December 1, 2020

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We write to inform you of a data security incident experienced by SK hynix America Inc. ("SKHA"), formerly known as Maxtor Corporation, that<<b2b_text_1("may have")>> involved your personal information. Below please find information on the breach, what data was compromised, and what steps the company is taking going forward.

What happened:

On August 16, 2020, SKHA became aware of a potential compromise to its computer server which<<b2b_text_1("may have")>> contained, in part, your personal information. Upon confirmation of the unauthorized access to SKHA's internal database files, SKHA discovered that it was a victim of a ransomware software attack by a group of computer hackers who operate under the alias "Maze Group," "Maze Team," or "Maze." Since the event, we have been focused on identifying who was impacted and working with a leading IT security solutions company to investigate the attack. Through this investigation, it was ultimately determined that the Maze Group infiltrated SKHA's internal database files from approximately August 3, 2020 to August 17, 2020. On or about August 18, 2020, the Maze Group publicly exposed confidential information, among which your personal information<<b2b_text_2("may have been")>> included, on its website mazenews.top. This website was subsequently taken down.

While we have no reason to believe that any information within the affected server was actually viewed or misused during this compromise, we are providing this notification to you out of an abundance of caution and so that you may diligently monitor your personal information and resources.

What information was involved:

The information on the internal database file that could have been viewed included personally identifiable information including your name, address, and<<b2b_text_3("possibly your")>> Social Security number. At this time, we are not aware of the information being used fraudulently against you.

What we are doing:

In response to the identified incident, we continue to review our technical and organizational controls in order to maintain the safety and security of our data. SKHA has taken every step necessary to address the incident and is committed to helping protect your information. Unfortunately, ransomware attacks have become more common and the data breach experienced by SKHA is similar to security breaches experienced by other companies and industries. Upon learning of this incident, we immediately took steps to enhance the security and monitoring of all information, to help prevent similar incidents from occurring in the future. We retained a leading IT security solutions company to conduct a thorough investigation and are offering you complimentary identity monitoring services.

Credit monitoring

As a safeguard, we have arranged for you to activate, at no cost to you, an online identity monitoring service for one year provided by Kroll. Due to privacy laws, we cannot activate you directly. Information regarding how to activate the complimentary identity monitoring service is below. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **February 21, 2021** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

What you can do:

We also want to inform you of additional steps you can take to help protect yourself. We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. We have provided additional information below about steps you can take to help protect yourself against fraud and identity theft.

Free fraud alert information

Whether or not you activate the identity monitoring services, 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. You may call one of the following three nationwide credit reporting companies to place your Fraud Alert: Equifax, TransUnion, 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. You may call (877) 322-8228 or make a request online at www.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, we recommend that you call your local law enforcement agency and file a police report. You should obtain a copy of the report because 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 www.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, you can visit the FTC's website at www.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 above. 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.

For more information:

We regret any inconvenience this may have caused, but it is important to us that your data remains safe and secure. We are notifying you so that you can take action you deem appropriate to help protect your information. Please feel free to contact Kroll at 1-833-910-3507, from 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, if you have questions.

Sincerely,

Byungsuh Min
Corporate Secretary

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements/personal account statements and monitoring your free credit report to detect errors resulting from the security breach and for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

For New Mexico residents: You are hereby notified of your rights pursuant to the federal Fair Credit Reporting Act.

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, www.oag.dc.gov, 1-202-727-3400.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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 Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, 1-401-274-4400, www.riag.ri.gov.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.