

COVID-19

UNEMPLOYMENT Fraud

FRAUDULENT CLAIMS ARE ON THE RISE

It's Monday morning and you get a call from one of your team members asking about a notice they just received from the state unemployment office. They are asking what they need to do with the unemployment benefit determination or debit card they just received, and you are confused because they have been working their regular schedule so they should not be filing with the state. Do you chalk this up as a simple error or is there some action you need to take?

Most likely, this is a fraudulent claim that has been filed without your team member's knowledge. Thomas & Company has seen a significant increase in the volume of fraudulent unemployment claims being filed. Taking advantage of an overloaded unemployment system, there are bad actors out there who are using personal information, obtained through identity theft or data breaches, to file for unemployment benefits in hopes that their fraudulent claim will just blend in with the millions of legitimate claims being filed.

How widespread is Unemployment Fraud?

The U.S. Department of Labor issued a notification to the state unemployment agencies back in March warning that as a result of the COVID-19 pandemic to expect an increase in this type of activity. Other government agencies have also been involved in the investigation of unemployment fraud attributable to identity theft.

The U.S. Secret Service issued an alert in May reporting information was received that indicated a Nigerian fraud ring was exploiting the COVID-19 crisis and was committing large scale fraud against state unemployment insurance programs.

Although certain states were being targeted initially, the US DOL indicated it was extremely likely every state was vulnerable and would be targeted. The FBI is also involved in the investigation of this activity and issued a press release in July confirming there has been a spike in fraudulent unemployment claims being filed related to the COVID-19 pandemic that involved the use of stolen personal information. The report indicated stolen identities are being obtained using a variety of techniques that include the online purchase of stolen PII, information available as a result of previous data breaches, computer intrusions, and from public websites and social media accounts, among other methods.

How can Thomas & Company help?

We identified an increase in this type of activity in the states mentioned in the alert, and as indicated, it has spread to other state agencies. When unemployment fraud began to rise a few years ago, Thomas & Company senior management had the opportunity to engage with numerous state unemployment fraud investigators, FBI agents, Special Agents with the U.S. Department of Labor and representatives with the Attorney General's office in several states.

One of the objectives of these meetings was to determine what actions can be taken when an unemployment claim has been fraudulently filed using the identity of another person.

The first step is for Thomas & Company, or any employer, to file a response with the unemployment agency to alert the state that a claim was fraudulently filed using the identity of an active team member. Please be aware that team members at all levels of the American workforce have had their identity used to file fraudulent unemployment claims, up to and including corporate CEO's. The fraud investigators we partnered with also recommended that the team member contact the fraud unit directly to report that their identity has been used to file a claim for UI benefits. This allows the fraud investigators to obtain information directly from the fraud victim to help resolve the case.

We will provide you with a state specific memo that outlines exactly what actions need to be taken and provide you with the state specific contacts and procedures to report the possible fraud. Based on recommendations provided by the majority of government agents we have partnered with; the memo also includes:

- A link to the Federal Trade Commission website for identity theft that has detailed information on the actions a victim of identity theft should take to protect themselves from further use of their stolen identity.
- The memo also includes the contact information for our Vice President of Regulatory Affairs in the event a client or their team member has any questions or wish to have a discussion concerning this issue.

We also have prepared an Employer Guide for fraud, including identity theft, that is available to our clients and their team members. This guide is included on the next few pages and can be shared with your team members. In consideration of the current volume of fraudulent claims being filed as a result of identity theft, Thomas & Company is making regular revisions to the guide including updating state contact information as individual agencies are making changes in how this type of fraud can be reported due to the increased activity.

How do you spot these fraudulent claims?

Some cases are easy to spot – your CEO calls and asks why he has received information from the state about a claim. That is most likely a fraudulent claim. If you receive a claim for someone who is still employed and they did not file for unemployment, or a claim for someone who has never been employed by your company, this could be a sign of unemployment fraud.

Why is reporting fraudulent claims so important?

Even though most claims filed due to COVID-19 will not be directly charged to your account, the monies paid out by the states to the 32 million unemployment workers – or one in every five people in the US workforce - are draining the state trust funds. Although the federal government is fully funding the additional benefits under the CARES Act, the act doesn't include funding to help states finance the huge increases in regular unemployment insurance benefits. When the state trust fund balances are depleted, the state's raise employers tax rates to build those balances back up. It will take years for the state trust funds to recover to pre-pandemic levels meaning that your tax rates can be impacted for years to come.

What should my team member do if they think they have been a victim of fraud?

Just as importantly, the impact to your team member should not be ignored. At best, their identity was only used to file for unemployment benefits. Unfortunately, in some cases, their identify may be used in other ways and they need to take actions to protect themselves and their identity from further harm. By following the guidelines that Thomas & Company has outlined with assistance from the various governmental agencies, they can quickly take actions to protect their identity from further harm. Please feel free to share this packet with any impacted team member.

It is recommended that the team member contact the state agency in question to report that their identity has been used to claim unemployment benefits. Filing a claim with another person's identity is a felony and is subject to prosecution. Therefore, the agency would like to obtain additional information for their case file. If our office receives a

fraudulent claim, we will file a response to indicate that the team member is job attached and has not filed a claim for benefits. We will also monitor the employer's account to ensure there are no erroneous charges associated with the claim.

The team member is also encouraged to review the Federal Trade Commission website (<https://www.consumer.ftc.gov/features/feature-0014-identity-theft>) for additional information and guidance related to identity theft. Recommended actions include, but are not limited to:

- Contact bank and credit card companies.
- Communicate with the IRS and complete the form associated with identity theft.
- Contact all three of the credit reporting agencies to place a freeze on their credit report.
- Contact the Social Security Administration.

How will this impact their ability to file for and collect unemployment benefits?

A team member who has been a victim of identity theft will still be able to file for and collect unemployment benefits. The state will remove the fraudulent case from the record once a claim is determined to be fraudulent. However, some states will put a hold or lock on the team member's account to protect them from future fraudulent activity. In these cases, the team member may have to start the claim process with their state's fraud unit so that their claim can be unlocked. We have found that this often helps speed up the process and jumps them "ahead" in the line.

Are there other types of fraud we should be looking for?

While most of the fraudulent claims that we are seeing are the result of possible identity theft, there also may be more intentional acts of fraud committed by your team members such as:

- knowingly submitting false information;
- continuing to collect benefits when knowing oneself to be ineligible;
- not being able and available to work while certifying for benefits under state law;
- or intentionally not reporting wages or income while collecting full benefits.

The state workforce agencies conduct routine audits to identify these types of fraudulent activities and will make a

determination if the act was intentional or a simple misunderstanding. If you are made aware of these types of activities, it is important to report them to protect your account and the Trust Fund balances.

What are the penalties for intentional unemployment fraud?

All states are required to assess a penalty of not less than 15% of the amount of the fraudulent payment. Other penalties under state unemployment insurance laws generally include:

- criminal prosecution with fines and/or incarceration;
- required repayment of fraudulently collected benefits;
- forfeiting future income tax refunds;
- and/or permanent loss of eligibility for unemployment compensation.

Commission of unemployment benefit fraud may also be prosecuted by the U.S. Department of Justice in federal courts under 18 U.S.C § 1341 or other appropriate federal statutes.

In addition to notifying Thomas & Company of suspected fraudulent activity, you should report the fraud to the State Workforce Agency and alert them of the following:

- Who is committing fraud?
- What is their Social Security number or employer number?
- What are they doing?
- When did they start doing this?

Our Unemployment Fraud Contact Directory at the end of this document lists the hotlines for reporting unemployment fraud to the state agencies. Many states allow the employer to remain anonymous when reporting this type of fraudulent activity.

Our office has been monitoring critical issues in the unemployment system such as this since our inception and the growing number of fraud cases during the COVID-19 pandemic is no exception. We will continue to provide updates to our clients as they become available. As always, if there are any questions please do not hesitate to contact us or visit our website at www.thomas-and-company.com.

UI Claimant Fraud Contacts				
State	Phone	Email	Online	Form
AK	877-272-4635	uifraud@alaska.gov		
AL	800-392-8019	BPC@labor.alabama.gov	AL Online Fraud Reporting	
AR	855-225-4440	ADWS.Info@arkansas.gov	AR Online Fraud Reporting	
AZ	800-251-2436		AZ Online Fraud Reporting	
CA	800-229-6297		CA Online Fraud Reporting	
CO	303-318-8225		FL Online Fraud Reporting	
CT	800-894-3490	dol.bpcu@ct.gov	CT Online Fraud Reporting	
DC	877-372-8360			
DE	302-761-8397			
FL	800-342-9909		FL Online Fraud Reporting	
GA	404-232-3440		GA Online Fraud Reporting	
HI	808-586-8947			
IA	515-281-5792		IA Online Fraud Reporting	
ID	877-540-8638	Fraud@labor.idaho.gov		
IL	800-814-0513		IL Online Fraud Reporting	
IN	800-891-6499		IN Online Fraud Reporting	
KS	785-581-7300	fraud@dol.ks.gov	KS Online Fraud Reporting	
KY	502-564-2387	uifraud@ky.gov	KY Online Fraud Reporting	
LA	800-201-3362		LA Online Fraud Reporting	
MA	877-626-6800	UIFraud@detma.org	MA Online Fraud Reporting	
MD	800-492-6804	ui.fraud@maryland.gov		MD Fraud Form
ME	207-621-5100	fraudreporting.mdol@maine.gov		ME Fraud Form
MI	866-500-0017		MI Online Fraud Reporting	
MN	651-296-8715		MN Online Fraud Reporting	
MO	573-751-4058, Option 4	ReportUIFraud@labor.mo.gov		MO Fraud Form
MS	800-843-8923	safe@mdes.ms.gov		
MT	406-444-0072	dliuidci@mt.gov	MT Online Fraud Reporting	
NC	919-707-1338		NC Online Fraud Reporting	
ND			ND Online Fraud Reporting	
NE	855-995-8863	NDOL.UnemploymentHelp@nebraska.gov	NE Online Fraud Reporting	
NH	800-852-3400, extension 84016		NH Online Fraud Reporting	
NJ	609-777-4304		NJ Online Fraud Reporting	
NM	505-243-7283	infodws@state.nm.us		
NV	775-684-0475		NV Online Fraud Reporting	
NY	888-598-2077		NY Online Fraud Reporting	
OH	800-686-1555, Option 1	ucbenprotest@jfs.ohio.gov	OH Online Fraud Reporting	
OK	405-557-5400	fraud@oesc.state.ok.us		
OR	877-668-3204		OR Online Fraud Reporting	
PA	800-692-7469		PA Online Fraud Reporting	
PR	*			
RI	401-462-1522	DLT.uitdifraud@dlt.ri.gov		
SC	803-737-2490		SC Online Fraud Reporting	
SD	605-626-7649		SD Online Fraud Reporting	
TN	615-206-3116	Esadmin.fraud@tn.gov		
TX	800-252-3642	TWC.fraud@TWC.state.tx.us		
UT	800-526-4400 (#4)	wsinv@utah.gov	UT Online Fraud Reporting	
VA	800-782-4001			
VI	*			
VT	802-828-4333		VT Online Fraud Reporting	
WA	800-246-9763		WA Online Fraud Reporting	
WI	800-909-9472		WI Online Fraud Reporting	
WV	800-779-6853	OICFraud@wv.gov		WV Fraud Form
WY	307-235-3236		WY Online Fraud Reporting	

* Puerto Rico and Virgin Islands do not have claimant contacts at this time.