THE WOLFF COMPANY

Via U.S. Mail

October 27, 2015

Re: Notice of Potential Data Incident at Transcontinental Fund Administration, Ltd.

Dear Partner:

You are receiving this communication because you are a limited partner in a Wolff-sponsored fund that is currently administered by Transcontinental Fund Administration, Ltd., of Chicago and the Cayman Islands (hereinafter "TFA"). As a third-party fund administrator, TFA provides accounting services, coordinates investor capital calls and distributions, and manages investor relations communication, among other services, across several Wolff funds.

In late September 2015, TFA notified us that, while still employed at TFA, one of its former employees had allegedly taken from its Chicago office information concerning multiple TFA clients, including a number of Wolff-sponsored funds that TFA administered. This information may have included limited partner names, addresses, tax identification numbers, social security numbers, and investment amounts. Upon learning of the alleged incident, TFA immediately implemented its loss-recovery processes, commenced a civil action against the former employee, and secured a temporary restraining order against the former employee to prohibit publication or sharing of the information allegedly taken. TFA also immediately contacted both the FBI and municipal law enforcement authorities, both of which have open and ongoing investigations. We are working to ensure the safe return of the information, which includes working closely with law enforcement and TFA.

As of this time, we have no evidence that any sensitive information that was allegedly taken has been used for fraud or identity theft purposes. We are informing you of this incident as a precaution and to help safeguard you from potential misuse of your sensitive information. As always, we recommend that you remain vigilant for incidents of fraud and identity theft. For more information on how you can help protect yourself, please review the enclosed *Steps You Can Take to Protect Yourself From Identity Theft.*

Thank you for your understanding. If you have any questions or concerns, please do not hesitate to contact us at (480) 315-9595.

Sincerely,

Fritz H. Wolff Jay Petkunas Steve Jasa

6710 E. Camelback Rd. | Suite 100
Scottsdale | Arizona 85251
(P) 480-315-9595 | (F) 480-315-1739

Steps You Can Take to Protect Yourself From Identity Theft

1. **Review your account statements and credit reports and notify law enforcement and Essex of suspicious activity.**

Even if you do not feel the need to register for a credit monitoring service, as a precautionary measure, we recommend that you regularly review statements from your bank, credit card, and other accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9532	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com
1.888.766.0008	1.888.397.3742	1.800.680.7289

When you receive your credit reports, look them over carefully. Look for accounts that you did not open and/or inquiries from creditors that you did not initiate. Also check to see if your personal information on the credit report is accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend that you remain vigilant in your review of your account statements and credit reports. You should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement and/or the Federal Trade Commission. A copy of a police report may be required by creditors to clear up your records.

2. **Consider placing a fraud alert or a credit freeze on your credit files.**

If you suspect that you may be a victim of identity theft, consider placing a fraud alert or a security freeze (also called a credit freeze) on your credit file. Security freeze laws vary from state to state. For more information about fraud alerts and security freezes, please see the Federal Trade Commission's guidance at http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes.

3. **Protect your passwords.**

You can minimize the threat of identity theft by improving your password practices. Use different passwords for all your accounts. Make those passwords strong with at least eight characters, including a mix of letters, numbers, and symbols ($%#!*@). Change your passwords from time to time. For additional guidance on passwords and securing your accounts, see http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/passwords-and-securing-your-accounts.

4. **Fight "phishing"--don't take the bait.**

Scam artists "phish" for victims by pretending to be banks, stores, government agencies, or other trusted sources. They do this over the phone, by email, and by postal mail. Do not respond to any request to verify your account number or password. Legitimate companies do not request this kind of information in this way. If an email looks suspicious, don't click on any links in that email.

5. **Learn more about how to protect yourself from identity theft.**

You may wish to review the Federal Trade Commission's guidance on how consumers can protect themselves against identity theft. For more information:

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580
www.ftc.gov/idtheft
1.877.ID.THEFT (1.877.438.4338)