



May 1, 2013

Attorney General Michael A. Delaney
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Peoples Bank of Commerce—Notice of Data Security Event

Dear Attorney General Delaney:

We are writing to notify you of a data event that may have compromised the security of personal information of two (2) New Hampshire residents. Peoples Bank of Commerce, 234 E. First Avenue, Cambridge, MN 55008 is informing your office of pertinent facts that are known at this time related to the data event described below. Peoples Bank of Commerce retained privacy and data security legal counsel to assist in the ongoing investigation of, and response to, the incident. The investigation is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Peoples Bank of Commerce does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

On February 1, 2013, a backup tape containing Peoples Bank of Commerce customer information was stolen from a secured vehicle in Roseville, Minnesota, belonging to a Peoples Bank of Commerce employee. The theft was promptly reported to the Roseville, Minnesota police department, to the Minnesota Department of Commerce, and the FDIC. Peoples Bank of Commerce initiated an internal investigation into the incident. Peoples Bank of Commerce retained independent computer forensic experts to assist with the investigation and to confirm the impacted population. Peoples Bank of Commerce retained privacy and data security legal counsel to assist in incident investigation and response preparation. This investigation revealed that the stolen back-up tape contained certain Peoples Bank of Commerce customer names, addresses, Social Security numbers/tax identification numbers, account numbers, and account balances. The backup tape was password-protected.

Notice to New Hampshire Residents

Although the investigation is ongoing, it appears that the personal information of two (2) New Hampshire residents was stored on the back-up tape at the time of the theft. These New

Hampshire residents were sent written notice of this data security event on or about February 26, 2013 in substantially the same form as the letter attached at *Exhibit A*. Supplemental notice of this incident was provided to these affected New Hampshire residents on or about April 29, 2013 in substantially the same form as the letter attached at *Exhibit B*.

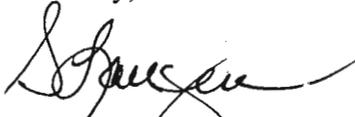
Other Steps Taken and To Be Taken

In addition to providing written notice of this incident to affected individuals, Peoples Bank of Commerce offered each affected customer one (1) free year of credit monitoring services. Peoples Bank of Commerce is also providing each individual with information on how to protect against identity theft and fraud. Peoples Bank of Commerce is providing written notice of this incident to other states' regulators, and to the national consumer reporting agencies. In addition, we have implemented additional security measures designed to prevent a recurrence of such an incident.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact our privacy and data security counsel, Jennifer A. Coughlin or John F. Mullen of Nelson Levine de Luca & Hamilton, LLC, at 215-358-5134.

Sincerely,



Scott Laugen
President and CEO, Peoples Bank of Commerce

Exhibit "A"

February 26, 2013

Name
Address
Address
City, State, Zip

Dear Valued Client:

We have recently become aware that certain confidential records, including customer information of Peoples Bank of Commerce, were stolen. This theft did not occur at Peoples Bank of Commerce. While we have no reason to believe your personal files have been or will be compromised, we wanted to notify you of the incident and outline the following steps we have taken in response.

First, the appropriate law enforcement authorities and regulatory agencies have been notified. Second, we have conducted a thorough investigation of the breach and retained a data forensic expert to review the types of information stolen. Third, we have also implemented additional security measures designed to prevent a recurrence of such an incident.

You can be assured that protecting the privacy of our customers is a responsibility we take very seriously. Therefore as a precaution, and to help you detect any possible misuse of your data, we are offering free credit monitoring to you for a 12-month period.

We have engaged Equifax to provide you with their *Silver Daily* product, which includes daily monitoring of your credit report and e-mail alerts of key changes to your credit report. You will have 45 days from the date of this notice to activate this credit monitoring by using a personal activation code that is unique to your use only. To obtain the code, please call us toll-free at 1-800-991-2317. Then to enroll in the *Silver Daily* product, go to www.myservices.equifax.com/silver and enter the code when prompted to do so. Our Customer Service Representatives are also available to help you Monday through Friday, 8:00 a.m. to 6:00 p.m. and Saturday, 9:00 a.m. to 12:00 p.m., Central Time.

Even if you decide not to register for the credit monitoring, we recommend that you remain vigilant over your financial matters and accounts. Among other things, you should consider:

- Periodically change your bank-related password, in accordance with best practices.
- Regularly review statements from your accounts and promptly report incidents of suspected identity theft to us and to proper law enforcement authorities, including the Federal Trade Commission (FTC). You have the right to obtain a police report if you are the victim of identity theft. Please visit the FTC's web site, <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> or call toll-free 1-877-ID-THEFT (1-877-438-4338), to learn more about protecting yourself from identity theft.

- Never share confidential information, such as your social security number, with unauthorized individuals.
- Periodically obtain your credit report from each nationwide credit reporting agency, and if you have any concerns, place a fraud alert on your credit file. A fraud alert puts your creditors on notice that you may be a victim of fraud and tells creditors to contact you before they open any new accounts or change your existing accounts. To place a fraud alert, contact any one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion
Phone: 800-525-6285 P.O. Box 105069 Atlanta, GA 30348-5069 http://www.equifax.com/answers/set-fraud-alerts/en_cp	Phone: 888-397-3742 P.O. Box 9532 Allen, TX 75013 https://www.experian.com/fraud/center_rd.html	Phone: 800-680-7289 P.O. Box 6790 Fullerton, CA 92634-6790 https://fraud.transunion.com

As soon as one credit bureau confirms a fraud alert, the other credit reporting agencies are notified to place fraud alerts as well. You may request that all three credit reports be sent to you, free of charge, for your review. You may also obtain a free copy of your credit report once every twelve (12) months by visiting www.annualcreditreport.com.

We greatly value you as a customer of Peoples Bank of Commerce and sincerely regret that this incident has occurred. The protection of your confidential information is the highest priority of the Bank, and we will continue to monitor the situation and keep you informed if there are any changes about which you should be aware. If you should have any questions or concerns, please contact our Customer Service Representatives at 1-800-991-2317. They are available Monday through Friday, 8:00 a.m. to 6:00 p.m. and Saturday, 9:00 a.m. to 12:00 p.m., Central Time.

Sincerely,

Scott Laugen
President and CEO, Peoples Bank of Commerce

Exhibit "B"

[Date]

[Bank Customer Name]

[Bank Customer Address]

[Bank Customer City, State Zip]

Dear [Bank Customer Name]:

We wrote to you on February 25, 2013, to advise you of a recent theft of Peoples Bank of Commerce customer information. We are writing to provide you with additional information on the incident, and on how to protect yourself against the possibility of identity theft and fraud.

As discussed in our February 25, 2013 letter to you, on February 1, 2013, a backup tape containing Peoples Bank of Commerce customer information was stolen from a secured vehicle in Roseville, Minnesota, belonging to a Peoples Bank of Commerce employee. The theft was reported to the Roseville police department, to the Minnesota Department of Commerce, and to the FDIC. An internal investigation into the incident was launched. Independent computer forensic experts were retained to assist with the investigation and to confirm the impacted population. These investigations revealed that the backup tape contained your name, address, Social Security number/tax identification number, account number, and account balance.

Our February 25, 2013 letter contained information on how to receive one (1) free year of credit monitoring services with Equifax's Silver Daily product. To further protect against possible identity theft or financial loss and in addition to activating your Silver Daily membership, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com, or call, toll-free, (877) 322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. The contact information for these bureaus is below.

We remain unaware of any actual or attempted misuse of your information. Nevertheless, you should report any suspicious activity to law enforcement, and to your state attorney general. You may also obtain information on how to place a fraud alert or security freeze on your credit file from your state attorney general. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. You can also obtain further information on identity theft, including how to place a fraud alert or security freeze on your credit file, the steps you can take to protect yourself, and how to file a complaint, by contacting: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Information on how to place a fraud alert or security freeze on your credit file is also available from the national consumer reporting agencies. The contact information for these agencies is contained within our February 25, 2013 letter.

We again apologize for any inconvenience or concern this may have caused you. Should you have any questions, please do not hesitate to contact our Customer Service Representatives, Monday through Friday, 8:00 a.m. to 5:00 p.m., Central Time, at (800) 991-2317.

Sincerely,

Scott Laugen
President and CEO, Peoples Bank of Commerce