



THE WOLFF COMPANY

— SINCE 1949 —

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

RE: Notice of Data Breach

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Wolff Principal Holdings, LP dba The Wolff Company (“The Wolff Company”) writes to notify you of a recent incident that may affect the security of some of your personal information. While there is currently no evidence that your information has been misused as a result of this incident, we are providing you with information about the incident, our response to it, and information related to what you may do to better protect your personal information, should you feel it appropriate to do so. This event is unrelated to the event about which we notified you on April 10, 2020.

What Happened? The Wolff Company recently became aware of suspicious activity affecting its computer systems. We took steps to secure our systems and began working with outside computer forensics specialists to determine the nature and scope of the incident. The investigation determined that an unknown intruder accessed our systems on February 13, 2020. The investigation also determined that the unknown intruder potentially copied a limited amount of data from The Wolff’s Company’s system. Although we are not aware of the misuse of any of this information, the Wolff Company undertook a thorough review of the contents of the copied data to determine whether sensitive information was present.

On June 2, 2020, The Wolff Company completed its review of the files potentially copied by the unauthorized actor and determined your personal information was located within one of the impacted files. To date, we are unaware of any actual or attempted misuse of your personal information as a result of this incident.

What Information Was Involved? Our investigation determined that at the time of the incident the affected data included your <<b2b_text_1(ImpactedData)>><<b2b_text_2(ImpactedData)>>.

What We Are Doing. Information, privacy, and security are among our highest priorities. The Wolff Company has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to improve the security of our systems by implementing advanced threat detection and response solutions across all endpoints and updated our risk management platform. As a precautionary matter, we also provided relevant regulatory notices. We are continuously working to increase our organizations cybersecurity posture by aligning with the latest frameworks and best practices.

While, to date, we have no evidence of actual or attempted misuse of your information as a result of this incident, we are notifying you so that you may take further steps to better protect your personal information should you feel it is appropriate to do so. We also secured the services of Kroll to provide identity monitoring services at no cost to you for twelve (12) months. For more information on these services, please review the enclosed “Steps You Can Take to Help Protect Your Information.”

What You Can Do. You may review the information contained in the attached “Steps You Can Take to Help Protect Your Information.” You may also activate to receive the identity monitoring services we are making available to you as we are unable to activate these services on your behalf.

For More Information. We understand that you may have questions about this incident that are not addressed either in this letter or future notices. If you have additional questions, please call our call center at [1-800-800-8000](tel:1-800-800-8000), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. You may also contact The Wolff Company by mail at 6710 East Camelback Road, Scottsdale, Arizona, 85251.

The Wolff Company takes the privacy and security of the personal information in our care seriously. Please let us know if you have any questions.

Sincerely,

A handwritten signature in cursive script that reads "Jay Petkunas".

Jay Petkunas

CEO

Wolff Principal Holdings LP

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Activate Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **October 15, 2020** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Monitor Your Accounts

In addition to enrolling in the complimentary services detailed above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160

Woodlyn, PA 19094

1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000

Chester, PA 19016

1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069

Atlanta, GA 30348

1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ 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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.

¹ 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.