

May 29, 2008

J. Beckwith Burr

+1 202 663 6695 (t)

+1 202 663 6363 (f)

beckwith.burr@wilmerhale.com

Consumer Protection  
Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001

Re: Notification of Information Security Incident

JUN - 2 2008  
OFFICE OF THE ATTORNEY GENERAL

To whom it may concern:

This letter is to inform you that State Street Bank and Trust ("State Street") will begin notifying individuals who may be affected by the theft of computer hardware containing personal information about certain of State Street customers and employees. While our notification will be made in accordance with the requirements of the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice issued by the OCC, Fed, FDIC, and OTS of March 29, 2005 (the "Interagency Guidance"), this letter is to notify you, pursuant to North Carolina Gen. Stat. § 75-65, of:

- o the nature of the incident;
- o the number of residents of the state affected by such incident at the time of notification; and
- o the steps State Street has taken and plans to take relating to the incident.

In April of 2007, following State Street's announcement of its agreement to acquire Investors Bank and Trust ("IBT"), IBT received a request for certain information from federal regulators. As is common practice, IBT engaged an established legal support service to review its electronic records in order to identify and compile the requested data. In order to provide this service, the vendor loaded IBT data onto computer equipment. That equipment was subsequently stolen from its facility.

Once informed of the theft, State Street conducted a thorough analysis of the complex data set at issue. Based on that analysis, State Street has determined that the stolen IBT data included (1) the name, address, social security number, and date of birth of legacy IBT employees and (2) the name, social security number, and in some cases account number and/or address of certain direct or downstream legacy IBT customers.

The data relates to approximately 45,000 individuals, 700 of whom are North Carolina residents, including both former employees and customers of IBT. There is no evidence to date to suggest

Page 2

that the data has been misused (or to suggest that legacy State Street customers and employees are impacted).

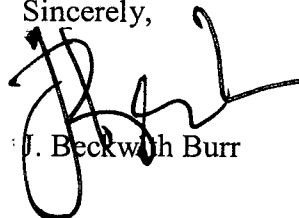
In accordance with the Interagency Guidance, since learning of the incident, State Street has:

1. Contacted local and federal law enforcement, as well as the office of the US Attorney;
2. Notified its primary Federal regulator, the Federal Reserve Board, and filed a Suspicious Activity Report;
3. Cooperated with federal law enforcement, which is actively investigating the incident;
4. Conducted a thorough investigation of the incident, including an assessment of whether or not the theft created any prospective data security risk;
5. Identified the sensitive personal information about employees and direct or downstream customers on the stolen equipment;
6. Monitored customer accounts for unauthorized or unusual activity and enhanced certain security procedures as a precautionary measure to prevent/detect data misuse;
7. Notified its institutional clients whose customers' personal information was on the stolen equipment; and
8. Made arrangements to notify affected individuals about the incident in accordance with the Guidelines, offer premium credit monitoring, ID theft insurance, and ID theft resolution services, and provide additional information about prevention and detection of ID theft including information about credit alerts and credit freezes.

We have attached a sample copy of the notification letters that will be sent to affected individuals beginning today. If you have additional questions about this incident, please feel free to call me at (202) 663-6695.

burr

Sincerely,



J. Beckwith Burr



STATE STREET.

State Street Bank and Trust Company  
200 Clarendon Street  
Boston, MA 02116

Dear [ ]

I am writing to let you know about the theft of computer equipment from a third party vendor engaged by Investors Bank & Trust Company ("IBT"), which was recently acquired by State Street in July 2007. IBT provided global custody, transfer agency, accounting and benefit payment services to a variety of fund shareholders, private clients and pension retirees. Because the stolen equipment contained data with certain personal information about you, we want to make sure that you are aware of the incident. In addition, although at this time we have no evidence to suggest that the data has been misused, we want to ensure that you have the information and tools you need to prevent and detect any misuse of your information.

#### Background

Shortly after State Street announced its agreement to acquire IBT, the company received a request for certain information from federal regulators relating to the acquisition of a public company. As is common practice, the company engaged an established legal support service to review IBT's electronic records in order to identify and compile the requested data.

In order to provide this service, the vendor loaded IBT data onto computer equipment, which was subsequently stolen from its facility. We have been in close contact with law enforcement, which is conducting a criminal investigation of the theft, and we have been conducting our own analysis of the data contained on the equipment.

Based on this investigation and our analysis, we believe that the stolen equipment contained certain personal information such as your name and social security number. Even with this information, we have controls designed to safeguard your accounts from being accessed.

Although we have no evidence suggesting that your relevant personal information on the equipment has been misused, we take our obligation to help you protect your information very seriously, and deeply regret that this has happened.

## Credit Monitoring and Identity-Theft Assistance

To help protect you against any possible misuse of this data, we have engaged ConsumerInfo.com, Inc., an Experian® company, to provide you with two years of free credit monitoring.

This credit monitoring membership will monitor and alert you about key changes in your three national credit reports that may help you identify fraudulent activity. The complimentary two-year membership in Triple Advantage<sup>SM</sup> Premium includes:

- Daily monitoring of your three national credit files from Experian, Equifax® and TransUnion®
- Notifications alerting you of any key changes to your credit reports which may help you identify possible fraudulent activity
- Monthly "no hit" alerts confirming the absence of key changes
- Monthly credit score updates
- One, free three-bureau credit report upon enrollment and unlimited access to your Experian credit report for the duration of the membership
- Access to a dedicated team of fraud resolution representatives if you should become a victim of identity theft
- Identity theft insurance
- Helpful information on preventing identity theft, as well as various financial calculators and tools

## Enrollment

You may enroll online, or by telephone. If you have questions or need help enrolling, toll-free registration assistance is available in both English and Spanish, seven days per week. You will be asked for the Activation Code shown below to activate this membership, regardless of the enrollment method you choose.

Your personal credit monitoring activation code is XXXXXXXXXX.

- To sign up online, please visit <http://partner.consumerinfo.com/statestreet> and follow the instructions. If you sign up online, all credit reports and alerts will be delivered via email.
- To sign up by telephone, dial 866-584-9479. If you sign up by telephone, all credit reports and alerts will be delivered by the US Post Office.

To take advantage of the free credit monitoring membership, you must enroll within ninety (90) days from the date of this letter. According to Federal law, we are not able to activate this membership for you.

## Additional Steps

There are several additional steps you can take to further protect your credit.

First, as always, you should review your bills and account statements upon receipt for unauthorized activity.

You can also request a free credit report annually from each of the three credit reporting companies.

These reports can be obtained by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com) or by contacting each of the three companies directly:

Equifax  
P.O. Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
1-800-525-6285

Experian  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

TransUnion  
P.O. Box 2000  
Chester, PA 19022  
[www.transunion.com](http://www.transunion.com)  
1-800-680-7289

The Federal Trade Commission (FTC) recommends that you also consider placing a fraud alert on your credit file, which tells creditors to contact you before they open any new accounts or change your existing accounts. (Please note, however, that this may delay your ability to obtain credit.) You can place a fraud alert by calling any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, it will notify the other two, which must then place fraud alerts in your file.

An initial alert stays in your file for at least 90 days. To place an initial alert, you will be required to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an *identity theft report*, which includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit.

Finally, all of the major credit bureaus also offer you the opportunity to freeze your credit file, which prevents the release of your credit report without your consent. You should be aware that a freeze and the process required to lift it in order to release your report may delay or interfere with approval of subsequent requests for credit (including point of sale credit), insurance, government services or payments, housing, employment, utilities and phone bills.

## Other Information

The FTC's website at <http://www.ftc.gov/bcp/edu/microsites/idtheft> contains a great deal of helpful information about identity theft prevention.

State Street is committed to protecting your privacy and confidentiality, and we sincerely apologize for any inconvenience or worry this causes.

Sincerely,

A handwritten signature in black ink, appearing to read "M. Rogers". The signature is fluid and cursive, with the first letter of the first name being a large, stylized "M".

Michael F. Rogers  
Executive Vice President