THE FEDERAL SAVINGS BANK

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

[First Name] [Last Name]
[Address]
[City, State, Zip]

2/8/2017

Dear [First Name] [Last Name]:

The Federal Savings Bank ("TFSB" or the "Bank") is committed to safeguarding the personal information of its customers and of others whose personal information comes into the Bank's possession. Unfortunately, I need to inform you of an information security incident that recently affected TFSB and which may affect you because your personal information is in TFSB's possession. I also want to tell you about the steps that TFSB is taking to address this incident and to assure you that we have taken steps to prevent a recurrence.

TFSB recently discovered that an employee's e-mail account was criminally hacked and then used to send phishing e-mails. We immediately isolated this e-mail account, stopped the phishing e-mails, locked out the hacker, and conducted a thorough investigation of the incident with the assistance of an outside computer forensic expert. That investigation found no evidence that any personal information in the employee's e-mail account had been accessed or acquired. Additionally, TFSB alerted federal law enforcement concerning this incident and will cooperate fully in any investigation.

Nonetheless, and out of an abundance of caution, we are notifying you because the computer forensic expert determined that your personal information was stored in the hacked e-mail account. That personal information may include your name, mailing address, Social Security number, driver's license number or other government-issued identification number, bank account or other financial account number without any passcode or security code, and credit or debit card number. **Please note that we have no information indicating that any of your personal information has been misused.**

To prevent a recurrence, we have conducted a thorough review of our e-mail system security and we have taken steps to enhance that security to prevent a recurrence. We also have provided additional training to employees to enhance their ability to identify potential hacking activity and to respond promptly to it.

In addition to these steps to enhance the security of your personal information, TFSB is offering you one year of credit monitoring at no cost to you. Your free one-year membership in ID Experts' MyIDCare™ will help you to detect possible misuse of your personal information and will provide credit protection services focused on identification and resolution of possible personally identifying information misuse. Once you activate your MyIDCare™ membership, your credit report will be monitored for leading indicators of identity theft. You will receive timely credit alerts from MyIDCare™ on any key changes in your credit report. We also highly recommend that you take the steps described on the following pages to protect yourself.

If you wish to enroll in MyIDCare™, you will need to do the following:

1. **VISIT** the MyIDCare™ web site**: www.myidcare.com/TFSBprotect**
   or call **800-939-4170** to enroll

2. **PROVIDE** your Activation Code**: [code]**

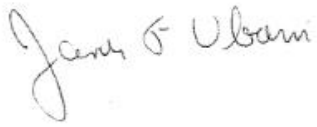
Enrollment Deadline: 5/8/2017

If you have any questions concerning ID Experts' MyIDCare™ or if you prefer to enroll over the phone for delivery of your membership via US mail, please call ID Experts at **800-939-4170**.

In addition to the steps TFSB has taken on your behalf, we have included with this letter additional information on steps you can take to protect the security of your personal information. We urge you to review this information carefully.

TFSB sincerely regrets any inconvenience this incident may cause you. If you have any questions, please call our dedicated call center at **800-939-4170** between 6 AM and 5 PM (Pacific Standard Time), Monday through Friday (excluding holidays).

Sincerely,



Javier Ubarri
President

(Enclosure)

Steps To Protect The Security Of Your Personal Information

By taking the following steps, you can help reduce the risk that your personal information may be misused.

1. Enroll in MyIDCare™. You must personally activate credit monitoring for it to be effective. Above are instructions and information on how to activate your MyIDCare™ membership. If you need assistance or if you want to enroll by telephone, you should contact ID Experts directly at **800-939-4170**. ID Experts' MyIDCare™ product will provide the following:

- **Credit Monitoring**: Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections.
- **CyberScan™**: Provides monitoring of underground websites, chat rooms, and malware to identify trading or selling of personal information.
- **Identity Theft Resolution**: If you have been a victim of identity theft, you will be assigned a dedicated ID Experts' identity theft Recovery Agent who will walk you through the fraud resolution process, from start to finish.
- **$1 Million Identity Theft Insurance**: As a MyIDCare™ member, you are immediately covered by a $1 million insurance policy that can help you cover certain costs, including typically lost wages, private investigator fees, and legal fees.

Please direct questions about the MyIDCare™ product to ID Experts. Enrolling in MyIDCare™ will not affect your credit score.

2. Review your credit reports. You can receive free credit reports by placing a fraud alert. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three national credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.

3. Review your account statements. You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities, and other service providers.

4. Remain vigilant and respond to suspicious activity. If you receive an e-mail or mail alert from ID Experts, contact a MyIDCare™ fraud resolution representative Toll-Free at **800-939-4170** or **www.myidcare.com/TFSBprotect.** If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You also should consider reporting such activity to TFSB, your local police department, your state's attorney general, and the Federal Trade Commission.

5. Consider placing a fraud alert with one of the three national credit bureaus. You can place an initial fraud alert by contacting one of the three national credit bureaus listed below. For 90 days, an initial fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit. If you decide to enroll in MyIDCare™, you should place the fraud alert after enrolling. The contact information for all three bureaus is as follows:

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

6. Additional Information. You can obtain additional information about steps you can take to avoid identity theft from the following:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.ftc.gov/bcp/edu/microsites/idtheft/
(877) IDTHEFT (438-4338)
TDD: (866) 653-4261