Pacific National Bank
FRAUD ALERT

Date: 02/06/17
Subject: **Fictitious Notification Regarding the Release of Funds Supposedly Under the Control of the Office of the Comptroller of the Currency**

Any document claiming that the OCC is involved in holding any funds for the benefit of any individual or entity is fraudulent. The OCC does not participate in the transfer of funds for, or on behalf of, individuals, business enterprises, or governmental entities.

Consumers have reported receiving communications that the OCC is holding $11,000 on their behalf as a refund for illegal fees charged by their financial institutions. The callers have been identified as both males and females with heavy accents who are using various names, including Alex, Miley, and Deborah Howells. The callers have the personal information of the potential victim including address, date of birth, and Social Security number. The potential victim is asked to confirm this information and to provide his or her bank routing number and account number so that a transfer may be made.

The telephone numbers involved in this scam include, but are not limited to, (218) 585-9128, (202) 649-6700, and (202) 649-8580, which are all Google Voice telephone numbers. When dialing these numbers, the potential victims are greeted by the Google Voice recording and required to speak their names. The service then attempts to forward the call to the telephone number associated with the established Google Voice account, where the call will be answered by the scammer.

Before responding in any manner to any proposal supposedly issued by the OCC that requests personal account information, or that requires the payment of any fee in connection with the proposal, the OCC recommends that consumers take the following steps:

- contact the OCC directly to verify the legitimacy of the proposal (1) via e-mail at occalertresponses@occ.treas.gov; (2) by mail to the OCC's Special Supervision Division, 400 7th St. SW, Suite 3E-218, MS 8E-12, Washington, DC 20219; (3) via fax to (571) 293-4925; or (4) by calling the Special Supervision Division at (202) 649-6450.
- contact state or local law enforcement.
- file a complaint with the Internet Crime Complaint Center if the proposal appears to be fraudulent and was received via e-mail or the Internet.
- file a complaint with the U.S. Postal Inspection Service by telephone at (888) 877-7644; by mail at U.S. Postal Inspection Service, Office of Inspector General, Operations Support Group, 222 S. Riverside Plaza, Suite 1250, Chicago, IL 60606-6100; or via the online complaint form at https://postalinspectors.uspis.gov/forms/MailFraudComplaint.aspx, if the proposal appears to be fraudulent and was delivered through the U.S. Postal Service.

Consumers who have provided bank account information should contact their financial institutions immediately to report the issue and to discuss options to protect their account assets. Consumers who have had their personal information compromised should visit the Federal Trade Commission's website at www.ftc.gov and follow the guidance for identify theft.

Date: 04/06/16
Subject: **Official-sounding Calls About an Email Hack – Reported by the Division of Consumer and Business Education,**
Federal Trade Commission (FTC)

There's a new twist on tech-support scams — you know, the one where crooks try to get access to your computer or sensitive information by offering to "fix" a computer problem that doesn't actually exist. Lately, we've heard reports that people are getting calls from someone claiming to be from the Global Privacy Enforcement Network. Their claim? That your email account has been hacked and is sending fraudulent messages. They say they'll have to take legal action against you, unless you let them fix the problem right away.

If you raise questions, the scammers turn up the pressure – but they've also given out phone numbers of actual Federal Trade Commission staff (who have been surprised to get calls). The scammers also have sent people to the actual website for the Global Privacy Enforcement Network. (It's a real thing: it's an organization that helps governments work together on cross-border privacy cooperation.)

Here are few things to remember if you get any kind of tech-support call (https://www.consumer.ftc.gov/articles/0346-tech-support-scams), no matter who they say they are:

- Don't give control of your computer to anyone who calls you offering to "fix" your computer.
- Never give out or confirm your financial or sensitive information to anyone who contacts you.
- Getting pressure to act immediately? That's a sure sign of a scam. Hang up.
- If you have concerns, contact your security software company directly. Use contact information you know is right, not what the caller gives you.

Read on to learn more about tech-support scams (https://www.consumer.ftc.gov/articles/0346-tech-support-scams) and government imposter scams (https://www.consumer.ftc.gov/articles/0048-government-imposter-scams). And, if you spot a scam, tell the FTC (https://www.ftccomplaintassistant.gov/#&panel1-1)

Date: 03/29/16

Subject: **Fictitious Correspondence Regarding the Release of Funds Supposedly Under the Control of the Office of the Comptroller of the Currency**

Any document claiming that the OCC is involved in holding any funds for the benefit of any individual or entity is fraudulent. The OCC does not participate in the transfer of funds for, or on behalf of, individuals, business enterprises, or governmental entities.

There are several variations of fictitious documents in circulation, and while the appearance of documentation may differ, the material is being sent to consumers in an attempt to elicit funds from them and to gather personal information to be used in possible future identification theft.

Variation No. 1

These documents may contain the letterhead of the U.S. Department of Homeland Security with the page footer containing the U.S. Department of the Treasury seal and wording. The letter claims that the OCC is holding funds until a Clearance Certificate fee has been verified as paid. Both the letter and "Official Receipt" appear to be signed by an official of Homeland Security. This material may be sent via e-mail from [info@ice-dphs.com].

Variation No. 2

This document references " "CEASE AND DESIST" ORDER OF FUNDS" and instructs the recipient to complete a FUNDS IMPORT CERTIFICATION & INTERNATIONAL TRANSFER PERMIT ORDER to ensure that the OCC releases funds to the beneficiary. This letter appears to be signed by an official of the OCC. This material may be sent via e-mail from [admin@occservice.org]. Please note that this e-mail address is not affiliated with the OCC and has been shut down. The OCC's Web site is www.occ.gov, and all e‑mail addresses associated with the OCC would end in [@occ.treas.gov].

Variation No. 3

The document contains both the Treasury Department and OCC seals and references "NOTIFICATION OF FULL CLEARANCE FOR CREDITTING". This document was issued to the recipient following his payment of an $8,900 "MT 103" fee. E-mail addresses used to perpetrate this fraud include: [koumbatebinta@gmail.com] and [dalibard@gmail.com].

Before responding in any manner to any proposal supposedly issued by the OCC that requests personal information or personal account information, or that requires the payment of any fee in connection with the proposal, recipients should take steps to verify that the proposal is legitimate. At a minimum, the OCC recommends that consumers:

- contact the OCC directly to verify the legitimacy of the proposal (1) via e-mail at occalertresponses@occ.treas.gov; (2) by mail to the OCC's Special Supervision Division, 400 7th St. SW, Suite 3E-218, MS 8E-12, Washington, DC 20219; (3) via fax to (571) 293-4925; or (4) by calling the Special Supervision Division at (202) 649-6450.
- contact state or local law enforcement.
- file a complaint with the Internet Crime Complaint Center at www.ic3.gov if the proposal appears to be fraudulent and was received via e-mail or the Internet..
- file a complaint with the U.S. Postal Inspection Service by telephone at (888) 877-7644; by mail at U.S. Postal Inspection Service, Office of Inspector General, Operations Support Group, 222 S. Riverside Plaza, Suite 1250, Chicago, IL 60606-6100; or via the online complaint form at https://postalinspectors.uspis.gov/forms/MailFraudComplaint.aspx, if the proposal appears to be fraudulent and was delivered through the U.S. Postal Service.

Date: 03/08/16

Subject: **FDIC Publishes a Bank Customer's Guide to Cybersecurity -** This is a special edition of consumer newsletter feature tips for preventing online fraud and theft.

Consumers increasingly rely on computers and the Internet for everything from shopping and communicating to banking and bill paying. While the benefits of faster and more convenient "cyber" services are clear, the strategies for preventing online fraud and theft may not be as well-known by many bank customers. That is why the FDIC has produced a special edition of the agency's quarterly *FDIC Consumer News* (Winter 2016) entitled "A Bank Customer's Guide to Cybersecurity." Here is a brief overview of the articles and other features in this special issue.

Safety precautions to take before connecting to the Internet with a personal computer, laptop, smartphone or tablet: The lead article discusses ways to protect log-in information for bank accounts and other financial accounts, including the use of "strong" user IDs and passwords that will be hard for a hacker to guess, basic security measures such as security software updates, and the need to be careful where and how to connect to the Internet. Other articles focus on security measures when using a smartphone or tablet (including "auto lock" features and the ability to remotely remove data if a mobile device is lost or stolen), how to protect computers from malicious software ("malware") that can steal valuable personal financial information, and ideas to help small businesses protect against losses from cyberattacks.

Tips on how to avoid identity theft online: One article advises on identifying and avoiding "phishing" and "pharming" scams that start with fake emails and websites and end with consumers providing Social Security numbers, bank account numbers and other valuable details. A second article offers assistance on preventing identity thieves from using social networking sites to learn enough information about individuals to figure out passwords, access financial accounts or commit identity theft. And a third provides guidance to help parents and caregivers protect young people from cyber-related identity theft and financial fraud, including the need to secure all electronics connected to the Web, even video games, because the equipment may link to information such as credit or debit card numbers.

What to know about the roles that banks and the government play in protecting customers: As explained in one article, federal law and regulations require financial institutions to have programs to ensure the security and confidentiality of customer information. The article also notes that banking regulators expect the institutions they supervise to have a framework for learning about emerging threats and provide guidance about the steps institutions can take to be prepared. Another article describes how federal consumer laws and financial industry practices protect cybertheft victims from losses under certain circumstances. And, our "Dear FDIC" feature answers questions about deposit insurance coverage and online banking.

Additional resources from the FDIC that can help educate consumers: The back of the guide features an eight-question quiz to test a consumer's knowledge of key information in this issue and a checklist with reminders about 10 simple things bank customers can do to help protect themselves from online criminals.

The goal of *FDIC Consumer News* is to deliver timely, reliable and innovative tips and information about financial matters, free of charge. The Winter 2016 special edition on cybersecurity can be read or printed at www.fdic.gov/consumers/consumer/news/cnwin16. Check back there for coming versions of this issue for e-readers and portable audio (MP3) players. To find current and past issues, visit www.fdic.gov/consumernews, or request paper copies by contacting the FDIC's Public Information Center in writing at 3501 North Fairfax Drive, Room E-1002, Arlington, VA 22226, by emailing publicinfo@fdic.gov, or toll-free at 1-877-275-3342.To receive an email about each new issue of the quarterly *FDIC Consumer News* with links to stories, go to www.fdic.gov/about/subscriptions/index.html.

The FDIC encourages financial institutions, government agencies, consumer organizations, educators, the media, and anyone else to help make the tips and information in *FDIC Consumer News* widely available. The publication may be reprinted in whole or in part without permission. Please credit *FDIC Consumer News*. Organizations also may link to or mention the FDIC Web site.

Date: 01/13/16
Subject: **Tax Identity Theft Awareness**

As Americans begin the process of filing tax returns, identity thieves are scheming to get their hands on that money. Tax Identity Theft has been the most common form of identity theft reported to the Federal Trade Commission for the past five years. PNB is using Tax Identity Theft Awareness Week, January 25-29, to raise consumer awareness and provide tips to prevent Tax Identity fraud.

Identity thieves look for every opportunity to steal your information, especially during tax season, and consumers should be on high alert and take every step they can to protect their personal and financial information.

Tax Identity Fraud takes place when a criminal files a false tax return using a stolen Social Security number in order to fraudulently claim the refund. Identity thieves generally file false claims early in the year and victims are unaware until they file a return and learn one has already been filed in their name.

To help consumers prevent Tax Identity fraud, PNB is offering the following tips:

- **File early.** File your tax return as soon as you're able giving criminals less time to use your information to file a false return.
- **File on a protected wi-fi network.** If you're using an online service to file your return, be sure you're connected to a password-protected personal network. Avoid using public networks like a wi-fi hotspot at a coffee shop.
- **Use a secure mailbox.** If you're filing by mail, drop your tax return at the post office or an official postal box instead of your mailbox at home. Some criminals look for completed tax return forms in home mailboxes during tax season.
- **Find a tax preparer you trust.** If you're planning to hire someone to do your taxes, get recommendations and research a tax preparer thoroughly before handing over all of your financial information.
- **Shred what you don't need.** Once you've completed your tax return, shred the sensitive documents that you no longer need and safely file away the ones you do.
- **Beware of phishing scams by email, text or phone.** Scammers may try to solicit sensitive information by impersonating the IRS. Know that the IRS will not contact you by email, text or social media. If the IRS needs information, they will contact you by mail first.
- **Keep an eye out for missing mail.** Fraudsters look for W-2s, tax refunds or other mail containing your financial information. If you don't receive your W-2s, and your employer indicates they've been mailed, or it looks like it has been previously opened upon delivery, contact the IRS immediately.

If you believe you're a victim of Tax Identity Theft or if the IRS denies your tax return because one has previously been filed under your name, alert the IRS Identity Protection Specialized Unit at 1.800.908.4490. In addition, you should:

- **Respond immediately to any IRS notice** and complete IRS Form 14039, Identity Theft Affidavit.
- **Contact your bank immediately**, and close any accounts opened without your permission or tampered with.
- **Contact the three major credit bureaus** to place a 'fraud alert' on your credit records:
    - Equifax, www.Equifax.com, 1.800.525.6285

  - Experian, www.Experian.com, 1.888.397.3742
  - TransUnion, www.TransUnion.com, 1.800.680.7289
- **Continue to pay your taxes** and file your tax return, even if you must do so by paper.

More information about tax identity theft is available from the FTC at ftc.gov/taxidtheft and the IRS at irs.gov/identitytheft.

In order to protect your personal information:

- Check your credit report on a regular basis for incorrect information. You are entitled to one free credit report each year at www.annualcreditreport.com or by calling 1.877. 322.8228.
- Do not to respond to any email that directs you to update your personal information by replying to the email or by dialing a telephone number. Only use the customer service number on the back of your debit or credit card.
- PNB personnel will never ask you to update your personal information via email or over the telephone.
- You may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You may contact the FTC by calling 1.877.IDTHEFT (1.877.438.4338) or online at https://www.ftccomplaintassistant.gov/.

FRAUD ALERT

Dear Customer:

It is important to identify and combat a type of Internet scam known as "phishing". The term is a play on the word "fishing," and that's exactly what Internet thieves are doing--fishing for confidential financial information, such as account numbers and passwords. With enough information, a con artist can run up bills on another person's credit card or, in the worst case, even steal that person's identity.

In a common type of phishing scam, individuals receive e-mails that appear to come from their financial institution. The e-mail may look authentic, right down to the use of the institution's logo and marketing slogans. The e-mails often describe a situation that requires immediate attention and then warn that the account will be terminated unless the e-mail recipients verify their account information immediately by clicking on a provided link.

The link will take the e-mail recipient to a screen that asks for account information. While it may appear to be a page sponsored by a legitimate financial institution, the information will actually go to the con artist who sent the e-mail.

The federal financial regulatory agencies want consumers to know that they should never respond to such requests. No legitimate financial institution will ever ask its customers to verify their account information online. It is also advisable:

- Never click on the link provided in an e-mail if there is reason to believe it is fraudulent. The link may contain a virus.
- Do not be intimidated by e-mails that warn of dire consequences for not following their instructions.
- If there is a question about whether the e-mail is legitimate, go to the company's site by typing in a site address that you know to be legitimate.
- If you fall victim to a phishing scam, act immediately to protect yourself by alerting your financial institution, placing fraud alerts on your credit files and monitoring your account statements closely.

If you believe that you have provided sensitive financial information about yourself through a phishing scam, you should:

- Immediately contact your financial institution.
- Contact the three major credit bureaus and request that a fraud alert be placed on your credit report. The credit bureaus and phone numbers are: Equifax, 1-800.525.6285; Experian, 1.800.397.3742; and TransUnion, 1.800.680.7289.
- File a complaint with the Federal Trade Commission, FTC at www.consumer.gov/idtheft, or by calling 1.877.438.4338.

AVISO DE FRAUDE

Estimado Cliente:

Es importante identificar y combatir un tipo de fraude a través del Internet conocido como "phishing". Este término viene de la palabra “fishing” (pescando), y es exactamente lo que están haciendo los estafadores por Internet, pescando información financiera confidencial de una persona, como son sus números de cuenta y claves. Con suficiente información, un estafador puede hacer crecer rápidamente cuentas de pagos en la tarjeta de crédito de una persona, o en el peor de los casos, robar la identidad de un individuo.

En una forma común de fraude, las personas reciben correos electrónicos que parecen venir de su institución financiera. El correo electrónico puede parecer auténtico, con logotipo y lemas de mercadeo de la institución. Los correos electrónicos a menudo describen una situación que requiere inmediata acción y luego alertan que la cuenta será cerrada, a menos que quienes estén recibiendo el mensaje verifiquen inmediatamente la información de sus cuentas haciendo “click” en el enlace proporcionado.

El enlace llevará el correo electrónico de quien recibe el mensaje a una pantalla que le pedirá información de la cuenta, y aunque pueda lucir como una página patrocinada por una institución financiera legítima, en realidad la información irá al portal del estafador que envió el correo electrónico.

Las agencias reguladoras federales financieras desean que los consumidores conozcan que nunca deberían responder a tales solicitudes. Ninguna institución financiera legítima le pedirá a sus clientes verificar información de sus cuentas a través del Internet.

También es aconsejable:

- Nunca hacer “click” al enlace proporcionado, dentro de un correo electrónico, si hay razón para creer que es fraudulento. El enlace puede contener virus. - No se deje intimidar por correos electrónicos que alertan de lamentables consecuencias por no seguir sus instrucciones.
- Si cree que el correo electrónico no es legítimo, visite el portal de la empresa usando la dirección de Internet que usted sabe es legítima.
- Si Ud. es víctima de fraude por Internet, para su protección, debe actuar rápidamente notificando a su institución financiera, colocando alertas de fraude en sus archivos de crédito y monitoreando sus estados de cuenta constantemente.

Si cree que ha proporcionado información financiera confidencial a través de este tipo de fraude, Ud. debe: -

Informar inmediatamente a su institución financiera.

- Contactar a las tres agencias nacionales de crédito y solicitar se coloque una alerta de fraude en su reporte de crédito. Los nombres y teléfonos de estas agencias son: Equifax 1.800.525.6285; Experian 1.800.397.3742; y TransUnion 1.800.680.7289.
- Presentar queja formal con la Comisión Federal de Comercio, FTC a través de la página de Internet www.consumer.gov/idtheft o llamando al número 1.877.438.4338.