

Protecting Your Business and Employees from Identity Theft

Identity theft is on the rise in both the private and public sector. The growing problem of committing unemployment fraud using stolen IDs not only affects the victims - those who have had their personal information compromised - but it also can have a negative effect on an employer's tax rate.

Identity theft occurs when someone uses another person's information to take on his or her identity. Identity theft can include wage and employment information as well as credit card and mail fraud. In the case of unemployment benefits, it could mean using another person's information such as name, Social Security Number and employment information.

As employers, you can help save millions of dollars in fraudulent payments by identifying suspected fraud. In many cases, you may be the first to have information that unemployment fraud is occurring.

What You Can Do to Protect Your Employees from UI Benefit Fraud and Lessen the Impact on Your Tax Rate

REVIEW Your Employer Notices

- Verify Social Security Numbers at the time of hire, to ensure that your employees' names and Social Security Numbers (SSN's) match the Social Security Administration's records. Visit the SSA at www.ssa.gov/employer to verify names and SSN's online.
- UI benefits paid to your current employees represent a charge to your account and may impact your tax rate. To protect your account, carefully review all notices received in your MiWAM account or by mail. When an employee files a claim for unemployment, employers will receive Form UIA 1575E, *Monetary Determination*, by mail and online via their MiWAM account. The monetary determination will contain information about the employee, the reason for separation, dates of employment and more. If you notice inaccurate information, or if the employee referenced is still working for you, it is very important that you notify us. Protesting the monetary determination (Form 1575E) timely in these occurrences may be the best way to stop a fraudulent claim from being paid.
- Review and verify all of the information on Form UIA 1136, *Bi-Weekly Statement of Charges/Credits to the Employer's Account*. This bi-weekly statement identifies each person receiving unemployment benefits and the amount being charged to your account.
- Review Form UIA 1770, *Summary of Statement of Benefit Charges and Credits*. This quarterly statement summarizes information previously included on Form UIA 1136.

Establish a Strong Data Security Plan

- Protect your employees' personal information.
- Do not use Social Security Numbers or driver's license numbers to identify employees on internal documents, correspondence, etc. Use an alternate employee ID number.
- Limit access to personal information to those employees who need it to perform their job duties.
- Don't mail, e-mail or fax correspondences to an outside source that include personal identifying information. Don't leave any personal information in plain view in the work place.
- Don't share your MiWAM or any other web account credentials where personal information is utilized.

What to Do if You Suspect Fraud or Identity Theft

- **Immediately** protest the *Monetary Determination* or the *Bi-Weekly Statement of Charges/Credits to the Employer's Account*. To be timely, the protest must be received by Unemployment Insurance no later than 30 calendar days from the mail date shown on the first page of the form (UIA 1575E or UIA 1136). Please note that although you have 30 days to protest, notifying us within 10 days of the mail date on the monetary determination will help prevent the claim from entering pay status.
 - To send a protest through MiWAM, select the *Account Services* tab, then the *Benefit Services* sub-tab. The link to *Determinations and Decisions* allow you to protest the Monetary Determination. The link to *View Benefit Charges & Credits* allows you to protest the UIA 1136, Bi-Weekly Statement of Charges/Credits to the Employer's Account.
 - To submit a written protest, mail or fax as instructed on the letter.
- Please be aware that once payments begin, they will continue until the investigative process is complete.
- Have the victim report the fraudulent activity **immediately** as well.
- You can also report fraud online at michigan.gov/uia through the *Report Fraud* or *Report Identity Theft* link or call the UI Fraud hotline at 1-855-UI-CRIME.

For more information on how you can protect your business from unemployment identity theft, contact our Office of Employer Ombudsman at 1-855-484-2636 or OEO@michigan.gov.

Resources for Victims of Identity Theft

Visit the Federal Trade Commission's web site at IdentityTheft.gov for the most up-to-date information on combatting identity theft. The site provides detailed advice to help you fix problems caused by identity theft along with the ability to:

- Get a personal recovery plan that walks you through each step.
- Update your plan and track your progress.
- Print pre-filled letters and forms to send to credit bureaus, businesses and debt collectors.
- Report it to the Federal Trade commission.
- Place a fraud alert and get your credit reports. A fraud alert is free. It will make it harder for someone to open new accounts in your name. To place a fraud alert, contact one of the three credit bureaus. That company must tell the other two.
 - Experian.com/fraudalert
 - TransUnion.com/fraud
 - Equifax.com/CreditReportAssistance
- Get your free credit reports from Equifax, Experian and TransUnion at annualcreditreport.com or call 1-877-322-8228.