

RECEIVED

JUN 20 2019

CONSUMER PROTECTION

CLARK HILL

Melissa K. Ventrone
T 312.360.2506
F 312.517.7572
Email: mventrone@clarkhill.com

Clark Hill
130 East Randolph Street
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999

clarkhill.com

June 17, 2019

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General MacDonald,

We are sending this notice on behalf of JD Bank, with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. JD Bank is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On February 26, 2019, JD Bank identified suspicious activity involving a limited number of JD Bank's corporate email accounts. Passwords for the email accounts were immediately changed and independent computer forensic experts were engaged to help investigate how the incident occurred, whether any information in the accounts was at risk, and steps that could be taken to prevent this from happening again. The forensic experts determined that an unauthorized individual may have had access to a limited number of corporate email accounts between February 19 – 26, 2019. The investigation confirmed that the incident was limited to these email accounts; the banking systems were not affected and remain secure. Forensic investigators were then asked to review the at risk accounts and determine whether any personal information was contained in the account. On April 2, 2019, the forensic investigators determined that personal information may have been contained in the at risk accounts. The type of information stored in the affected email accounts contained some combination of name, Social Security number or Tax ID number, financial account number, and, for a limited number of individuals, credit card number, driver's license and/or state ID, and date of birth. Extracting the personal information from the at-risk accounts took significant time as it involved reviewing all relevant documents, attachments, and emails. While we have no evidence that the unauthorized individual viewed or opened any emails or documents containing the personal information, out of an abundance of caution JD Bank notified potentially affected individuals about the incident.

June 17, 2019

Page 2

2. Number of New Hampshire residents affected.

On May 17th, 2019, JD Bank learned that a limited number of residents outside the state of Louisiana were affected by the security incident. Three (3) New Hampshire residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on June 17, 2019 via regular mail (a copy of the form notification letter is enclosed).

3. Steps taken or plan to take relating to the incident.

Steps have been taken to help prevent a similar occurrence in the future. JD Bank hired an independent forensic investigator and worked diligently to identify those individuals who may have been affected by the incident. All passwords have been changed, additional access control measures have been enabled on the email accounts, and JD Bank will be retraining employees on recognizing and responding to suspicious computer activity and other security threats. A letter was sent to impacted individuals which included details about the security incident, information about the Federal Trade Commission, the three major credit reporting agencies, and offered free identity protection services through ID Experts for one year. JD Bank also provided customers with a toll-free number for any questions.

4. Contact information.

JD Bank takes the security of the information in its control seriously, and is committed to ensuring its customers' and employees' information is protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Very truly yours,

CLARK HILL



Melissa K. Ventrone

Enclosure

CLARK HILL



C/O ID Experts
<<Address 1>>
<<City>> <<State>> <<ZIP>>

ENDORSE



NAME

ADDRESS1

ADDRESS2



2Dcode
SEQ

CSZ

COUNTRY

BREAK

To Enroll, Please Call:

(800) 370-3006

Or Visit:

<https://ide.myidcare.com/jdbank>

Enrollment Code:

<<XXXXXXXXXX>>

<<Mail Date>>

Notice of JD Bank Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to notify you of a data security incident that may have involved your personal information, including your Social Security number or Tax ID number. We value and respect the privacy of your information, and we sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and the resources we are making available to help you.

What happened?

We recently identified suspicious activity involving a limited number of JD Bank's corporate email accounts. We immediately changed the passwords for the email accounts and brought in independent computer forensic experts to help us investigate how the incident occurred, whether any information in the accounts was at risk, and steps we can take to prevent this from happening again. Our forensic experts determined that an unauthorized individual may have had access to a limited number of corporate email accounts between February 19 – 26, 2019. The investigation confirmed that the incident was limited to these email accounts; our banking systems were not affected and remain secure. On April 2, 2019, we determined that your personal information may have been contained in one of the email accounts. While we have no evidence that the unauthorized individual viewed or opened any emails or documents containing your information, out of an abundance of caution we wanted to let you know about this incident and offer you complimentary identity theft protection services.

What information was involved?

Impacted information may have included your name and Social Security number or Tax ID number. Your financial account number may also have been included, however, no additional information was included that would have allowed access to any online account. For a limited number of individuals, their credit card number, driver's license and/or state ID, and date of birth may have been included.

What we are doing:

We want to assure you that we are taking steps to prevent this type of incident from happening in the future. We have changed passwords for all email accounts, implemented additional security methods for email access, and will be retraining employees on recognizing and responding to suspicious computer activity and other security threats. Although we think it unlikely this incident could result in misuse of your information, you can find additional information on steps you can take to protect yourself from identity theft below.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. 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.

What you can do:

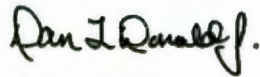
We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (800) 370-3006 or going to <https://ide.myidcare.com/jdbank> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 7 am - 7 pm Central Time. Please note the deadline to enroll is September 17, 2019.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. It is always a good idea to review your credit card and bank statements, and immediately notify your financial institution if you identify any suspicious activity.

Other important information.

If you have any questions or concerns, please call (800) 370-3006 Monday through Friday from 7 am - 7 pm Central Time. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,



Dan Donald
CEO and Chairman



Recommended Steps to help Protect your Information

- 1. Website and Enrollment.** Go to <https://ide.myidcare.com/jdbank> 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 (800) 370-3006 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.alerts.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.

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.