CYBERSCOUT®

Case Study

Washington Couple Overcomes Unemployment Insurance Fraud with Support from Cyberscout Identity Theft Resolution Services

In Washington state, officials estimate the damage of unemployment fraud at $550-$650 million[1]

Between March and April, unemployment fraud reports in Washington State jumped 27-fold[2]

1 Fox Television Stations, "FTC warns of 'large scale' unemployment fraud scam amid coronavirus pandemic," June 4, 2020.
2 Krebs on Security, "US Secret Service: "Massive Fraud" Against State Unemployment Insurance Programs," May 16, 2020.

Challenge

When Matt B. received a letter from the Washington state Employment Security Office encouraging him to consider creating a new business, it seemed like it had been sent in error. Then his wife, Lindsey, noticed something ominous—the letter included a claimant identification number and a claim date. Someone had stolen Matt's identity and used his Social Security Number to initiate a fraudulent unemployment claim.

"Matt's been one of the lucky people who was deemed an essential employee and never laid off. When we got this letter, at first, we just thought it was a mistake," recalled Lindsey. "Looking closer, we saw there was a claimant ID and a date of a claim on it of April 12th, while the letter itself was dated May 8th. It became scary at that point, because we knew something had been going on for a month."

As Americans rapidly lost tens of millions of jobs during the COVID-19 pandemic, the government temporarily implemented more generous unemployment benefits. The combination of additional money and overwhelmed state unemployment agencies attracted cybercriminals who generated an unprecedented number of fraudulent claims.

"At that time, there was just beginning to be reports in the news about Washington having a problem with unemployment fraud, so I can't say we were shocked. We just wanted to make sure that we got it shut down as quickly as we could, because we know these things can escalate and get out of hand," Lindsey said.

CYBERSCOUT®

Solution

Matt immediately notified both his employer and the Washington Employment Security Department. The couple placed temporary credit freezes with the three major credit bureaus.

Cyberscout identity management services are included as part of the couple's insurance policy, so they called for additional advice. Their Cyberscout fraud resolution specialist provided in-depth case management, guiding them through a step-by-step plan tailored to their situation and designed to shut down the unemployment fraud quickly and prevent future incidents.

"What I appreciated most was that Steven was very methodical. When you're a bit unsettled and rattled, it's really a benefit to have somebody who's got your back and making sure you don't miss little steps," said Lindsey, "It was really reassuring to have him there, knowing that he's been down this road many times before, whereas for us, it was the very first time."

Working with Stephen, Matt and Lindsey followed Cyberscout's guidance in order to:

- Place one-year fraud alerts on their credit accounts.
- Add verbal passwords on their financial accounts as an added layer of security.
- Open a fraud alert with ChexSystems to make sure the identity thief couldn't open a checking or savings account in Matt or Lindsey's names. This helped ensure that if the thief had succeeded in any fraudulent schemes, they would have had nowhere to go with the money.
- Request a copy of Matt's yearly earnings statement once he received notification that the fraudulent unemployment claim was resolved.
- Regularly review their credit reports and receive alerts of any suspicious activity.

"As far as I know, our case has been resolved. We got a letter from the Employment Security Department saying that they had completed their investigation and that the unemployment insurance claim is no longer connected to Matt's Social Security Number. That's reassuring, because if the COVID situation continues and he does get laid off, presumably he could then claim benefits legitimately," explained Lindsey.

About two months after the initial unemployment fraud, Matt received another letter, this time from a financial institution specializing in cryptocurrency.

It contained a debit card and encouraged them to activate a new account. They called Cyberscout and Steven investigated. Because they cancelled the card without activating the account, the identity thief could not steal any money.

*Although this story is based on an actual customer incident, some of the details have been changed to protect the actual customer

Results

The couple received a full year of Cyberscout credit monitoring benefits to help them catch any additional incidents, should they occur. Lindsey credits Cyberscout for putting her mind at ease:

"I'm not spending a lot of time thinking about it anymore. It's been dealt with, and that year of free credit monitoring is just icing on the cake to help me feel like if something does crop up, we'll get it covered."

Why Cyberscout

At Cyberscout, we are committed to protecting the privacy of individuals and businesses and believe that everyone needs to understand cyber risk in order to better fight back against the growing tide of cybercrime.