



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, fraudsters have been cashing in on their victim's personal information by collecting Unemployment Insurance (UI) benefits*. This can cause serious problems for both employees and employers. Cascade Centers is committed to helping keep your private information, private.

Protecting yourself from COVID-19 unemployment fraud

Red flags for Victimization

- 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

- Full name, Social Security number, date of birth, addresses
- May result in credit score damage
- May result in garnishments, overpayments and legal matters
- Increased stress to resolve issues

Available EAP Resources

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

Help from your EAP 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.

For more information, call
800-433-2320

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.ccidprotect.net)

**US News, Unemployment During Coronavirus Pandemic. Accessed 7 May 2020.*

Unemployment Fraud Preventative Steps

Steps to protect your identity

Contact your Unemployment Office Fraud Division at <https://www.dol.gov/general/maps/fraud> to 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 your credit reports for free at annualcreditreport.com. Accounts or activity that you don't recognize could indicate identity theft.

Set up an account with the Social Security Administration. Creating an account at 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.

Consider credit and identity monitoring. True protection tracks both your credit and identity. Cascade Centers offers discounted monitoring services through CLC ID Protect (*page 3*).

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. When placing a security freeze, the bureaus may send you a confirmation pin number that will be used to lift your freeze at your convenience. We recommend only lifting the freeze temporarily when you need to use your credit. You can place the security freezes by going to these links:

Experian: <https://www.experian.com/ncaonline/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 of your compromised information by filling out the IRS Affidavit.

Use Chex Systems Alerts. You can place an alert with chexsystems.com to alert banks and financial institutions of your compromised information. This will help keep fraudsters from opening bank accounts in your name.

File a police report. If you have proof that you are a victim, make sure to file a police report. A police report is typically a required document by most creditors 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 regularly. Make them as complex as possible by including letters, numbers and symbols. Utilize two factor authentication features whenever possible.

Beware of phishing emails and phone scams. Once fraudsters gather personally identifiable information, they usually send official-looking texts, emails or phone calls to gather even more data. Never click on any links in emails or respond to unknown senders. If you receive a call from UI, Social Security, 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. Free consultation, call 800-433-2320.

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 identify whether you've been a victim of identity theft and provide guidance to 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 instances of your SSN.

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

\$ **10**^{.95}

Per month upgrade to Premium Protection!
This includes credit monitoring, identity monitoring and full-service restoration.

Cascade Centers offers discounted monitoring services, reduced from \$14.95/mo. to \$10.95/mo.

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

Simple to Start!

1

Start by visiting covid.clcidprotect.net

2

Submit your name and email address

3

Use our 'Welcome Email' to access online tools