Protecting Your Business and Employees from Unemployment Insurance (UI) Fraud

Fraudsters looking to defraud UI programs can target both employees and employers. Protection requires vigilance, attention to details and an understanding of common fraudulent behaviors. These tips can help you reduce the risk of UI fraud and protect your business from the financial and operational impact of fraudulent claims and schemes.

Secure Your Online Employer Account

Utilize strong passwords and Multi-Factor Authentication (MFA), when offered, to prevent unauthorized access. MFA adds another layer of security by requiring a one-time code from a secondary device, such as your cell phone, to complete the login process.

Review and Monitor UI Claims Information

Review any information on a claim you receive from the UI agency for accuracy (i.e. - notice of first payment, quarterly statements, wage requests). Report all inaccuracies and unusual/unauthorized UI claims linked to your employees.

Education and Awareness

Educate employees about the risks of identity theft and common cybercrime. These include phishing emails, suspicious phone calls, or fraudulent requests for personal information.

Ensure Your Employer Account is Accurate

Ensure your account information is updated and correct to receive requests and important information from UI.

Verify Requests for Employee Information

If you have doubts or questions regarding a request for employee information from a UI agency, contact the agency promptly by using the official contact information on the agency website to confirm the request.

Report Suspected UI Fraud

Immediately report suspected UI fraud to the appropriate state agency. If Identity theft is suspected, report it to the UI agency and law enforcement. More info: **Report Unemployment Identity Fraud**

Stay Informed Check the UI agency website for alerts on scams affecting UI claimants and employers. Always stay updated on the latest UI fraud trends and security measures.