PROPERTY CASUALTY 360°

September 9, 2016

4 ways technology is disrupting fraud

By: Dennis Jay, Coalition Against Insurance Fraud

America is morphing into a vast neural network of high-IQ sensors.

Connected, smart and processing cavalcades of storable data are being transmitted every minute of every day — and it's only just beginning.

The Internet of Things (IoT) is poised to take anti-fraud decision-making to the next level. The industry is on the verge of a grand explosion comprising smart vehicles, homes, clothing, devices and businesses.

Some 6.4 billion connected things are in use worldwide according to information technology research firm Gartner. That's up 30 percent from 2015, and the number is expected to reach 20.8 billion by 2020. In addition, 5.5 million new things will be connected every day this year.

Fresh troves of data, amped-up intelligence

IoT connectivity is breeding fresh troves of granular data and documentation. Amped-up intelligence will help insurers improve claims and anti-fraud decisions, upgrade the customer experience and downgrade scammer capabilities.

Suspect claims can be investigated with more data-driven confidence, and legitimate claims can be paid more-promptly, avoiding costly investigations and lawsuits. IoT data can also provide convincing evidence at trial.

Deterrence is important too. Many workers who wear sensor-embedded clothing on jobsites, for instance, may think twice before filing a false injury claim.

New generations of fraud

New generations of fraud and fraudsters may also emerge. Skilled digital natives will relentlessly probe sensor-driven devices and networks for soft spots to purloin insurance money. They may try to hack, manipulate and even invent data to disguise scams.

4 disruptive technologies

The good news is there are new technologies that will assist in the fraud battle, making it harder for fraudsters to fake information for claims and lawsuits. Several of these include:

1. Telematics. Vehicles are becoming packed with internet-enabled sensors that can speed rich troves of data to investigators. Some 250 million vehicles will have wireless network connections by 2020. Self-driving vehicles will be part of the mix. Telematics can quickly determine things such as G force, crash location, date and time, speed and direction.

> *Smartwatches, fitness trackers, augmented and virtual-reality headsets such as Google Glass, and wearable cameras such as GoPro are among the consumer devices consumers are snatching up and using in large numbers.*
>
> Coalition Against Insurance Fraud

In an incident where a car passenger asserts that a crash inflicted painful whiplash, he may insist on lengthy regimens of costly chiropractic treatment, MRIs and other insurer-paid expenses. Granular data can help insurers calculate the likelihood of a whiplash-caliber incident and whether to pay the claim.

Maybe a driver says someone damaged her parked car with a hit-and-run late one night. Vehicle sensors can determine the vehicle was being driven instead of parked — and in a different county. Sensors might also show that an uninsured $7,000 sideswipe happened two weeks ago — after the prior policy expired and before the driver bought a new one.

2. Wearables. Sensor-embedded clothing and self-tracking devices such as the Fitbit or Apple Watch can help reveal the truth behind injury claims. These devices are in their infancy as anti-fraud tools, although they offer great potential. In the future, 63 percent of insurers say wearables will have a high or very high impact on their organizations.

Smart workplace clothing can help track an employee's whereabouts and activities throughout the day. Sensors can prove whether an employee was at the loading dock when he claimed he

View the entire article. View other articles quoting the Coalition Against Insurance Fraud.

injured his lower back.

AIG is investing in a wearables firm that embeds trackable devices in construction workers' vests. The sensors monitor employee movements in factories, on construction sites and other high-risk workplaces. Data can transmit in real time.

Investigative uses

Smart consumer wearables are taking off and the data could unearth scams. Smartwatches, fitness trackers, augmented and virtual-reality headsets such as Google Glass, and wearable cameras such as GoPro are among the consumer devices consumers are snatching up and using in large numbers.

Imagine a claimant who says she tripped on the crack in a neighborhood sidewalk, resulting in a painful back injury. She sues for $450,000, yet discovery shows she wears a Fitbit wristband, smart watch, heart-rate monitor or other personal tracking device. Her data might track strenuous activity — maybe jogging, tennis or gym workouts. She'll have a hard time asserting she's nearly crippled.

Similar scenarios could occur with workers' compensation injury claims such as a purported crash victim who makes inflated claims for chiropractic treatment until his fitness device shows he lifts weights at the fitness center each morning.

Consider a homeowner who says he wasn't near his home during a suspicious fire, but his smartwatch geo-locator places him in the neighborhood when the fire breaks out. In one case, a Canadian attorney is using Fitbit personal-training data to try and prove his client *didn't* fleece an insurer.

The market for wearable devices is projected to triple to more than $25 billion in the next five years. That's up from 84 million units in 2015, and expected to spike to 245 million units in 2019.

3. Drones. These airborne eyeballs can unearth clues after storms or other natural catastrophes. They can also verify workers' compensation and disability claims.

Commercial sales are projected to reach 2.7 million units in 2020. It is the most dynamic aviation growth sector, and insurance will be one of the largest markets.

A drone can gather important ground-level data immediately after a weather event, and forward it for real-time analysis. Drones can provide high resolution, close-up views of roofs, siding, windows, gutters and other components, providing answers to questions like: How damaged was a claimant's house after a hailstorm, and was any damage preexisting? Did the damage happen at all? Drones can also be especially helpful to short-staffed insurers after major storms.

Data captured during or after a suspected home arson can help investigate why the blaze spread. Was it wind and ventilation or fuel? Was there an outside catalyst such as a fraudster with gasoline?

The FAA has been approving insurer applications for drone use for some time and these airborne tattlers are poised for expansive use in claims, risk assessment and anti-fraud work.

4. Dashcams. These onboard digital eyes are popular in Russia, and many people there consider it a blood sport to leap onto hoods of moving vehicles for false injury claims.

Dashcams are slowing gaining acceptance in the U.S. private-passenger market. They have great potential to head off setup crash injuries and expensive bad-faith lawsuits because insurers can gain an objective car's-eye view of road activity.

Byron Fulghum was involved in multiple crashes in North Carolina. His dashcam video allegedly shows him appearing to set up crashes. Another allegedly shows Fulghum intentionally veering into an elderly woman's car and making her vehicle flip.

Video evidence can unearth staged crashes on roads and in parking lots. The same is true with Russian-style pedestrians who barge onto hoods. From a deterrence standpoint, drivers may think twice if they know their dashcam may capture their antics.

Usage and anti-fraud impact should increase as prices for the dashcams drop, drivers get excited about using them, and if insurers offer premium discounts.

3 management challenges

Despite these technological advances, there are several factors that make them targets for hackers or create issues that require careful consideration.

1. Privacy. A world with billions of sensors tracking our daily lives inspires vigorous debates about claimant privacy boundaries. Courts already allow fraud fighters wide access to a claimant's social-media accounts. A supposedly injured worker's Facebook photos of his marathon or karate workouts are fair game for investigators.

What about Fitbit data or other personal-tracking wearables? Are there HIPAA barriers to obtaining medical data from such devices? What privacy limits will drones generate?

Managing public perception of insurers as Orwellian invaders of people's lives will be equally important. In fact, 82 percent of American adults are concerned about how wearables will invade their privacy. Expect new laws, regulations and court decisions along with vigorous ethics debates.

View the entire article. View other articles quoting the Coalition Against Insurance Fraud.

2. Security. Databases full of private information will be tempting targets for hackers. Securing information is a major challenge of an insurer's connected world. Compiling data is one thing; keeping it safe is another. Some tech-skilled insureds might try to alter claims data by hacking their own or others' devices.

3. Big Data. Insurers that figure out how to seamlessly store, analyze and act on those petabytes will have an advantage over fraudsters. Imagine data several degrees of magnitude larger as digital connectivity increases throughout people and devices. Then again, imagine claims and anti-fraud decisions several degrees of magnitude more-efficient and accurate.

Making sense of the petabyte data gushers of the IoT will be a forward-thinking challenge of the first order for fraud fighters. The secret sauce? Enterprise. Anti-fraud efforts should seamlessly sync with an enterprise-wide commitment to the people, technology and prodigious data required to make the fast-emerging IoT era a digital frontier of boundless complexity and opportunity.

View the entire article. View other articles quoting the Coalition Against Insurance Fraud.