNTRY

To Enroll, Please Call:
1-833-953-1735
Or Visit:
https://ide.myidcare.com/lifemark
Enrollment Code: <<XXXXXXXX>>

November 19, 2019

Notice of LifeMark Securities Corp. Data Security Incident

Dear NAME:

We would like to thank you for the trust you have placed in LifeMark Securities Corp., and our registered representative, <<Rep>>, with regard to your investments and financial services. This letter is to notify you of a data security incident that may have involved your personal information, including your name and Social Security number. While we have no evidence that your personal information was compromised, we wanted to let you know about this incident out of an abundance of caution. We value and respect the privacy of your information, and we sincerely apologize for any concern or inconvenience this may cause you. Please be assured that we have taken measures to address the incident and enhance the security of our systems.

Following is a brief description of the security incident, steps you can take to further protect your information, resources we are making available to you, a copy of LifeMark's Privacy Policy, and finally a New Account Agreement UPDATE form that will ensure we have the most current contact information along with suitability information to ensure your current investments are suitable compared to your investment objectives and risk tolerance. Please complete this New Account form and either return it to your registered representative or directly to LifeMark at 400 W. Metro Financial Center, Rochester, NY 14623.

1. What happened and what information was involved?

On September 4, 2019, we identified suspicious activity involving a limited number of LifeMark email accounts. In response to the suspicious activity, we immediately changed all email passwords and hired independent computer forensic experts to help us investigate. Our investigation recently concluded, and we have determined there were successful unauthorized connections to a limited number of LifeMark email accounts as a result of a phishing attack. We were unable to identify with certainty whether any emails or attachments were viewed as a result of the incident but wanted to let you know as your information may have been stored in one of the email accounts. If you sent sensitive information or documents containing your name, address, Social Security number, or financial account information to LifeMark via email, then that information may be at risk. Any information sent via a secure file share website remains unaffected and secure. This incident was limited to email accounts, other LifeMark systems were not impacted and remain secure.

2. What are we doing and what can you do?

We are offering complimentary identity theft protection services called MyIDCare through ID Experts. MyIDCare services include: 12 months of Credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-953-1735 or going to https://ide.myidcare.com/lifemark and using the Enrollment Code at the top of this letter. MyIDCare

experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 19, 2020.

We want to assure you that we have taken steps to prevent this type of incident from happening in the future. We have changed passwords for all email accounts along with implementing additional security controls. In addition, we have increased password complexity requirements, implemented a shorter password expiration policy, anti-threat protection tools for our email environment, and an enhanced third-party spam filter tool.

You should also pay careful attention to your financial statements over the next 12 to 24 months and immediately report any suspicious activity to your financial institution.

3. For more information:

You will find detailed instructions for enrollment on the enclosed ***Recommended Steps to Help Protect Your Information*** document enclosed with this letter. Also, you will need to reference the Enrollment Code in this letter when calling or enrolling online, so please do not discard this letter.

We take the security of your information seriously, and again apologize for any inconvenience this may cause you. Please call 1-833-953-1735 or go to https://ide.myidcare.com/lifemark for assistance or for any additional questions you may have.

Sincerely,

Jim Prisco
President
LifeMark Securities Corp.

MyIDCare™

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to https://ide.myidcare.com/lifemark and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-833-953-1735 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

SEQ
CODE 2D

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a violator. 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. You can 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.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.