# Pacific National Bank
## FRAUD AND CUSTOMER NOTIFICATION ALERTS

Date: 07/08/20
Subject: **COVID-19 Imposter Scams**

PNB advising everyone to please be alert to COVID-19 impostor scams, which generally involve fraudsters posing as officials or representatives from the IRS, the Centers for Disease Control and Prevention, the World Health Organization or other healthcare or nonprofit groups and academic institutions. Such scams often seek to coerce victims to provide personal information or send payment in order to receive coronavirus-related government benefits, or to share information as part of contact tracing efforts.

Date: 02/18/20
Subject: **Five Ways to recognize a Social Security scam – by Erin Scheithe**

In July, the Consumer Financial Protection Bureau (CFPB) reported on a rise in scam attempts where Social Security beneficiaries were being asked to pay to reactivate, protect, or restore their benefits. Currently, Social Security scams are the most commonly reported type of fraud and scam, and according to the Social Security Administration's Office of the Inspector General (OIG), these scams continue to evolve. The OIG is now warning the public that scammers are making phone calls and then following up with emails containing falsified documents aimed at convincing people to pay.

You may have received one of these calls – either a recorded voice or a person falsely claiming to be a government employee, warning you of an issue with your Social Security number, account, or benefits, including identity theft. The caller may threaten arrest or other legal action, or they may offer to increase benefits, protect your assets, or resolve identity theft if you provide payment using a retail gift card, cash, wire transfer, internet currency such as Bitcoin, or a pre-paid debit card.

**How to tell if it's legitimate or a scam**
Scammers are aware that people are catching on to their attempts, so they're coming up with new ways to convince Social Security beneficiaries that their frauds are legitimate. Here's what to watch for so you can protect yourself and others from Social Security scams.

**1. Threatening arrest or legal action:** If you receive a threatening phone call claiming that there's an issue with your Social Security number or benefits, it's a scam. The Social Security Administration (SSA) will never threaten you with arrest or other legal action if you don't immediately pay a fine or fee.

**2. Emails or texts with personally identifiable information:** If there's a legitimate problem with your Social Security number or record, the SSA will mail you a letter to notify you of any issues.

**3. Misspellings and grammar mistakes:** If the caller follows up with emails containing falsified letters or reports that appear to be from the SSA or SSA's OIG, look closely. The letters may use government "jargon" or letterhead that appears official in order to help convince victims, but they may also contain misspellings and grammar mistakes.

**4. Requests for payment by gift or pre-paid card, cash, or wire transfer:** If you do need to submit payments to the SSA, the agency will mail a letter with payment instructions and options through U.S. mail. You should never pay a government fee or fine using retail gift cards, cash, internet currency, wire transfers, or pre-paid debit cards. Scammers ask for payment this way because it's difficult to trace and recover.

**5. Offers to increase benefits in exchange for payment:** Similarly, SSA employees will never promise to increase your Social Security benefits, or offer other assistance, in exchange for payment.

**How to report a scam**
If you think you've been the victim of a Social Security scam, report it immediately to the Federal Trade Commission (FTC) at FTC.gov/complaint and to the SSA Office of Inspector General Fraud at oig.ssa.gov .

Date: 01/02/20
Subject: **Tax Identity Theft Awareness Week**

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 27-January 31 2020, 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/.

Date: 10/01/19
Subject: **October is Cybersecurity Awareness Month**

At PNB we are always vigilant concerning privacy and fraud prevention. We would like to direct you to a website targeted directly to protection, fraud protection and prevention, reporting fraud, and enhanced security. We hope you will find this interesting and informative. http://www.diproductsite.com/security_microsite/

***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/.

Date: 05/24/19

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

The Office of the Comptroller of the Currency (OCC) has advised that consumers have reported receiving fictitious e-mail messages, allegedly initiated by the Office of the Comptroller of the Currency (OCC) or senior officials at the agency, regarding funds purportedly under the control of the OCC.

Any communication 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 poorly written email messages from the following email addresses, which are not associated with the OCC: [office2comptroller90@gmailcom], [deadhead@kfedisbroke.com], [*name*@kfedisbroke.com], [*name*@officeocc.com], [*name*@naver.com], [*name*@mynet.com], [*name*@outlook.com], and [123office@fork.ocn.ne.jp].

Following are four samples of frequently received messages:

**Example #1**

*"I write to inform you that after so much deliberation with the Federal Reserve System and the United Nation as regards unsettled debts, lottery and compensation funds, the sum of $1.5 million has been approved in your favor as result of all unsettled debts, lottery and compensation funds due to you. We have been trying to reach you to know if this funds has been remitted to you and 109.195.209.147glad we have finally reached you through our Cyber experts and will ensure you get this funds.*
*Will advise you reach me with below details so I can guild you on how best to have this already approved funds transferred to you:*
*Name:*
*Email: [name@mynet.com] (Will contact you with official email after we have opened communication)"*

**Example #2**

*"Hello,*
*I am **[NAME AND TITLE REMOVED]** United States Of America (OCC) you can read more about me here:* https://www.occ.treas.gov/about/who-we-are/leadership/index-leadership.html. *The Office of the Comptroller of the Currency (OCC) is an independent bureau within the United States Department of the Treasury that was established by the National Currency Act of 1863 and serves to charter, regulate, and supervise all national banks and thrift institutions and the federally licensed branches and agencies of foreign/local banks in the United States. A directive has been issued to us to settle all outstanding payments accrued to individuals with respect to local and overseas contract payment, debt re-scheduling and outstanding compensation payment. We have been notified that you are yet to receive your fund. Fortunately, you have been selected alongside a few other beneficiaries to receive your own payment of $1,500,000.00 (One Million Five Hundred Thousand United States Dollars only). This money will hence be transferred to your nominated bank account. To our surprise One **[NAME REMOVED]** wrote us that you asked her to claim the funds and presented below account details for the funds transfer:*
*Bank name :*
*Account name :*
*Account number:*
*Routing number:*
*Swift code:*
*Bank Address :*
*Most importantly, confirm to us urgently if you gave permission to **[NAME REMOVED]** to claim the fund on your behalf and if case you did not authorize anybody, then, You will have to stop communicating with the impersonators and the organizations, because they are trying to divert your fund to themselves. She tries, so hard to change the fund ownership to her name.*
*Await your response:*
*Email: [name@mynet.com]*
*Thanks."*

**Example #3**

*"Office of the Comptroller*
*of the Currency (OCC)*
*400 7th Street, SW*
*Washington, D.C. 20219*
*Thank you for your email and I will ensure* ***[NAME REMOVED]*** *is arrested. I am glad to have developed communication with you as the sole beneficiary to this funds and will ensure you get your funds which is in line of the oath of office. Again The Office of the Comptroller of the Currency (OCC) is an independent bureau within the United States Department of the Treasury that was established by the National Currency Act of 1863 and serves to charter, regulate, and supervise all national banks and thrift institutions and the federally licensed branches and agencies of foreign/local banks in the United States. I have attached the OCC FORM for you to fill personal details as requested, please do not fill the part made for officials because this form is an evidence that establishes transaction between yourself and the Office of the Comptroller of the Currency (OCC) for reference purpose and to fulfil legal demands, after which your funds can be released to you. I will wait to read from you after you have filled the necessary details.*
*Thanks,*
*United States Of America (OCC).*
*Note: You can as well fill the needed details as below if you are unable to print out and fill, the Department will get it documented for you*
*Full Name:*
*Full Address:*
*Sex:*
*Age:*
*Next Of Kin:*
*Working Telephone Number:*
*Company Name:*
*Position in the company:"*

**Example #4**
*"THIS MAIL IS FOR THE OWNER OF THIS E-MAIL ADDRESS:*
*REGARDING YOUR APPROVED FUND: $136,000.000.00 US DOLLARS.*
*A payment which you are supposed to receive last year, this is a compensation payment approved to you by Office of the Comptroller of the Currency (OCC) . We are truly sorry for the delayed payment. Having reviewed all the obstacle and problems surrounding the release of your $136,000.000.00 USD. The bank manager Mr. [NAME REMOVED] of the First Citizens Bank he was behind in all the delay, his plan was to divert the funds to his personal bank account. I am really worried we never heard from you for the past months, i don't know if you are dead or still alive? Two people from California came to our office few days ago, a lady with a man they told us that you sent them to receive the $136,000.000.00 on your behalf. Here is the information they provided to us:*
*Street, LOS ANGELES, CA 90039*
*Names, [NAMES REMOVED]*
*Please confirm to us, do you know these two people from Los Angeles California? We are not comfortable with their claim to the $136,000.000.00 because i know that the $136,000.000.00 were approved to you by Office of the Comptroller of the Currency (OCC) . We don't want to release the money to a wrong person.*
*I wait to read back from you ASAP, also confirm if those two people [NAMES REMOVED] were sent by you?*
*Thank you"*

The communication may include a fictitious "Funds Clearance Application Form," a sample of which is attached. Consumers should understand that as email addresses are reported and shut down, the scammers will continue to create new email addresses. Do not respond in any manner to any proposal purported to be issued by the OCC that requests personal account information, or requires the payment of any fee in connection with the proposal, or suggests the OCC is a participant in the transfer of funds for or on behalf of others. The OCC recommends that consumers file complaints with the following agencies, as appropriate:

- OCC: by email at occalertresponses@occ.treas.gov; by mail to the OCC's Special Supervision Division, 400 7th St. SW, MS 8E-12, Washington, DC 20219; by fax to (571) 293-4925; or by calling the Special Supervision Division at (202) 649-6450.
- U.S. Department of the Treasury, Office of Inspector General (OIG): by telephone at (800) 359-3898 or by visiting the OIG website.
- Federal Trade Commission (FTC): by telephone at (877) FTC-HELP or, for filing a complaint electronically, via the FTC's website.
- National Consumers League (NCL): by telephone at (202) 835-3323 or by email. To file a fraud complaint, visit the NCL fraud website.
- Better Business Bureau (BBB): The BBB system serves markets throughout Canada, Puerto Rico, and the United States and is the marketplace leader in advancing trust between businesses and consumers. The website offers contact information for local BBBs, objective reports on more than 2 million businesses, consumer scam alerts, and tips on a wide variety of topics that help consumers find trustworthy businesses and make wise purchasing decisions.
- Federal Bureau of Investigation Internet Crime Complaint Center (to report scams that may have originated via the internet).
- If correspondence is received via the U.S. Postal Service, contact 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.

Additional information concerning this matter that should be brought to the attention of the Office of the Comptroller of the Currency (OCC) may be forwarded to

Office of the Comptroller of the Currency
Special Supervision Division

400 7th St. SW, MS 8E-12
Washington, DC 20219
Phone: (202) 649-6450
Fax: (571) 293-4925
www.occ.gov
occalertresponses@occ.treas.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.