

SunGard EXP Mailing  
350 Automation Way  
Ironton, AL 35210

June 18, 2008

Client Name: {Male Initial} {Last Name}  
{ADDRESS (No.)}  
{Address 2}  
{City} {STATE} {Zip Code}

Dear {Last Name}:

We sincerely regret to tell you that a laptop computer belonging to an employee of SunGard Data Systems Inc.'s Phase3 business unit ("Phase3") was lost on May 11, 2008, and may have contained certain personal information regarding you and your account at Newedge USA, LLC ("Newedge")(formerly known as Preferred Trade and Fimat Preferred). Phase3 is a securities processing system that processes trade data for retail and institutional brokerage firms such as Newedge.<sup>1</sup> Although we are not aware that any of your personal information has been misused, the laptop has not been found.

Specifically, the laptop was lost on May 11, 2008, when a Phase3 employee left a bag containing the laptop in a taxi at an airport. The laptop was password-protected, but the data on the laptop was not encrypted. Because the employee was working with your data as part of a back-office system migration for Newedge, the laptop contained certain Newedge customer account information. Phase3 notified Newedge of the incident on June 6, 2008. The laptop *may have* contained your name and Social Security Number, and potentially other information about you, including date of birth, home address and telephone number, net worth, annual income and your Newedge account number.

Phase3 deeply regrets this incident and any inconvenience it may cause you. Again, there is no indication that any information has been misused, and we are continuing to monitor the situation. However, we wanted to inform you of these circumstances and advise you on the precautions you should take and how we can help. We recommend that you take steps to protect yourself from the possible misuse of your personal information.

#### **What Phase3 Is Doing to Help Protect Your Privacy and Security**

In coordination with Newedge, Phase3 has made arrangements with *ConsumerInfo.com, Inc.*, an Experian<sup>®</sup> company, to provide you with two years of credit monitoring, free of charge. This product, known as **Triple Alert**, will identify and notify you of key changes in your three national credit reports that may indicate fraudulent activity.

---

<sup>1</sup> Phase3 is not a US-registered broker-dealer. Phase3's only affiliation with Newedge is as a service provider.

Your free two-year membership includes:

- Daily monitoring of all three credit files with Experian, Equifax<sup>®</sup> and TransUnion<sup>®</sup>
- Email alerts if key changes are detected on any of your three credit reports
- Monthly "No Hit" alerts, if applicable
- Dedicated team of fraud resolution representatives for victims of identity theft
- \$25,000 in identity theft insurance provided by Virginia Surety Company, Inc. with no deductible.\*

\*Due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York.

You have ninety days to activate this membership, which will continue for two full years. We encourage you to activate your credit monitoring membership quickly.

Please visit <http://partner.consumerinfo.com/phase3laptop> on the Experian website and enter the activation code provided below. You will be instructed on how to initiate your online membership.

Your Credit Monitoring Activation Code is: «Code»

If you have issues with the credit monitoring website, please call the Experian ConsumerInfo customer care line at 1-866-252-0121.

#### **Further Steps You Can Take to Protect Yourself**

In addition to registering for these credit monitoring services, there are other things that you can do to help protect yourself from fraud or identity theft.

(1) Review your account statements and credit report statements for any suspicious/unauthorized activity and remain vigilant for incidents of fraud and identity theft.

(2) Request a copy of your credit report at [www.annualcreditreport.com](http://www.annualcreditreport.com). You are entitled to one free report per year from each of the three major credit reporting bureaus:

<b>Credit Bureau</b>	<b>Credit Report Toll Free No.</b>	<b>Website</b>
Equifax	1-800-685-1111	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	1-877-322-8228	<a href="http://www.transunion.com">www.transunion.com</a>

(3) Contact one of the three major credit reporting bureaus to request that a "fraud alert" be placed on your credit file. A fraud alert indicates to anyone requesting your credit file that you may be a victim of fraud or identity theft. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the creditor should take steps to verify that you have authorized the request. If it cannot, the request should not be satisfied. There is no charge for this service, and it is easy to request. To activate a fraud alert, call any one of the three major credit bureaus listed below. As soon as you alert one credit bureau, it will notify the other two to place fraud alerts on your account.

Equifax 1-888-766-0008 P.O. Box 740241 Atlanta, GA 30374-0241 <a href="http://www.equifax.com">www.equifax.com</a>	Experian 1-888-397-3742 P.O. Box 9532 Allen, TX 75013 <a href="http://www.experian.com">www.experian.com</a>	TransUnion 1-800-680-7289 P.O. Box 6790 Fullerton, CA 92834-6790 <a href="http://www.transunion.com">www.transunion.com</a>
--	--	---

(4) Contact the credit reporting bureau that provided your credit report if you do not understand an item on it. Report any suspected incidents of identity theft to your local police or sheriff's office and the Federal Trade Commission at 1-877-IDTHEFT (438-4338).

(5) You may also place a security freeze on your credit report by contacting the national credit reporting bureaus listed above. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. **Therefore, using a security freeze may interfere with or delay your ability to obtain credit.** The credit reporting bureau may charge a reasonable fee (typically from \$5-\$20) to place a freeze or temporarily or permanently remove a freeze. You should contact the consumer reporting bureaus listed above for additional details on credit freezes.

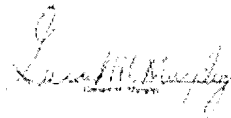
Further, a website has been established at [www.sungard.com/phase3lostlaptop](http://www.sungard.com/phase3lostlaptop) to provide you with additional information about this incident and how to protect your identity. We recommend you review this information and consider taking these steps to help guard against potential identity theft.

Both SunGard Data Systems Inc. and Phase3, as well as Newedge, take this incident and the protection of confidential information very seriously. Beyond the services provided above, we are taking immediate steps to minimize the likelihood of similar events in the future, including a top-to-bottom review of the company's information security policies, limiting the amount of personally identifiable information stored on devices, and increasing the use of encryption and other protective technologies.

In the event you believe that your account at Newedge has been subject to identity theft resulting from this incident, or in the event you have any other questions relating to your brokerage account at Newedge, please contact Newedge. Should you have any other questions or concerns regarding this incident and/or the protections available to you, you may contact our representative at the following toll-free number: 1-866-520-2413. Outside of the United States, you can call 407-215-2650.

Again, we apologize sincerely for this incident and hope the steps we have instituted help allay any concerns you may have.

Sincerely,



Gerard Murphy  
President and CEO  
SunGard Phase3

cc: Mr. Mike Liciardello  
Director, Equities Sales and Trading  
Newedge USA, LLC