

# COVID-19 AND IDENTITY THEFT

## Employee Assistance Program

### ■ **Unemployment Fraud Impact**

The spread of the novel coronavirus (COVID-19) has impacted many of us more than expected. With unemployment claims rising to more than 33 million Americans<sup>1</sup>, fraudsters have been using stolen personal information to collect someone else's Unemployment Insurance (UI) benefits.<sup>2</sup> This can cause serious problems for both employees and employers. Cigna is committed to helping you keep your private information secure.

### **Protecting yourself from unemployment fraud**

#### **Red Flags for ■ Unemployment Fraud**

- › Employer receives falsified UI claim
- › Filing a legitimate UI claim and finding one already exists
- › Surprise request for information from UI
- › IRS statement (Form 1099G) reporting supposed UI benefits

#### **Compromised Personally Identifiable Information**

- › May include full name, social security number, date of birth, addresses
- › May result in credit score damage
- › Fraudulent activity could lead to garnishments, overpayments and legal matters
- › Resolving credit issues related to identity theft can be time-consuming and stressful

#### **Available EAP Resources**

- › Unemployment fraud preventative steps *(described on page 2)*
- › Identity theft prevention best practices *(described on page 3)*
- › Free tools and discounted monitoring services *(described on page 3)*

The EAP described herein provides access to identity theft protection services offered by a US-based team of Fraud Resolution Specialists. If legal or financial advice is required, please contact an attorney or financial advisor.

**For more information  
and support, call EAP.**

- ➡ Free 60-minute consultation with a Fraud Resolution Specialist
- ➡ Free breach search tool and free ID Threat Score (dark web scan)
- ➡ Discounted monitoring services ([covid.clcidprotect.net](https://covid.clcidprotect.net))

### ■ **Help from professionals.**

With 20 years of industry experience, our identity theft protection program serves as an epicenter for education, guidance and counseling assistance to victims of fraud-related crimes. With your EAP benefit, you don't have to protect your private information on your own.

**Together, all the way.®**



## ■ **Unemployment Fraud Preventative Steps**

### **Steps to protect your identity**

**Contact your ■ Unemployment Office Fraud Division** at [www.dol.gov/general/maps/fraud](http://www.dol.gov/general/maps/fraud) if you suspect 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 necessary to investigate.

**Check your credit reports** for free at [annualcreditreport.com](http://annualcreditreport.com). Accounts or activity that you don't recognize could indicate identity theft.

**Set up an account ■ it ■ the Social Security Administration.** Creating an account at [ssa.gov/myaccount](http://ssa.gov/myaccount) allows you to monitor your annual earnings to ensure a fraudster is not using your SSN for employment purposes.

**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.<sup>3</sup>

**Consider credit and identity monitoring.** For broader protection, track both your credit and identity. Cigna EAP offers discounted monitoring services through CLC ID Protect (page 3).

**Placing a security freeze ■ it ■ the credit bureaus** locks your credit, making it inaccessible to creditors. You can go to credit bureau websites to place a security freeze for free. When placing a security freeze, the bureaus may send you a confirmation personal identification number (PIN) that you can use to lift the freeze at your convenience. We recommend only lifting the freeze temporarily when you need to use your credit. You can place a security freeze by going to these links:

- › **Experian:** <https://www.experian.com/ncaconline/freeze>
- › **Transunion:** <https://www.transunion.com/credit-freeze/place-credit-freeze>
- › **Equifax:** <https://www.freeze.equifax>

**Set up authentication on financial accounts.** Ask your bank to require a password or PIN to complete account transactions.

**File an IRS Affidavit.** Alert the IRS by filling out an [IRS Affidavit](#) if you suspect your personal information has been compromised.

**Use Che Systems Alerts.** If you suspect your personal information has been compromised, you can place an alert with [chexsystems.com](http://chexsystems.com) to alert banks and financial institutions. This helps prevent fraudsters from opening bank accounts in your name.

**File a police report.** If you suspect that you are a victim of identity theft, file a police report. Creditors typically require a police report to clear up fraudulent activity.

# Identity Theft Prevention Best Practices

## Steps to protect your identity

**Change all your passwords regularly.** Smart account management should include passwords that are changed frequently. Make passwords as complex as possible by including letters, numbers and symbols. Utilize two factor authentication features whenever possible.

**Be aware of phishing emails and phone scams.** When fraudsters obtain personally identifiable information, they often send official-looking texts, emails or phone calls to gather even more data. Do not click on suspicious links in emails, even from trusted contacts, or respond to unknown senders. If you receive a call from UI, the Social Security Administration, the IRS, your bank, a bill collector or other source that is soliciting information, you need to validate the request. Hang up and call the entities independently at their verified phone numbers.

## EAP Services Explained

**Staying vigilant against COVID-19 fraud: For a free consultation, please call your company's designated EAP toll-free number.**

Your free 60-minute identity theft fraud consultation assists you at the inception of a fraud-related emergency. A licensed, US-based Fraud Resolution Specialist will help you determine whether you've been a victim of identity theft and provide guidance for your current situation.

### Free online ID theft prevention tools

Dark Web Scan with ID Threat Score – A one-time full scan of the dark web for appearances of your SSN.

Breach Search Tool – Unlimited access to search your email address for involvement in data breaches.

**\$14.95 per month upgrade Premium Protection**

This includes credit monitoring, identity monitoring and full-service restoration.

As a Cigna EAP customer you have access to discounted monitoring services, reduced from \$14.95/mo to \$10.95/mo.

## Simple to Start

### 1. Start by visiting [covid.clcidprotect.net](https://covid.clcidprotect.net)

- ☐ Submit your name and email address
- ☐ Use our 'Welcome Email' to access online tools

*To access the Premium Protection upgrade, you must first register a free account.*

The Employee Assistance Program (EAP) described herein provides assessment and referral services to EAP participants for legal services offered by a network of contracted specialty firms through employer-based participation. Neither the EAP nor its employees directly or indirectly provide legal services, representation or advice. Legal assessment and referral services are not available to participants if the issue is related to a potential cause of action against the employer.

All Cigna products and services are provided exclusively by or through operating subsidiaries of Cigna Corporation, including Cigna Health and Life Insurance Company, Connecticut General Life Insurance Company, Cigna Behavioral Health, Inc., and HMO or service company subsidiaries of Cigna Health Corporation. The Cigna name, logo, and other Cigna marks are owned by Cigna Intellectual Property, Inc.

