$5.6 Billion of Unemployment Insurance Benefits were lost in 2014 to improper payments.

The Federal Trade Commission recently announced that identity theft was the number one consumer complaint in 2014, marking the 15th year in a row the complaint topped the list.[1] What's different today versus 15 or 10 or even 5 years ago, is not only how easy it is to use stolen identities to perpetrate fraud, but also the type of fraud that's being perpetrated: government benefits fraud. While there are many government programs being defrauded, a rising form of identity-based government benefits fraud is unemployment insurance fraud.

Unemployment insurance fraud is increasing in frequency and sophistication

In a recent press conference announcing a bust of 40 suspects in an identity theft ring, a U.S. Attorney in Florida said it best, "As the heat has been going up on stolen identity-tax fraud the bad guys...still need to find other targets to use those stolen identities. The crime du jour is unemployment insurance claims."[2]

We know that unemployment insurance is an increasing target for organized criminal groups looking to use stolen identities to make a quick buck. In 2014, the U.S. Department of Labor reported that $5.6 billion, or 11.6% of total unemployment insurance payments made throughout the states were improper payments.[3] While some portion of the improper payments is due to administrative errors, overpayments and simple mistakes, fraud represents as much as 7% of the total improper payments.[4] This is why the U.S. Department of Labor granted over $66 million in 2015 to fund program integrity initiatives that aim to prevent identity fraud in 48 states.

The New Jersey Department of Labor has reported $4.4 million in identity fraud prevention in their unemployment insurance program.

LexisNexis®

Risk Solutions
Government

Here's the challenge: in most states, unemployment insurance agencies rely on self-reported data. It isn't like the "old days" when an individual appeared at the unemployment office, filled out the necessary paperwork, presented a picture ID and then went home to search for employment while waiting for a check to arrive in the mail. With more and more services moving online and increased demand to deliver benefits faster and more efficiently, states have made it easy—individuals can apply for unemployment insurance online. In most cases, all that is required to stake a claim for unemployment insurance is a name, a Social Security number (SSN) and information about their most recent employer.

This is extraordinarily problematic given the massive leaks of personal identification information (PII) through recent data breaches. As a result, there is a huge black market supply of PII, which has created unbelievably low prices for information like SSNs. The Office of the National Counterintelligence Executive estimates that SSNs can be purchased for as little as $3.[5] The availability of identity information coupled with its cheap price makes the prevention of identity fraud more difficult than ever before using traditional prevention methods. Simply put: states can no longer take the applicant's word for it that he or she is who they say they are and is the true owner of that identity. It's time to begin using a multi-layered approach to identity fraud prevention.

Stolen identities are big business

According to the Privacy Rights Clearinghouse, over 816 million personal identification information (PII) records have been breached since 2005.[6] The U.S. Census Bureau notes there are more than 320 million people in the United States today.[7] It is, therefore, likely that most people have had their PII stolen at least once, if not more than once.

Identity proofing solutions are effective and efficient

Identity proofing is already being used to prevent identity-based unemployment insurance fraud in several states and has saved the New Jersey Department of Labor over $4 million—protecting citizens against identity fraud and keeping program dollars going to those in need. Other states have seen similar success preventing identity-based fraud in program areas such as tax refund fraud, Medicaid fraud and Supplemental Nutrition Assistance Program fraud. The most effective identity fraud prevention methods use public records data, the device information, such as geolocation and IP Address, and hundreds of other elements along with sophisticated identity analytics and advanced linking technology to automatically assess the risk of an identity, then verify and authenticate a claimant's identity before the claim is submitted.

Based on sophisticated algorithms, the identity is given a risk score. An agency may choose to send the low risk identities immediately through to adjudication, whereas higher risk identities may be automatically routed to various levels of identity authentication. This can be done by a variety of means, including:

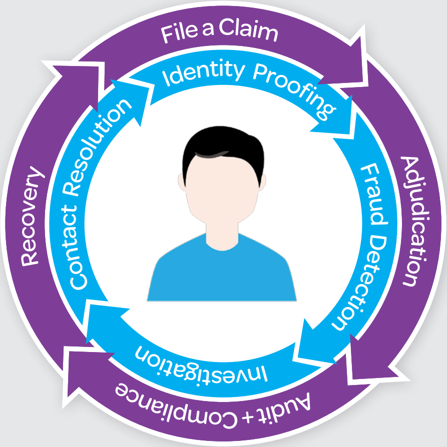
- Asking the applicant a series of questions, either through an automated online quiz or by telephone, to which only the authentic identity holder would know the answers
- Automatically sending a one-time-password to a known phone number or e-mail address
- Electronic verification of identity documents, such as driver's license or Social Security card via a mobile application
- For the highest risk identities, in person identity authentication may be requested

This multi-layered approach to identity authentication may sound familiar because the banking industry has effectively been using similar identity fraud prevention practices for years now.

The value of identity proofing solutions extends beyond just the dollar figures saved. Identity proofing solutions complement prevention practices currently in place and do not require an expensive and time consuming structural overhaul of the benefits system. Moreover, the proofing process does not impose a significant time hindrance on the applicant, and applicants always have the ability to opt-out of the quiz in favor of providing proof of identity in person.

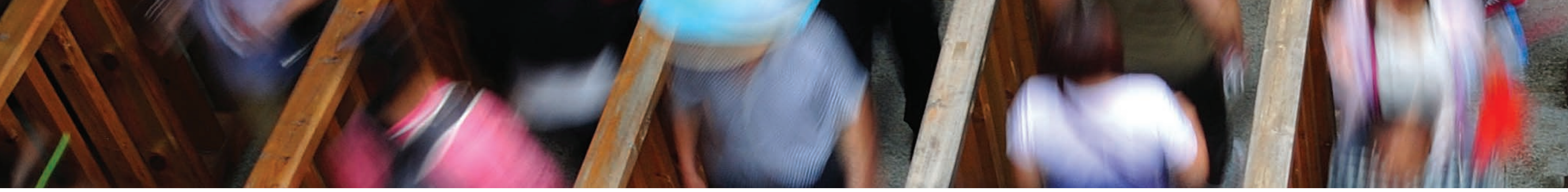
Comprehensive Identity Fraud Prevention Process

While the best strategy should be geared toward early fraud detection, it's also necessary to have the tools in place to continuously monitor for fraudulent activity, and recognize and investigate changes and anomalies that could indicate fraud at every phase of your agency's enrollment workflow. Continuous monitoring and investigation are important components in stopping fraud and also support the overall integrity of your agency's program and back-end overpayment recovery component.



Conclusion

As identity-based unemployment insurance fraud increases in popularity among organized criminal groups, states must ensure prevention technology outpaces the sophistication of threats. Identity proofing solutions have saved millions in their localized areas of implementation. Extrapolating from this, a nationwide identity proofing unemployment insurance effort has the potential to put a considerable dent in reducing the $5.6 billion in improper payments. It is in the best interest for the taxpayer who bears the financial consequences of fraud for each state to implement comprehensive and standardized identity proofing measures to ensure that unemployment insurance funds go to those who need them most.



For more information:

Visit IdentityGov.com/UnemploymentInsurance or call 888.579.7638

About LexisNexis Risk Solutions
LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our government solutions assist law enforcement and government agencies with deriving insight from complex data sets, improving operational efficiencies, making timely and informed decisions to enhance investigations, increasing program integrity, and discovering and recovering revenue.

LexisNexis®

[1] https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer-complaint-categories-again-2014

[2] http://www.miamiherald.com/news/local/crime/article17932964.html

[3] https://paymentaccuracy.gov/tracked/unemployment-insurance-ui-2014

[4] http://watchdog.org/122591/unemployment-fraud-congress/

[5] http://www.ncsc.gov/issues/cyber/identity_theft.php

[6] https://www.privacyrights.org/fs/fs33-CreditMonitoring.htm

[7] http://www.census.gov/newsroom/press-releases/2014/cb14-tps90.html