

**North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach:	<u>Newedge USA</u>	PLEASE SUBMIT FORM TO: Consumer Protection Division NC Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 Telephone: (919) 716-6000 Toll Free in NC: (877) 566-7226 FAX: (919) 716-6050
Address:	<u>550 West Jackson Blvd. Suite 500</u> <u>Chicago, IL 60661</u>	
Telephone:	<u>312-441-4745</u>	
Fax:	<u>312-441-4359</u>	
Email:	<u>Eric.nield@newedgegroup.com</u>	

Date Security Breach Reporting Form submitted: June 24, 2008

Date the Security Breach was discovered: June 6, 2008

Estimated number of affected individuals: 21,600

Estimated number of NC residents affected: 570

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): SunGard Phase3

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: Please see attached response

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. Please see attached response If so, please describe the security measures protecting the information: _____

Describe any measures taken to prevent a similar Security Breach from occurring in the future: Please see attached response

Date affected NC residents were/will be notified: June 20, 2008


If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): N/A

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. § 75-65(e))

Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

<input checked="" type="checkbox"/> written notice
<input type="checkbox"/> electronic notice (email)
<input type="checkbox"/> telephone notice
<input type="checkbox"/> substitute notice

Signature:  Date: June 24, 2008

Contact Person, Title: Divonne Smoyer

Address: 1825 Eye Street, NW
Washington, DC 20006-5403

(if different from above)

Telephone: (202) 420-2665 Fax: (202) 420-2201 Email: SmoyerD@dicksteinshapiro.com

**Addendum to North Carolina Security Breach Reporting Form
June 24, 2008**

Q. Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format:

A. On May 11, 2008, an employee of SunGard Phase3 ("Phase3"), which processes trade data for retail/institutional brokerage firms, left a bag containing a password-protected laptop in a taxi at the Ft. Lauderdale-Hollywood International Airport. Phase3 took immediate steps to locate the laptop, but it has not been recovered.

Phase3, in conjunction with experts it had retained for this purpose and Newedge forensic experts, conducted a review of information believed to be on the laptop. This review indicated that the laptop contained data in electronic format belonging to Newedge USA, a Phase 3 client. The review established that the laptop may have contained names and Social Security numbers, and in some instances, dates of birth, home addresses and telephone numbers, net worth, annual incomes and Newedge account numbers of approximately 21,600 individuals, including approximately 570 North Carolina residents.

Q. Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. If so, please describe the security measures protecting the information:

A. The information on the laptop was not password-protected or encrypted. However, the laptop itself was equipped with a password.

Q. Describe any measures taken to prevent a similar Security Breach from occurring in the future:

A. Phase3, and its parent company, SunGard Data Systems Inc., are undertaking a number of additional measures to protect the information stored on their computers, including: encrypting laptops; minimizing the amount of confidential information on laptops; developing new materials and procedures to ensure employees understand and comply with their data security obligations; and retaining experts to review and improve data security policies and develop best practices for the future.

SunGard EXP Mailing
350 Automation Way
Irondale, AL 35210

June 18, 2008

«First_Name» «Middle_Initial» «Last_Name»
«ADDRESS_INFO»
«Address_2»
«City», «STATE» «Zip_Code»

Dear «First_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.¹ 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[®] 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.

¹ 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® and TransUnion®
- 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. You are entitled to one free report per year from each of the three major credit reporting bureaus:

Credit Bureau	Credit Report Toll Free No.	Website
Equifax	1-800-685-1111	www.equifax.com
Experian	1-888-397-3742	www.experian.com
TransUnion	1-877-322-8228	www.transunion.com

(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 www.equifax.com	Experian 1-888-397-3742 P.O. Box 9532 Allen, TX 75013 www.experian.com	TransUnion 1-800-680-7289 P.O. Box 6790 Fullerton, CA 92834-6790 www.transunion.com
--	--	---

(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 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