WHITE PAPER

The Evolution of Fraud in the Insurance Industry

iovation®

Introduction

The insurance industry is certainly no stranger to online fraud, whether it's being directed at insurers or the consumers they serve. Sadly, it has become a significant problem for a variety of businesses across the insurance landscape. The Coalition Against Insurance Fraud, for example, indicates that $80 billion worth of insurance fraud occurs in the U.S. every year. But this is hardly a firm figure, given the often intangible nature of insurance fraud, and doesn't precisely identify the operational costs incurred.

With many forms of insurance going unchecked, an educated guess as to how much fraud loss insurers are dealing with – both in the U.S. and abroad – is often the only viable estimate. The Association of British Insurers (ABI), for example, estimates that insurance companies in the UK lost £3bn in 2015 and spent £200m on fraud prevention. Other business costs resulting from fraud include retailer fees, benefit and health service costs, and legal costs. Ultimately, all are paid for by policyholders and taxpayers.

Regardless of how you slice up the data, it's crystal clear that fraudsters are having a significant negative impact on the insurance industry.

The Challenge of Profiling Fraudsters

Adding even more blurriness to the insurance fraud picture is the constantly changing face of a typical fraudster. In other words, there is no easy way to define one. However, fraudulent acts typically fall into one of three categories:

- **Organized criminal activity** – "Crash-for-cash" staged accidents
- **Opportunistic, but pre-mediated** – Buying a travel insurance policy after an accident abroad
- **Opportunistic "spur of the moment"** – Inflation of a claim value on a home policy

While a certain amount of "grey area" exists when one takes into account simple error and misunderstanding, the key differentiating factor is "intent." In the end, the traditional perception of a fraudster is one who has intent to commit fraud.

Emerging Fraud Trends in 2016

While the extent fraud losses in the insurance industry remain somewhat murky, the fraud trends insurance companies are facing are becoming quite clear. Fortunately, as is the case with all industries, instituting comprehensive protection from evolving fraud threats begins with awareness of the tactics fraudsters are using to cheat the system.

The following identifies some of the key trends that are in motion for the insurance industry in 2016, which are already having a significant impact on the way insurance companies interact with customers online and implement security measures to combat fraudsters.

Rising Consumer Demand for an Omni-Channel Experience

As consumers increasingly engage and interact with insurance companies and their partners via multiple channels, digital or otherwise, creating seamless experiences for the consumer across all channels is now critical for success. Since the bulk of premium revenue is now being generated digitally, businesses that pursue an omni-channel approach will significantly outperform slower adopters.

Still, while using an omni-channel approach allows insurers to build a 360-degree view of their customers, integrating the various channels customers use in a seamless manner can be a daunting challenge. This approach also gives fraudsters more channels to prey upon. For many insurance businesses, these channels may not be properly set up to detect emerging fraud patterns.

With this in mind, the need for insurance companies to develop tools and equip employees to support an omni-channel approach is of the utmost importance – not only for improving the overall customer experience, but also for identifying fraud when it happens, regardless of the channel.

Brick & Mortar Locations Continue to Evaporate

As consumers use more types of mobile and other Internet-enabled devices to make purchases and conduct personal business, shopping for insurance is now easier than ever. However, this introduces additional risks for the businesses they engage, largely by opening up new opportunities for fraudsters to misrepresent information or act on behalf of legitimate customers without their knowledge.

As a result, the ability to identify both good and bad users online has become a necessity for insurance businesses, and the strategies and tools they put in place will have a tremendous impact on not only the customer experience, but also the bottom line.

Consumers Rapidly Migrating to Mobile

As insurance businesses shift their focus away from physical locations, they're concentrating heavily on providing customers with access to key services via mobile apps. Insurance mobile apps today allow consumers to:

- View policy details and download policy documents
- Review coverage and discounts
- Make mid-term adjustments changing the risk profile of the policy
- Pay premiums
- View past statements
- Renew policies

According to iovation data, use of mobile apps has more than doubled since 2014 across ALL subscriber sites. Additional data points also show:

- One third of all digital consumption is mobile
- A 42% growth rate for mobile use is forecast for the next couple of years, according to Gartner*

Naturally, this provides an immense opportunity for fraud that requires close monitoring, as fraudsters migrate to the newest areas of an insurance business. As a result, this is sparking higher review rates, which can lead to a more cumbersome experience for the consumer. This is one of the most significant challenges for the insurance industry. That is, striking a balance between providing security for the business, while offering a frictionless experience for consumers.

Insurance Aggregators Rising in Popularity

The proliferation of insurance aggregators is perhaps one of the biggest trends in the industry, which arose in response to the growing volume of business and expanding broker channels. With aggregator sites – such as InsuranceQuotes.com, InsuranceOnline.com and GoCompare.com – consumers can submit their information (or application) just once and receive quotes from numerous providers. This saves consumers time and money, and the experience is often far more efficient than submitting multiple applications via traditional insurer sites.

The U.S. insurance market is seeing a marked increase in the use of aggregators, which continue to gain momentum as consumers become more comfortable with them. In the UK, however, more than 80% of customer quotes/leads originate from aggregator sites today, up from 60-70% just a few years ago.

Still, the rise of aggregators introduces new challenges:

- Insurers have less data visibility and direct contact with the customers
- Higher rates of quote manipulation can be expected as consumers may manipulate information to obtain a better quote, such as a false address and number of claimants. Applicants are able to request 100-200 quotes in a short amount of time with slight changes, such as where a vehicle is kept for an automobile policy.
- Fraudsters can operate from any region, and can easily change their tactics to evade detection if no verification is in place.

Proliferation of Ghost Brokers

Ghost brokers, also referred to as “street” brokers, falsely represent themselves as an employee of an insurance company who has special access to consumer discounts, and often advertise on trusted sites such Craigslist and Gumtree.

Acting as self-appointed intermediaries between insurers and consumers, ghost brokers will often use bots to find the ‘right answers’ to insurers’ application questions (by filing 100-200 applications, all with slightly modified answers). Of the results, the ghost brokers will serve up the lowest priced policy to the consumer, charge them for the policy, deliver the consumers legitimate policy documents, and then -without the consumer’s knowledge- cancel the policy and pocket the refund!

These brokers are not authorized or appointed by an insurance company, but may use a carrier’s direct web portal to secure a new policy on behalf of a consumer. In many cases, ghost brokers charge consumers an excessive fee and may not even provide them with a legitimate policy.

Device Intelligence and the Future of Fraud Defense

As these trends – and many others – play themselves out in 2016 and beyond, insurance businesses will need to take deliberate steps to craft and implement a comprehensive customer authentication and fraud prevention strategy that enables the business to combat new forms of fraud AND meet increasing consumer expectations for convenience and ease of use.

This is precisely why iovation spotlights each device and its unique network of relationships to ascertain if the device is authorized to access an account, the location of the device, and if it has a history of risk.

Today, iovation fraud prevention and authentication, powered by its Global Device Intelligence Platform, is enabling insurance businesses to mitigate fraud risk at all stages of the policy lifecycle and prevent loss at key transaction points including:

- **At quote and policy inception** – Before any loss can be incurred
- **At endorsement or MTA** – When a new risk might be introduced
- **At a claim** – As an extra layer of identity verification
- **During renewal** – To minimize future exposure

Both insurers and aggregators are using iovation to prevent fraudulent applications from entering into their review queues, effectively shutting them out at the front door. As more and more insurance organizations contribute data about known-bad devices to iovation's Device Intelligence Platform, the new shared information benefits them all.

To see iovation's Customer Authentication and Fraud Prevention services in action, schedule a demo at info@iovation.com or visit www.iovation.com.

ABOUT IOVATION

iovation protects online businesses and their end users against fraud and abuse, and identifies trustworthy customers through a combination of advanced device identification, shared device reputation, device-based authentication and real-time risk evaluation. More than 3,500 fraud managers representing global retail, financial services, insurance, social network, gaming and other companies leverage iovation's database of billions of Internet devices and the relationships between them to determine the level of risk associated with online transactions. The company's device reputation database is the world's largest, used to protect 15 million transactions and stop an average of 300,000 fraudulent activities every day. The world's foremost fraud experts share intelligence, cybercrime tips and online fraud prevention techniques in iovation's Fraud Force Community, an exclusive virtual crime-fighting network.
For more information, visit www.iovation.com.

GLOBAL HEADQUARTERS

iovation Inc
111 SW 5th Avenue, Suite 3200
Portland, OR 97204 USA

PH +1 (503) 224-6010
FX +1 (503) 224-1581
EMAIL info@iovation.com

UNITED KINGDOM

PH +44 (0) 800 058 8731
EMAIL uk@iovation.com