PROPERTY CASUALTY360

September 1, 2017

Using smart technology to combat insurance fraud

By: Hannah Smith

Insurance fraud has been an issue since the inception of insurance policies in the 18th century. It involves any act committed with the intent to obtain a fraudulent outcome from an insurance process.

Fraud can occur when a claimant tries to gain a benefit to which they are not entitled, or when an insurer knowingly denies a benefit that is due. Fraud by insurers and insureds is actionable in court. According to the Coalition Against Insurance Fraud, up to $96 billion is stolen each year through insurance fraud schemes, a number which could be much higher since no one knows how many fraud schemes are successfully executed without raising suspicion.

New ways to cheat

As fraudsters develop new creative ways to cheat insurers out of claims payouts, insurers have to re-evaluate their detection methods to decrease the payouts for false claims. Countless fraud attempts have been foiled by technology through security camera footage, personal social media sites, location applications, posted pictures, and YouTube videos. Since most adults use social media today, they often leave a trail of public information including what they think and say, what they have done, and who they are associating with, which allows insurance companies to uncover discrepancies between the public story and the one told when a claim was filed.

Through the Internet of Things (IoT) millions of data points are being collected on a daily basis from devices ranging from fitness trackers to pacemakers, to home security, video doorbells, climate control systems, and even some appliances. Many everyday wearable objects track steps, breathing, distance traveled, calories burned, heart rate and diabetes risk, and sun exposure; by no means an exhaustive list.

Smart home devices can allow the user to remotely open and close garage doors, adjust the thermostat, lock and unlock doors and windows, and monitor and interact with the refrigerator. This past year an increasing number of smart devices yielded some interesting information to uncover fraud.

Technology sleuths

Recently, an Ohio court determined that data gleaned from a pacemaker was admissible in what is believed to be the first case using data from a beating heart as evidence in an insurance fraud case. The fraudster stated that he was asleep when a fire started and he awoke to his home ablaze. He proceeded to pack some belongings in a suitcase and broke a window with a walking stick in order to throw the belongings out and escape through the window.

> ***"When he was using the wood burners, he was always very careful. He could smell the smoke, and he would get up and take care of it, so he was extremely wary of any kind of smoke in that house," older brother Phil O'Dell said.***
>
> Coalition Against Insurance Fraud

Several reasons to suspect arson arose, and the police obtained a search warrant for the data from the cardiac pacing device. The cardiologist who reviewed the data deemed it "highly improbable" that the defendant could have collected, packed, and removed the number of items from the house, exited the bedroom window, and carried all of the objects to his car during the short period of time that his heart rate was recorded as elevated. The court determined that the pacemaker data was similar to a blood sample, and was no more private or unconstitutional than medical records, which police can obtain for use as evidence in criminal cases.

A woman in Pennsylvania claimed she had been awoken and assaulted by an intruder. However, criminal charges were filed against her when her fitness tracker, among other evidence, showed she had not slept at all that night and she could not have been awakened by an intruder.