FBI Sees Spike in Fraudulent Unemployment Insurance Claims Filed Using Stolen Identities

The FBI has seen a spike in fraudulent unemployment insurance claims complaints related to the ongoing COVID-19 pandemic involving the use of stolen personally identifiable information (PII).

U.S. citizens from several states have been victimized by criminal actors impersonating the victims and using the victims' stolen identities to submit fraudulent unemployment insurance claims online. The criminals obtain the stolen identity using a variety of techniques, including the online purchase of stolen PII, previous data breaches, computer intrusions, cold-calling victims while using impersonation scams, email phishing schemes, physical theft of data from individuals or third parties, and from public websites and social media accounts, among other methods. Criminal actors will use third parties or persuade individuals who are victims of other scams or frauds to transfer fraudulent funds to accounts controlled by criminals.

Many victims of identity theft related to unemployment insurance claims do not know they have been targeted until they try to file a claim for unemployment insurance benefits, receive a notification from the state unemployment insurance agency, receive an IRS Form 1099-G showing the benefits collected from unemployment insurance, or get notified by their employer that a claim has been filed while the victim is still employed.

The FBI advises the public to be on the lookout for the following suspicious activities:

- Receiving communications regarding unemployment insurance forms when you have not applied for unemployment benefits
- Unauthorized transactions on your bank or credit card statements related to unemployment benefits
- Any fees involved in filing or qualifying for unemployment insurance
- Unsolicited inquires related to unemployment benefits
- Fictitious websites and social media pages mimicking those of government agencies

Tips on how to protect yourself:

- Be wary of telephone calls and text messages, letters, websites, or emails that require you to provide your personal information or other sensitive information, especially birth dates and Social Security numbers. Be cautious with attachments and embedded links within email, especially from an unknown email sender.
- Make yourself aware of methods fraudsters are using to obtain PII and how to combat them by following security tips issued by the Cybersecurity and Infrastructure Security Agency, including:
  - Avoiding Social Engineering and Phishing Attacks
  - Protecting Against Malicious Code
  - Preventing and Responding to Identity Theft
- Monitor your bank accounts on a regular basis and request your credit report at least once a year to look for any fraudulent activity. If you believe you are a victim, review your credit report more frequently.

- Immediately report unauthorized transactions to your financial institution or credit card provider.
- If you suspect you are a victim, immediately contact the three major credit bureaus to place a fraud alert on your credit records. Additionally, notify the Internal Revenue Service by filing an Identity Theft Affidavit (IRS Form 14039) through irs.gov or identitytheft.gov.

If you believe you have been a victim of identity theft related to fraudulent unemployment insurance claims, report the fraud to law enforcement, state unemployment insurance agencies, the IRS, credit bureaus, and your employer's human resources department. The FBI encourages victims to report fraudulent or any suspicious activities to the Internet Crime Complaint Center at ic3.gov. You may consult identitytheft.gov for help in reporting and recovering from identity theft.