WILMERHALE

J. Beckwith Burr

+1 202 663 6695 (t)
+1 202 663 6363 (f)
beckwith.burr@wilmerhale.com

January 11, 2010

Office of the Attorney General of New Hampshire
33 Capitol Street
Concord, NH 03301
Telephone (603) 271-3658
Fax (603) 271-2110

Re: Notification of Information Security Incident

To whom it may concern:

This letter is to inform you that Suffolk County National Bank ("SCNB") will today begin notifying individuals who may be affected by an unauthorized intrusion into a computer server hosting the bank's Online Banking system. SCNB is a full-service, nationally chartered commercial bank, with its principle pace of business at 4 West Second Street, Riverhead, NY 11901. 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 N.H. Rev. Stat. Ann. §§ 359, of:

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

An unauthorized intruder accessed Log In information for approximately 8,400 online banking customers of the Suffolk County National Bank ("SCNB"), including approximately 6,900 individuals, 1 of whom is a resident of New Hampshire. The compromised accounts were identified through an internal security review on December 24, 2009. Based on SCNB's investigation, which is ongoing, the unauthorized access appears to have occurred during a six-day-period between November 18 and November 23, 2009 and affected fewer than 10 percent of SCNB's total customers. The intrusion appears to have been limited in duration and scope, and SCNB has taken additional steps to ensure the security of data on the server. To date, SCNB has

found no evidence of any unauthorized access to Online Banking accounts, nor received any reports of unusual activity or misuse of customer information.

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

1. Contacted law enforcement;

2. Notified its primary Federal regulator, the Office of the Comptroller of Currency, and filed a Suspicious Activity Report;

3. Notified national consumer reporting agencies (Equifax, Experian, TransUnion);

4. Conducted a thorough investigation of the incident, including an assessment of whether or not the theft created any prospective data security risk;

5. Notified the hosting service identified by forensic investigators as the source the potential source of the intrusion;

6. Isolated and rebuilt the affected server;

7. Identified affected customers and the sensitive personal information compromised by the incident;

8. Reviewed its Online Banking system for unauthorized or unusual activity and enhanced certain security procedures as a precautionary measure to prevent/detect data misuse;

9. 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 to be sent to affected customers. If you have additional questions about this incident, please feel free to call me at (202) 663-6695.

Sincerely,

J. Beckwith Burr

- We recommend that you initially check your credit report. Please pay particular attention to any recent inquiries, and make certain that if there are any, that you initiated them.
- Also, please check through your November and December, 2009 account history or bank statements and inform us of any transaction that you cannot reconcile. As indicated above, to date, we have not been informed of any unusual activity.

The security of customer information is of utmost importance to SCNB. While we know that our diligence in this regard allowed us to uncover this incident, and to take action to protect our customers, we also recognize that the provision of financial services over the Internet requires our dedication to continuous monitoring and security. You have previously received notification that toward the end of this month, we will be introducing many improvements to our Online Banking service. This project has been underway for some time, and among the enhancements are additional security features.

We know that this kind of incident is a matter of concern, even if your personal information is not misused, and we apologize for that concern and any inconvenience that this incident may have caused you. Please feel free to call me, or [BranchManagerName], Branch Manager at [BranchTelephoneNumber], to answer any further questions. Thank you for maintaining your banking relationship with the Suffolk County National Bank. Please be assured that we will continue to hold the protection of your customer information paramount and will take all precautions necessary to do so.

Sincerely,

J. Gordon Huszagh
President & CEO

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 to identify possible fraudulent activity. Your complimentary two-year membership in Triple Advantage℠ Premium includes:

- Daily monitoring of your three national credit files from Experian, Equifax® and TransUnion®
- Notifications alerting you of key changes to your credit reports which may help you to 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
- $10,000 in identity theft insurance coverage with zero deductible provided by Virginia Surety Company, Inc. for certain identity theft expenses*
- Helpful information on preventing identity theft, as well as various financial calculators and tools

* Insurance coverage is not available in US overseas Commonwealth or Territories (i.e. Puerto Rico).

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 your personal Activation Code included in the accompanying letter to activate this membership, regardless of the enrollment method you choose.

- To sign up online, please visit http://partner.consumerinfo.com/scnb 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) 252-0121. If you sign up by telephone, all credit reports and alerts will be delivered by the US Postal Service.

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 for unauthorized activity upon receipt.

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 or by contacting each of the three companies directly. The credit reporting companies, their addresses and telephone numbers are as follows:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	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 Federal Trade Commission's (FTC) website at http://www.ftc.gov/bcp/edu/microsites/idtheft contains a great deal of helpful information about identity theft prevention.