



John B. Griffith
Senior Vice President,
General Counsel and Secretary

100 North Michigan Street
P.O. Box 1602
South Bend, IN 46634
574 235-2494
574 235-2033 Fax
Griffith@1stsource.com

May 29, 2008

Steven Rowe
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Dear Attorney General Rowe:

On May 12, 2008, we discovered a computer system breach at 1st Source Bank. We immediately began working with law enforcement officials and with an outside computer security firm to investigate the incident. We learned that the attackers penetrated our computer defenses and gained access to debit card and ATM card information of some of our account holders, including 1 Maine resident. We also learned that the attackers gained entry to a portion of one of our systems where personal identity information (name, address, date of birth, and Social Security number) of our account holders, including 27 Maine residents, was stored. Although the attackers gained entry to this portion of our system, the evidence we have collected 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.

1st Source Bank is taking this matter very seriously. We have been working diligently to investigate the unauthorized activity and block the method of unauthorized access. We are continuing to work with law enforcement and our outside computer security firm to investigate the incident. We also have taken steps to strengthen our security controls and our arrangements with our vendors to prevent this from happening again.

We are sending today (May 29, 2008) the attached debit and ATM card notification letter to the cardholders whose debit card and ATM card information was compromised. We are also sending tomorrow (May 30, 2008) the attached notification letter to those 1st Source Bank account holders who are not cardholders but whose personal identity information was stored on one of the systems to which the attackers gained entry.

If you have any questions or need additional information, please feel free to contact me at 574-235-2494.

Sincerely,

A handwritten signature in black ink, appearing to read 'John B. Griffith', written over a printed name.

John B. Griffith

JBG/lsw
Attachments

CONSUMER PROTECTION DIVISION
RECEIVED
JUN 03 2008
OFFICE OF ATTORNEY GENERAL

Date

[Customer Name]

[Address]

[City, State, Zip]

Dear [Customer]:

On May 12, 2008, we discovered a computer system breach at 1st Source Bank. We immediately began working with law enforcement officials and with an outside computer security firm to investigate the incident. The attackers penetrated our computer defenses and gained access to some of the debit and ATM card information on our systems. We believe that information on your debit card or ATM card may have been taken.

To protect your account, we will be issuing a new 1st Source Bank debit or ATM card to you. You should receive your new card sometime within the next few weeks. Since the new debit or ATM card will have a new card number, you will be able to continue to safely use your current PIN.

You may continue to use your current debit or ATM card until your new card arrives. **Please activate the new card as soon as possible and destroy your old card.** Your old card will be deactivated shortly after your receipt of the new card. We do ask that you **please notify us immediately if you see any activity on your account that you do not recognize.** You will not be responsible for any fraudulent activity related to the security breach as long as we are notified promptly.

We 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 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.

Protecting your information continues to be our highest priority. If you still have concerns, we are pleased to offer you a free membership to Deluxe ID Theftblock for twelve months. This service will proactively monitor your credit files for early signs of identity theft. If suspicious activity occurs, you will be notified, and if you become a victim, you will receive professional recovery support. To arrange your coverage, please call client services at 574-235-2000 or talk with your personal banker.

Over

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.
- 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