INVESTACORP® MEMBER • FINRA/SIPC

April 19, 2012

Office of the Attorney General
State of California
P.O. Box 944255
Sacramento, CA 94244-2550

Re: Information Security Breach Notification

Dear Sir or Madam:

This letter is for the purpose of notifying your office that a vendor of the clearing broker-dealer utilized by Investacorp, Inc. ("Investacorp") was involved in a data breach incident that potentially affected five clients who are residents of California. Investacorp is an independent federally regulated broker-dealer and uses National Financial Services LLC, a Fidelity Investments company ("NFS"), to clear and process its securities transactions. NFS is also a federally regulated broker-dealer and as such, is subject to the privacy and safeguarding requirements set forth under the Securities and Exchange Commission's Regulation S-P. On or about March 12, 2012 Invetsacorp was notified by NFS that an NFS vendor had inadvertently shared electronic files that included personal information on a number of Investacorp clients with another federally regulated broker-dealer that also clears through NFS. Unfortunately, the personal information included the name, social security number, and account level data of five clients.

It is Investacorp's understanding that the vendor conducted an internal investigation and then worked with the broker-dealer to delete the files from its systems. Investacorp has received an executed affidavit from the broker-dealer certifying the destruction of the electronic files. A copy of its affidavit is enclosed with this letter. The vendor then provided NFS with a final report of the investigation, which included a root cause analysis and its remediation plans. The vendor has also reported that it updated its internal processes concerning electronic and will provide additional security training to its employees. Also included is a copy of the memorandum issued by NFS more fully describing the incident and the remediation plans.

While it is important to note that the vendor responsible for this data breach was not, in any way, a vendor of Investacorp, the incident ultimately impacted five clients residing in your state. Investacorp does not currently believe NFS will be independently notifying your office of this data breach incident. Nonetheless, we felt it necessary and prudent to provide this notification in the event NFS does not do so. Over the next few days, NFS will also be sending a notification letter, a copy of which is attached. The letter describes the incident and provides the clients with an opportunity to enroll for one year of credit monitoring from Equifax, at NFS's expense.

If you have any questions regarding this incident, please contact me at 305-557-3000 x332.

Sincerely,

Rick Slavik
Assistant Director
Compliance Department

Enclosures

CERTIFIED RETURN RECEIPT

4400 Biscayne Blvd., 11th Floor, Miami, Florida 33137
(305) 557-3000, NATIONAL (800) 327-7900, FAX (305) 362-9650

DATE

Client name
Client address

Promotional Code: [PROMO CODE #]

Dear client:

We are writing in regard to a recent matter that involved some personal information about your [NAME OF CORRESPONDENT] account that is held with National Financial Services LLC, a Fidelity Investments company. On November 29, 2011 a Fidelity vendor inadvertently shared electronic files that included personal information with one of our other broker-dealer client firms. The information that was sent included your name, Social Security number, mailing address, account number, holdings, balances, and historical account level data.

On February 13, 2012 our other client firm notified our vendor regarding issues with the electronic file. Upon learning of the matter, our vendor conducted an internal investigation and notified Fidelity of the matter on February 17, 2012. The vendor then worked with the other client firm to delete the files from their systems, which it completed on February 23, 2012.

The distribution of this information was limited to one correspondent broker-dealer client firm. Fidelity presently has a written agreement that includes confidentiality clauses with the other client firm. In addition, our other client firm recognized the sensitivity of the information they received and worked diligently to remove the information from their systems promptly. While we do not believe your personal information has been or will be misused, we thought it necessary and prudent to inform you in writing of the incident. Fidelity deeply regrets this situation and is keenly aware of how important the security and privacy of your personal information is to you. The vendor has provided us with a final report of the investigation, which included a root cause analysis and its remediation plans. The vendor has also reported that it updated the internal processes concerning data that is sent outside of the network and will also be providing additional security training to its employees.

As a precautionary measure, we recommend that you remain vigilant for incidence of fraud and identity theft by reviewing account statements, monitoring free credit reports, and promptly reporting any suspicious activity. Additionally, Fidelity has arranged for you to enroll, at your option, in a credit monitoring service for one year at no cost to you. This service allows you to monitor your credit and to detect any unusual activity that may affect your personal financial situation. The service is provided by Equifax, a major credit reporting company. For details on how to enroll in this service and for additional ways you may protect yourself, please refer to the enclosed instruction sheet.

We take the protection of customer information very seriously and sincerely apologize for any concern or inconvenience this matter may cause you. If you have any questions regarding this situation, please feel free to call [Fidelity] at [NUMBER], or your registered representative at his/her place of business

Sincerely,

William S. Duserick

William Duserick
Chief Privacy Officer

CREDIT MONITORING INSTRUCTION SHEET

Fidelity INVESTMENTS

We have arranged with Equifax Personal Solutions to help you protect your identity and your credit information at no cost to you. The steps to follow are:

1. Enroll in Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product. This product is being provided at no cost to you.
2. Additionally, you may choose to adopt an increased level of protection by placing a fraud alert on your credit file at Equifax and the other two credit reporting agencies.

Enroll in Equifax Credit Watch™ Gold with 3-in-1 Monitoring

Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit reporting agencies. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your Equifax, Experian, and TransUnion credit reports
- Wireless alerts and customizable alerts available
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Up to $1 million in identity theft insurance with $0 deductible, at no additional cost to you †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information
- 90 day Fraud Alert placement with automatic renewal functionality (available online only)

How to Enroll

To sign up online for **online delivery** go to www.myservices.equifax.com/tri

1. Register: Complete the form with your contact information (name, gender, address, date of birth, Social Security number and telephone number) and click the "Continue" button. Complete the form with your email address, create a User Name and Password, enter the Promotion that is at the top of the first page of this letter in the "Promotion Code" box. The Promotion Code eliminates the need to provide a credit card number for payment. Then click the "Accept Terms & Conditions" button. All of the information that you enter is in a secured environment.
2. Verify ID: The system will then ask you to answer up to four security questions. The questions and answers support the Equifax Identity Verification Process. Please answer the questions and then click the "Submit Order" button.
3. Order Confirmation: This page shows you your order. Please click the "View My Product" button to access the product features.

To sign up for **US Mail delivery**, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. Promotion Code: You will be asked to enter your promotion code as provided at the top of your letter.
2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security number.
3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax can not process your enrollment.
4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

† Identity theft insurance underwritten by subsidiaries or affiliates of Chartis Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions. This product is not intended for minors (under 18 years of age).

ADDITIONAL STEPS TO PROTECT YOURSELF

Fidelity INVESTMENTS

Directions for Placing a Fraud Alert

You may want to consider placing an initial fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies. The agency that processes your fraud alert will notify the other two credit reporting agencies on your behalf. An initial fraud alert stays on your credit report for 90 days. When you place this alert on your credit report, you will receive information about ordering one free credit report from each of the credit reporting companies. Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your Social Security number, address(es), full name and employer(s). Notify the credit reporting companies if any information is incorrect.

Equifax: 877-478-7625 www.equifax.com; PO Box 740241, Atlanta GA, 30374-0241
Experian: 888-397-3742 www.experian.com; PO Box 9532, Allen TX 75013
TransUnion LLC: 800-680-7289 www.transunion.com; PO Box 6790, Fullerton CA 92834

You can also obtain information from the credit reporting agencies to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

Directions for Obtaining a Credit Report

Please remember that while this matter may not involve significant risk, it is always good practice to take sensible steps to protect yourself by regularly reviewing your account statements and your credit report. As you may know, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the major credit reporting agencies. You may obtain a free copy of your credit report by calling 1-877-FACT ACT (1-877-322-8228) or by visiting www.annualcreditreport.com.

Resources

Additional information on identity theft is available from the Federal Trade Commission (FTC). You may contact the FTC to report any incidents of identity theft and to obtain guidance about protecting against identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
Toll-free Identity Theft Helpline: 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261
Website: www.ftc.gov/bcp/edu/microsites/idtheft/

For Massachusetts Residents:

Police Reports

Under Massachusetts law, you have the right to obtain any police report filed in regard to a breach of security. Because of the accidental nature of this incident, which did not involve a theft, a police report was not filed. If you are the victim of identity theft, you have the right to file a police report and obtain a copy of it.

Directions for Placing a Security Freeze

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

Fidelity INVESTMENTS

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

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 the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze

For North Carolina Residents:
Additional information about steps to avoid identity theft is available from the following sources:
North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: 1-877-566-7226
Website: www.ncdoj.com/Protect-Yourself/2-4-3-Protect-Your-Identity.aspx

In November 2011, a National Financial (NF) correspondent requested data transmission feeds from one of our vendors, First Rate, who provides performance reporting for certain customers of your firm. Specifically, the NF correspondent was requesting a copy of the data that NF sends to First Rate on its behalf to support and perform testing on an internal project. On November 29, 2011, First Rate sent the transmission feeds that contained data from November 23, 2011 and November 25, 2011. First Rate failed to edit the feeds to only include data that belonged to the requesting correspondent. As a result, the transmission included data for certain end client accounts that belonged to other correspondent firms, including yours. This data included: names, Social Security or Tax Identification numbers, addresses, account numbers, holdings, balances, securities, historical account level data and Streetscape ID. The NF correspondent stored the data transmission feeds in a test region and subsequently loaded it to a test database. As a majority of the data on the transmission feed was for their own customers, they did not realize that the data feeds included accounts that did not belong to their firm until very recently. On February 13, 2012, the correspondent firm contacted First Rate because they could not identify some of the accounts. Upon learning of the matter, First Rate conducted an internal investigation and notified NF of the matter on February 17, 2012. First Rate then worked with the correspondent to delete the files from their systems; this was completed on February 23, 2012. The vendor provided NF with a final report of the investigation, which included a root cause analysis and their remediation plans on March 2, 2012.	
PROBLEM RESOLUTION STEPS	First Rate has updated its internal process for requests c data that is sent outside of their network. These types of requests must now go through their Security Committee will require the completion of a transmission authorizatio form. The transmission authorization form requires five signatures to verify that: 1) the data owner has authorize in writing, the transfer of the data to the requestor; 2) the requestor has written authorization to accept the data; 3) content of the data is reviewed to confirm the existence/r existence of multi-firm data and sensitivity of the data to assess risks in delivery of data to requestor; 4) the transmission mode is validated to confirm the data is delivered in accordance with security requirements; 5) th source and destination servers are validated and authori to receive the data; and 6) storage location of the files ar properly protected and categorized. Additionally, a review of the location and storage of curre client files will be conducted to ensure that data is clearly marked. Lastly, additional security training will be provided to employees to familiarize them with the new process and emphasize the existing security requirements around protecting client data.

First Rate 1903 ASCENSION BLVD. • ARLINGTON, TX 76006 • P: 817.525.1900 • F: 817.525.1903 • www.FirstRate.com
YOUR PERFORMANCE SOLUTION PARTNER

Affidavit of Data Destruction

My name is Tracy Stuart. I am competent to make this affidavit. The facts stated in this affidavit are within my personal knowledge and are true and correct.

"On 2/17/2012, First Rate notified SunTrust of a security incident that involved the inadvertent disclosure of confidential information from First Rate to SunTrust, specifically two days of extract files for the dates of 11/23/2011 and 11/25/2011 ("Extract").

"In the notification, First Rate requested that all data related to the Extract be removed from SunTrust computers and all data storage environments, including, but not limited to any backup tapes, backup drives, or other data archival devices.
"In accordance with SunTrust's communications with First Rate, I, the undersigned, do hereby certify and attest that the Extract was deleted from any and all SunTrust computers and all data storage environments, including, but not limited to any backup tapes, backup drives, or other data archival devices.

"SunTrust further acknowledges that the Extract did not leave SunTrust's facilities and remained at all times within SunTrust. The Extract was not printed by SunTrust, and no hard copies of the Extract exist within SunTrust.

"SunTrust agrees to hold any residual non-tangible information related to the Extract in strict confidence and, absent a Court Order or otherwise required by law, shall not disclose the existence of any such residual information to any persons."

Tracy K. Stuart
Signature

Tracy K. Stuart
Printed Name

SIGNED under oath before me on March 16, 2012.

Notary Public, State of Georgia

JEFF ROUGEAUX
Notary Public
Cherokee County
State of Georgia
My Commission Expires Feb 23, 2016