

*Handwritten marks: "KIND" and "OFF" with a checkmark.*

### 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: 1st Source Bank  
 Address: 100 N. Michigan St.  
South Bend, IN 46601  
 Telephone: (574) 235-2000  
 Fax: \_\_\_\_\_  
 Email: griffith@1stsource.com

**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

Date Security Breach Reporting Form submitted: May 29, 2008  
 Date the Security Breach was discovered: May 12, 2008  
 Estimated number of affected individuals: 193,335  
 Estimated number of NC residents affected: 267

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)): \_\_\_\_\_

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: See attached notification letters.

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

Describe any measures taken to prevent a similar Security Breach from occurring in the future: Security controls are being added to the systems affected.

Date affected NC residents were/will be notified: May 29, 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): \_\_\_\_\_

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.

- written notice
- electronic notice (email)
- telephone notice
- substitute notice

Signature: *John Griffith* Date: 5-29-08  
 Contact Person, Title: John Griffith, General Counsel  
 Address: 100 N. Michigan St., South Bend, IN 46601  
 (if different from above) \_\_\_\_\_  
 Telephone: 574-235-2494 Fax: \_\_\_\_\_ Email: griffith@1stsource.com

Date

**[Customer Name]**

**[Address]**

**[City, State, Zip]**

Dear **[Customer]**:

On May 12, 2008, we discovered a computer systems breach at 1st Source Bank. We immediately began working with law enforcement agencies and with an outside computer security firm to investigate the incident. The attackers penetrated our computer defenses and gained access to some of the 1st Source Bank debit and ATM card information on our systems. Fortunately, if you are receiving this letter and, in addition, are a cardholder, we have determined that the information on your debit card or ATM card was **not** exposed.

We also have found no evidence that any personal identity information we have about you was targeted, accessed or copied by the attackers. Although the attackers gained entry to a portion of our system with some of your personal data, including your social security number, the evidence and the prior experience of law enforcement and of our computer security consultants with these attackers point to credit and debit card information as their target and **not** personal identity information.

We are taking this matter very seriously. We have blocked the method of unauthorized access. We also have strengthened our security controls and our arrangements with our vendors to prevent this from happening again.

This incident should remind us all of the need for vigilance. Theft of credit card and personal identity information continues to be a growing problem. 1st Source Bank will continue to devote substantial resources to protect against these types of attacks. Here are some additional steps you should take or consider for further protection:

- Report any suspicious account activity immediately. Stop by your banking center, call your banker, or call our client service line at (574) 235-2000 to report a suspected problem.
- Review your bank account activity regularly, which can be done quickly online at [1stsource.com](http://1stsource.com).
- Change your password frequently if you have online banking (click Tools in right hand corner and follow the prompts).
- Place a "fraud alert" on your credit files. Note that if you do this, you will have to go through significant security procedures to obtain credit or new loans.
- If you think that your personal information is being improperly used in any manner, you can also contact the Federal Trade Commission at 1-877-ID-THEFT (877-438-4338).

Over

**Page 2**

- Monitor your credit reports. We recommend that you periodically obtain a credit report from each of the nationwide credit reporting agencies and have any information relating to fraudulent transactions deleted. Consumers may obtain a free credit report annually from each of the three credit bureaus. You can call the bureaus listed below or go to [annualcreditreport.com](http://annualcreditreport.com), the official site authorized by the three credit reporting agencies to distribute the free credit reports.

Equifax  
800-525-6285

Experian  
888-397-3742

TransUnion  
800-680-7289

We sincerely apologize for any concerns this may cause you, and have taken steps to prevent this type of incident from happening again. Again, if you have concerns, please do not hesitate to talk with your personal banker or feel free to contact us at 574-235-2000 with any questions or concerns you may have. Thank you for understanding.

Sincerely,



Wellington D. Jones, III  
President