Employee Assistance Program

Fraud Protection & Recovery

Taking proactive steps to monitor and secure your identity are of the utmost importance. Here are specific steps to consider if you've been impacted by identify theft or fraud:

Contact the Unemployment Office Fraud Division. Report someone is using your information to file claims. Your employer may have done this for you but you will want to ensure you provide any documentation needed to investigate.

Check credit reports (annualcreditreport.com). Accounts or activity that you don't recognize could indicate identity theft.

Place a fraud alert or Security Freeze on your credit file. Once you place a fraud alert with one bureau, they will alert the other two. Placing a Security Freeze with the credit bureaus locks your credit, making it inaccessible to creditors. You can now place a freeze on the credit bureaus websites for free. You can place the Security Freezes by going to these links:

- Experian: https://www.experian.com/ncaconline/freeze
- Transunion: http://www.transunion.com/credit-freeze/place-credit-freeze,
- Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Establish authentication on financial accounts. Ask your bank to require a password or pin to complete account transactions.

Set up an account with the Social Security Administration. This allows you to monitor your annual earnings to ensure a fraudster is not using your SSN for employment purposes.

File an IRS Affidavit. Alert the IRS of your compromised information by filling out the **IRS Affidavit.**

Place an alert with Chex Systems Alerts. This will help keep fraudsters from opening bank accounts in your name.

Change all your passwords regularly. Smart account management should include complex passwords that are changed regularly. Use a private email and different passwords on any financial accounts. Utilize two factor authentication features whenever possible.

Beware of phishing. Once fraudsters gather identifying information, they usually use official-looking texts, emails or phone calls to gather more data. Never click on any links in emails or respond to unknown senders. It may allow the fraudster to implant malware or viruses on your phone or computer.

Beware of phone scams. If you receive a call from a unemployment, social security or a bill collector or other source soliciting information or for money on a past due bill, you need to validate the request by calling entities directly confirm information and debts with verified phone numbers.

For more information on this topic or for further assistance, please contact your Employee Assistance Program by calling your toll-free number below or exploring resources online at EAPHelpLink.com.

---

www.EAPHelplink.com

Company Code: CITSPO

1.800.999.1077

KEPRO INTELLIGENT VALUE