29309

HAMILTON PARKER

<<Date>> (Format: Month Day, Year)

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

Notice of Data Breach

Dear <<first_name>> <<last_name>>,

Hamilton Parker has deep roots in central Ohio's commercial and residential building sectors that has allowed us to grow and serve our customers. Our expansion would not have been possible without our customers and as a result of this strong relationship, we owe transparency to those who have helped us over the years. Accordingly, Hamilton Parker is writing to inform you of a recent security incident that may have inadvertently exposed your personal information and to provide you with steps you can take to help protect your information in response.

What Happened?

In late January of this year, we initially discovered that we were the victim of a ransomware attack that encrypted our systems. Upon discovery of the security incident, we engaged legal counsel and a data breach remediation firm to conduct an investigation into the scope of the security incident. As you can imagine, such investigations take time and can result in additional findings. After conducting an investigation consistent with any measures necessary to determine the scope of the breach, we are providing notice to you now because our investigation has determined that an unauthorized third-party may have had access to your information.

What Information Was Involved?

At this time, it is our understanding that the type of information that may have been accessed includes your full name, postal address, bank account number, and Social Security number.

What We Are Doing

Following discovery of the security incident, we immediately initiated remedial security measures to further safeguard your information. These measures included, among others, retaining legal counsel and a data breach remediation firm to help investigate the scope of the security incident, implementing multi-factor authentication, leveraging information technology resources to recover and rebuild our systems, initiating a password reset for all system end users, and installing endpoint detection and response software, among various other measures.

We are also taking steps to implement additional safeguards, review policies and procedures relating to data privacy and security, and enhance employee cybersecurity training in order to help protect against similar incidents in the future. In addition, we will be notifying regulators of the event should we be so required.

What You Can Do

We want to make sure you are aware of steps you may take to guard against potential identity theft or fraud. Please review the attached supplement, Steps You Can Take to Protect Your Information, for detailed information about additional actions you can take to further help protect your personal information.

As an added precaution, Hamilton Parker has secured the services of Kroll, a cybersecurity firm, to provide identity monitoring services at no cost to you for twelve months. These services include Single Bureau Credit Monitoring, Fraud Consultation, and Identity Theft Restoration services.. Kroll is a global leader in risk mitigation and response, and their team has extensive experience with data breach response. Below are the instructions on how to activate these services:

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **<<b2b_text_6(activation deadline)>>** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included in the attached supplement.

For More Information

We have also established a call center with Kroll to respond to any questions you may have about the security incident and the services offered to you. Please call (866) 869-0253, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding some major U.S. holidays, with any questions. Please have your membership number ready.

Sincerely,

Adam Lewin
CEO, Hamilton Parker

Christie Miller
President, Hamilton Parker

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

You can take the following steps to help protect your information and be proactive in regard to your tax returns:

IRS Identity Protection PIN. The Internal Revenue Service ("IRS") offers the option to create an Identity Protection PIN ("IP PIN") to prevent someone else from filing a tax return using your Social Security number. The IP PIN is a six-digit number known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. For more information on how you can opt-in to using an IP PIN, please visit www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

IRS Form 14039. If you discover another tax return has been filed with your Social Security number, you will use IRS Form 12039 to alert the IRS. When completing this form, you will indicate that someone has stolen your identity and it has affected your tax account since they have filed a return using your identifying information. You will also provide information about the tax year affected and the last return you filed prior to the identity theft.

Contact the IRS or the Ohio Department of Taxation. Both agencies can help determine if your personal information has been used to file a tax return without your permission and provide you with additional steps you can take to help protect against identity theft. You can reach the IRS by phone at 1-800-908-4490 and the Ohio Department of Taxation by phone at 1-800-282-1780.

Review your Social Security Statement. You also may review earnings posted to your record on your Social Security Statement. The Statement is available online to workers age 18 and older. To get your Statement, go to www.ssa.gov/myaccount and create an account. If you suspect someone is using your number for work purposes, you should contact the Social Security Administration ("SSA") to report the problem. The most convenient way to reach the SSA is to visit www.ssa.gov, or you can call toll-free at 1-800-772-1213.

You can take the following additional steps to help protect your personal information more generally:

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'll 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 help 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.

Contact Information for the three Nationwide Credit Reporting Agencies.

Equifax	**Experian**	**TransUnion**
PO Box 740241	PO Box 2104	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-685-1111	1-888-397-3742	1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant over the next twelve to twenty-four months by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft.

It is recommended that you periodically obtain and review a copy of your credit report from each of the three nationwide credit reporting agencies, and have any information relating to fraudulent transactions deleted. You may obtain a copy of your credit report, free of charge, once every twelve 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).

Your Rights Under the Fair Credit Reporting Act. You have several rights related to the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. To learn more about your rights under the Fair Credit Reporting Act, please visit www.consumerfinance.gov/learnmore/ or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

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 Additional Identity Theft Resources. 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 ("FTC"). You may contact the FTC by phone at 1-877-IDTHEFT (438-4338) or by mail at Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You may also visit www.identitytheft.gov.

In addition, the FTC provides additional resources with steps you can take to help protect against identity theft. For more information, please visit www.ftc.gov/bcp/edu/microsites/idtheft/. A copy of *Taking Charge: What to Do if Your Identity is Stolen*, a comprehensive guide from the FTC to help you guard against and deal with identity theft is available on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

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 Attorney General's office in your home state. You may also contact the Attorney General's office for information on how to prevent or minimize the risks of identity theft.

Reporting of Identity Theft and Obtaining a Police Report. Please review your account statements for any suspicious activity. If you detect any suspicious activity on an account or suspect identity theft, you should immediately report it to the financial institution or company with which the account is maintained. You have the right to obtain any police report filed concerning this incident. If you are the victim of identity theft, you also have the right to file and obtain a copy of a police report.

HAMILTON PARKER

[XX], 2023

[First Name] [Middle Name] [Last Name]
[Address 1]
[Address 2]
[City], [State] [Zip Code]

Supplement to Notice of Data Breach

Dear [First Name] [Last Name]:

We write to supplement our Notice of Data Breach mailed to you on March 30, 2023. That Notice indicated Hamilton Parker had contracted with Kroll to provide you with identity monitoring services at no cost to you for twelve months. As a Massachusetts resident, you are actually entitled to ***eighteen months*** of identity monitoring services. We sincerely apologize for any confusion.

As noted in our previous Notice, we have established a call center to respond to any questions you may have about the security incident and the identity monitoring services offered to you as a Massachusetts resident. Please call (**866) 869-0253** toll-free, Monday through Friday from 9:00 a.m. to 6:30 p.m. ET, with any questions you may have.

Yours truly,

Adam Lewin
CEO, Hamilton Parker

Christie Miller
President, Hamilton Parker

COLUMBUS
1865 Leonard Ave.
Columbus, OH 43219
614.358.7800

DELAWARE
188 E. William St.
Delaware, OH 43015
740.363.1196

CINCINNATI
2931 E. Kemper Rd.
Sharonville, OH 45241
513.276.4840

CLEVELAND
1100 Resource Dr.
Brooklyn Heights, OH 44131
216.351.2030