Pacific National Bank

FRAUD AND CUSTOMER NOTIFICATION ALERTS

Date: 08/19/24
Subject: **Important Information Regarding National Public Data (NPD) Data Breach**

We want to inform you that National Public Data (NPD) has suffered a massive data breach. This breach exposed 2.9 Billion records that include names, social security numbers, address history, phone numbers and other personal information.

We recommend you use the tool created by security firm, Pentester, to determine if your records may have been exposed.

https://npd.pentester.com/

If your data was exposed, you may want to consider placing a freeze on your credit with the three major credit reporting agencies.

- **Equifax** - Equifax.com/personal/credit-report-services - 800-685-1111
- **Experian** - Experian.com/help - 888-EXPERIAN (888-397-3742)
- **TransUnion** - TransUnion.com/credit-help - 888-909-8872

We understand that such news can be concerning, so we want to reassure you that Pacific National Bank is taking all necessary steps to ensure your account and personal information remain secure. As a result of this breach, the Bank may implement additional security measures to validate your identity. These additional measures are to ensure the security of your data and accounts with Pacific National Bank. Thank you for trusting Pacific National Bank.

Date: 05/29/24
Subject: **Fictitious Notification Regarding the Release of Funds Supposedly Under the Control of the Office of the Comptroller of the Currency**

Consumers have reported receiving various fictitious via email, Google Chat, and the U.S. Postal Service related to up-front fee scams involving fictious inheritance or beneficiary payouts. The notifications appear to be initiated by senior officials at the Office of the Comptroller of the Currency (OCC) regarding funds purportedly under the control of the OCC. Scam correspondence may include the names of other governmental agencies who are purportedly involved in the fake transaction.

In all instances, victims are initially contacted regarding funds being held on their behalf by the OCC and are asked to provide the scammers general personal information including name, address, and telephone number.

Follow-up correspondence from the scammers includes requests for more specific personal information including, but not limited to Social Security number, bank account details, and copies of driver's licenses and passports. Correspondence is generally poorly written with typographical and grammatical errors and may include instructions for the victim to pay thousands of dollars in required fees or taxes for the release of the supposedly held funds.

These scams not only involve the theft of victim funds, but also their identities. There are at least four know variations of this scam.

Variation #1
Victims are initially contacted via email regarding unclaimed assets being held on their behalf by the OCC. The correspondence further states that final payment will be made to the victim via bitcoin. Email addresses used in this scam include:

- [Citibankcentral.usa@gmail.com]
- [occfile.details@hotmail.com]

Refer to Sample Fictitious Correspondence Variation 1 for an example of the fictitious correspondence.

Variation #2
Following initial contact by the scammers, victims receive letters with the subject line of "Request for Currency Conversion Settlement," which include an embedded image of the victim's passport as well as reference to their Social Security number. The victim is instructed to pay a currency conversion fee of $5,500 for the held funds to be credited to the victim's bank account. Scammers conducting this fraud typically use a telephone number of (202) 978-7477, which is not affiliated with the OCC.

Refer to Sample Fictitious Correspondence Variation 2 for an example of the fictitious correspondence.

Variation #3
Victims of previous financial scams are contacted via telephone and email by individuals identifying themselves as employees of the Financial Crimes Division of the OCC. The alleged purpose of the communication is to notify the revictimized individuals that the OCC is issuing a large dollar compensation payment to them for money lost in previous scams. The victims of this scam are informed that they must pay $1,500 in attorney fees prior to receiving a compensation check. Once the fee is paid, victims are instructed to visit an OCC Office to retrieve a large dollar compensation check. Non-OCC-affiliated contact information used in this scam includes:

- Loretta Shepard (fictitious OCC employee)
- Ray Parker (fictitious OCC employee)
- David Bradley (authorized agent)
- [Deptoftreasury@usa.com] / (202) 968-0104

Refer to Sample Fictitious Correspondence Variation 3 for an example of the fictitious correspondence.

Variation #4
Once purported fees and taxes are paid to the scammers, the victims are instructed to visit an OCC office to retrieve a large-sum check supposedly being held for them.

Scammer contact information being used in this fraud includes, but is not limited to:

- [pugha2410@gmail.com]
- [Frank.Anselmo@outlook.com]
- [Info.federalreservebank101@gmail.com] / (203) 516-7051
- [militarybase.military72base11@gmail.com]
- [danibaker123@gmail.com]
- Kimberly A Jabal (via Google Chat, purports to be associated with an overnight delivery service)
- Richard A Varn (via Google Chat, purports to be associated with a financial institution)

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. Recipients of such correspondence should not respond in any manner to a proposal purportedly issued by the OCC that requests personal identifiable information, requires the payment of any fee in connection with a proposal, or suggests the OCC is a participant in the transfer of funds for or on behalf of others.

Consumers who have provided personal information to a scammer should immediately contact their financial institution to take steps to safeguard their assets. Additionally, consumers should file an identity theft report with the Federal Trade Commission's Identity Theft Division (https://www.identitytheft.gov) and initiate a recovery plan by following the instructions on the website.

Consumers who have been victimized or targeted in an upfront fee scam should file complaints with the following agencies, as appropriate:

- U.S. Department of the Treasury, Office of Inspector General (OIG): by telephone at (800) 359-3898 or by visiting the OIG website at https://www.oig.treasuryt.gove/report-fraud-waste-and-abuse
- Federal Trade Commission (FTC): by telephone at (877) FTC-HELP or, for filing a complaint electronically, via the FTC's website at https://reportfraud.ftc.gov.
- National Consumers League (NCL): by telephone at (202) 835-3323 or by visiting the NCL fraud website at https://nclnet.org/fraud-org/.
- Federal bureau of Investigation Internet Crime Complaint Center at https://www.ic3.gov/ (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 compliant form at https://ehome.uspis.gov/fcsexternal/default.aspx.

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 OCCAlertResponses@occ.treas.gove.

For additional information regarding other types of financial fraud, please visit the OCC's Fraud Resources page - https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/index-fraud-resources.html

Date: 01/02/24
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 29-February 2, 2024, 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**. To report Identity Theft, use the **IdentityTheft.gov** website.

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 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: 09/05/23
Subject: **Fake Versions of two Android Apps – Signal and Telegram**

If you installed two apps on your ***Android*** or ***Galaxy*** phone that you thought were the messaging apps Signal and Telegram, please delete them immediately. These two apps, ***Signal Plus Messenger*** and ***FlyGram***, have subsequently been removed from the Play Store, the Galaxy Store, and third-party app storefronts from where they were sideloaded (installed from third-party app storefronts) on Android Phones. The Galaxy Store listings now state, "Application not supported" and "This app is no longer available for purchase or is not supported in this country".

These two apps were versions of Signal and Telegram that delivered malware to the phones that the apps were loaded on and are labeled as malicious apps capable of stealing your personal data; therefore, make sure to unlink your Signal and Telegram accounts from these apps before deleting them. The recommendation is to check your Connected Devices list periodically to make sure no unknown new device has been given access to your account.

Subject: **Protect Yourself From Email PHISHING Scams**

Identity thieves continue to focus on email PHISHING scams to obtain personal information to commit identity theft. Please protect yourself by knowing the following information:

- Do not trust any email that urgently requests your confidential information such as PINs, passwords, account numbers, or "special phrases". We will never ask you for this information.
- Do not click on any links contained within such an email and do not respond to such an email.
- Always keep your browser application current, and use a firewall, and anti-virus/anti-spyware.
- Please report any incidents to us.

For your Online Banking account, use a strong password (letters, numbers, special characters) and do not share it.

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.