LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Jay F. Kramer
77 Water Street, 21st Floor
New York, NY 10005
Jay.Kramer@lewisbrisbois.com
Direct: 347.300.5120

September 12, 2018

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-Mail: SecurityBreach@atg.wa.gov

Re: Notification of Data Security Incident

Dear AG Ferguson:

I represent Skagit Bancorp, Inc. ("Skagit") located in Burlington, Washington. This letter is being sent because Skagit Bank has determined that in connection with a recent data security incident, unauthorized access was obtained to one employee email account potentially affecting five hundred nineteen (519) Washington residents.

On June 12, 2018, Skagit Bank learned that an unauthorized individual gained access to a Skagit Bank employee's email account. Upon learning of the incident, Skagit Bank undertook an immediate internal investigation, and retained an independent third party forensic firm to also investigate the incident. The goals of the investigation were to determine what happened and whether any customer's personal information had been accessed without authorization. On or about August 1, 2018, the investigation first revealed that certain customers' personal information may have been accessed by unauthorized individuals. Skagit Bank specifically learned that the personal information of five hundred nineteen (519) Washington residents were potentially affected. The unauthorized access to these customers' information potentially included: customer names, addresses, dates of birth, Social Security and Driver's License numbers or other state or tax identification numbers, bank account information, username and passwords for emails, security passwords and in some instances financial security codes.

In response to this incident, Skagit Bank took a number of steps. They immediately instituted password resets on all email accounts across their enterprise, and have enabled Multi Factor Authentication (MFA) for access to all email accounts. In addition, Skagit Bank is in the process of notifying the affected Washington residents via the attached letter. Further, this incident has been reported to the FBI's Internet Crime Complaint Center for any additional action deemed necessary.

Skagit Bank is committed to protecting the sensitive information in its control. If you have any questions, please do not hesitate to contact me at (347) 300-5120, or at Jay.Kramer@LewisBrisbois.com.

Very truly yours,

Jay F. Kramer of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Consumer Notification Letter

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Subject: Notice of Data Security Incident

Dear <<Name 1>>,

We are writing to notify you of a recent data security incident that may have involved some of your personal information. At Skagit Bank we take the privacy and security of your information very seriously and that is why we are informing you of this incident as well as providing you with information on additional steps that can be taken to protect your personal information. While we have no information that any of your personal data has been misused, out of an abundance of caution, we are also offering you a period of free credit and identity and credit monitoring.

What happened?

On June 12, 2018, Skagit Bank learned that an unauthorized individual gained access to a Skagit Bank employee's email account.

What information was involved?

The information contained in the compromised email account may have included: customer names, addresses, dates of birth, Social Security and Driver's License numbers or other state or tax identification numbers, bank account information, username and passwords for emails, security passwords and in some instances financial security codes.

What are we doing:

Upon learning of this incident, Skagit immediately launched an internal investigation and reported the matter to appropriate authorities. We also retained an independent third party forensics firm to investigate the incident, and sought the advice of legal and cybersecurity experts. We regret that this incident has occurred and want to assure you that Skagit Bank has also added additional security features and taken other steps to minimize the chance that an event like this could occur in the future.

Although we have no information that your personal data has been misused, as an added precaution, we have arranged to have TransUnion protect your identify for twelve (12) months at no cost to you. We are also providing you additional information about steps you can take to protect your personal information.

What you can do: Keep a copy of this notice for your records. Because your Social Security or driver's license number may have been involved, to protect yourself from the possibility of identity theft we recommend that you place a fraud alert on your credit files and order copies of your credit reports by following the recommended privacy protection steps outlined in the enclosure. Check your credit reports for any accounts that you do not recognize. If you find anything suspicious, follow the instructions found in the enclosure.

In some instances, bank account information and pin numbers were involved as well. Please reset and change your pin number associated with your bank account and additionally review your bank statements for any fraudulent activity. **Please contact us immediately if you notice any suspicious activity**.

If you provided your email username and password to Skagit Bank, please reset them and, in addition, check for suspicious activity in potentially affected email accounts.

We encourage you to enroll and receive the free credit monitoring and identity restoration services through TransUnion. Please see the following page for enrollment instructions and suggested steps you can take to protect your information.

For more information: If you have any questions, please call Epiq at 1-877-854-9980 Monday through Friday 6:00 a.m. – 6:00 p.m. PT (excluding U.S. holidays).

At Skagit we value the relationships we enjoy with our customers, and look forward to continuing to provide the quality services you have come to expect from us. We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

Cheryl R. Bishop

Cheryl R. Bishop
Chief Executive Officer
Skagit Bank

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Enroll in Credit Monitoring: As an added precaution, we have arranged to have TransUnion protect your identity for 12 months at no cost to you. The following identity protection services start in the date of this notice and you can use them at any time during the next 12 months.

MyTrueIdentity To enroll in this service, go to the *my*TrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code," enter the following 12-letter Activation Code <<INSERT UNIQUE ACTIVATION CODE>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, three-bureau credit monitoring service, via U.S. Mail Delivery, please call the TransUnion Fraud Response/Service toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code <<INSERT static 6-digit Telephone Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service any time between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available to individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit reporting score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraud alerts, new inquiries, new accounts, new public records, later payments, change of address and more.

The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order activate your monitoring options.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC at the address below or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.