Shufti Pro
Identity Verification

Insurance Industry

Customer Verification To Combat Growing Fraud Rate

White Paper

What's Inside

Insurance Sector - Outlook

2020 has been a life-altering year so far and sitting atop the list of reasons is the Covid-19 pandemic. Before coronavirus brought a halt to all plans, the insurance industry was on a good track and was recording considerable growth as well. In 2019, the gross premiums grew 4.4% from the previous year to 3.906 trillion euros[1], driven by a recovery in China and the United States. Life insurance (without health) had a better growth year than property and casualty (P&C), with growth rising to 4.4% from 2.8%in 2018[2]. P&C growth went to 4.3% from 5.4%. The US insurance industry posted an underwriting gain of $5.4 billion in the first half of 2019 and a profitable combined ratio of 97.3 (up from 96.2 in 2018). Globally, Lloyd’s, the world’s biggest insurance market entity, reported a profit of US$2.8 billion during the same period.

Asia’s premium growth (excluding Japan) doubled to 6.8% with total premiums amounting to 947 billion euros. The two big markets of the world, North America and Western Europe recorded a growth of 4.2% and 4.3%, respectively. Whereas in Western Europe in 2019, the United Kingdom, France, Germany, and Italy cornered nearly three-quarters of the premiums of 1.063 trillion euros written in the region.

While in 2020 the global premiums income is seen shrinking by 3.8% and reversing last year’s gains, life insurance premiums could contract by 4.4% and P&C could decline by 2.9%. But according to the global insurance report by Allianz, once the Covid-19 crisis ends and the world recovers in 2021, global premiums growth should settle at 4.4% over the next decade.

[1] Insurance Outlook 2020

[2] Deloitte Insurance Insights

Source: Allianz

The report further states that the growth rate will increase considerably after 2021, and China's premium pool will grow by a whopping 777 billion euros – the market size of the UK, France, Germany, and Italy combined. Growth in Asia will be around 8.1% until 2030.

Growing financial crime

Insurance companies might assume that financial criminals do not have them in their sights, but there is no room for carelessness. They indeed represent a less direct means to legitimize dirty money and to pursue suspicious transactions, unlike banks, which provide an ongoing service, insurers tend to sell products in one-off interactions. However, financial criminals are constantly on the lookout for new opportunities, particularly where they think their endeavors will be less obvious.

A research conducted by PwC suggests that fraud and financial crimes against insurers have been spiking upwards in recent times. PwC in 2018 conducted a Global Economic Crime Survey including over 275 responses from the global insurance community, found that around 62% of global insurers had been exposed to fraud or financial crime.[3]

At the top was consumer fraud with 67% of respondents, however many insurers reported actual exposure to a wide range of financial crime threats as well, which included 46% asset misappropriation, 36% business misconduct, 25% cybercrime, 17% bribery and corruption, 14% accounting fraud, 14% procurement fraud and 9% money laundering.

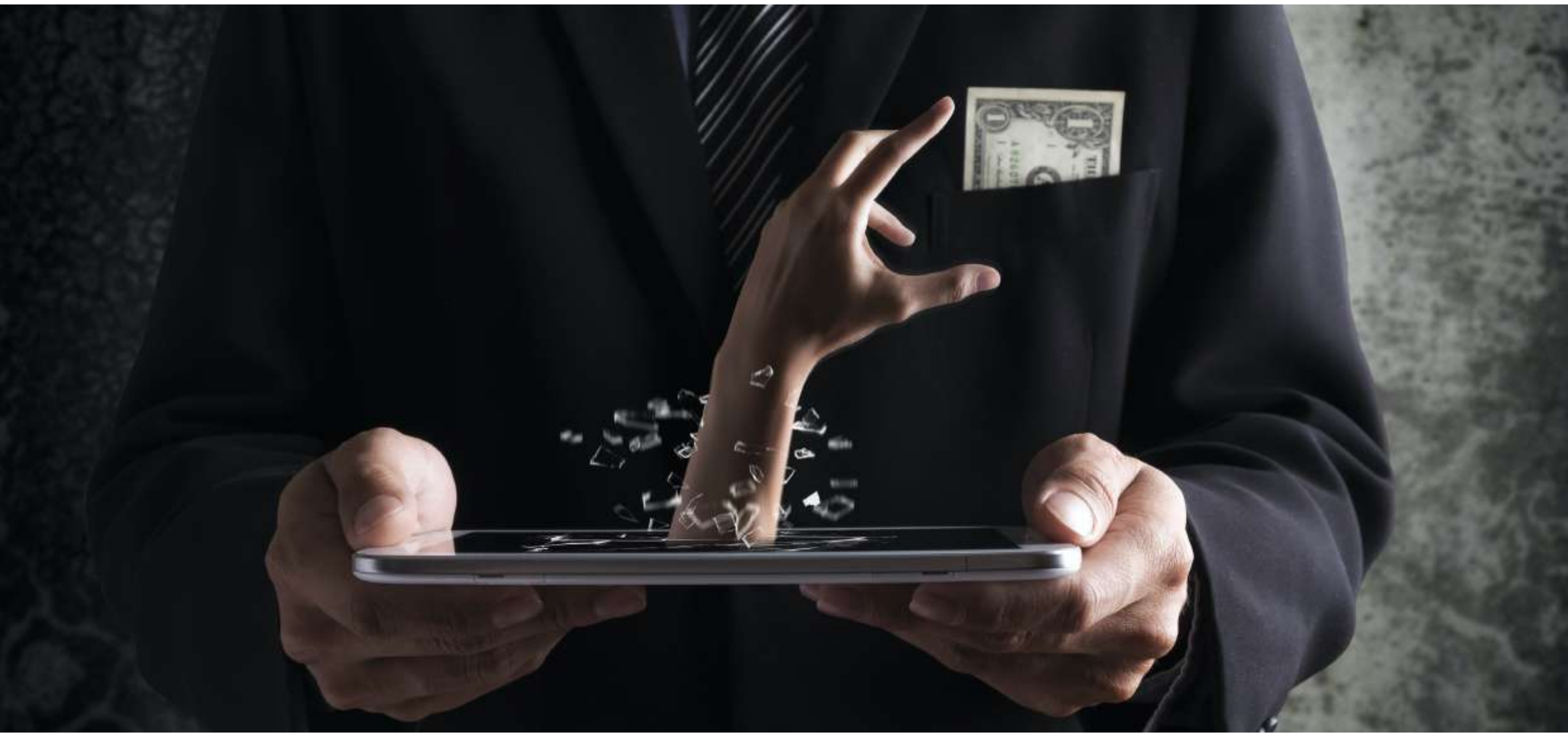
Moreover, as per figures provided by ABI, in 2019 insurers uncovered 130,000 fraudulent claims worth £1.32 billion and estimated that a further £1.3 billion goes undetected.[4]

[3] Financial crime in insurance industry

[4] ABI.org.uk

Hence, preventing financial crime in insurance remains an industry strategic priority. The Financial action task force (FATF) has also warned that certain insurance products are getting increasingly attractive to criminals.[5] It stated that two-thirds of insurance sector cases worldwide relate to life insurance and the general insurance still poses a higher risk as well. The insurance brokers, often unaware of the risks, are becoming an easy target for financial crimes.

Considering these growing financial risk factors the insurance companies that do not take due diligence and anti-money laundering (AML) regulations seriously are putting themselves at substantial risk. They can suffer serious reputational damage when a problem comes to light, furthermore, they are also increasingly at risk of regulatory sanctions, with authorities in many jurisdictions now taking much more aggressive and wide-ranging action on money laundering and corruption.



[5] FATF - Risk-based Approach Guidance for the Life Insurance Sector

Frauds and Threats in the Insurance Sector

According to the FBI, the insurance industry consists of more than 7,000 companies that collect over $1 trillion in premiums each year.[6] This massive size of the industry contributes significantly to the cost of insurance fraud by providing more opportunities and bigger incentives for committing illegal activities.

Application fraud

One of the biggest frauds that the insurance industry faces is application fraud, also known as new account fraud (NAF), which leads to billions of dollars in losses every year. Criminals use two main techniques to initiate false insurance policies online. They either take over existing identities or create fake ones forged from stolen personal information. These fake or forged identities are used by criminals to execute an array of frauds.

Worryingly, application fraud is only the beginning. Once fraudsters successfully manage to create an account and get past the entry checks, false claims, diverted payments, and other forms of fraud quickly follow, often going undetected for weeks. Furthermore, the companies have to face non-compliance penalties as well for not performing identity checks effectively.

[6] FATF - Risk-based Approach Guidance for the Life Insurance Sector

Ghost brokers

Ghost brokers are scammers who sell fake and forged car insurance policies to motorists. These insurance fraudsters typically pretend to be a genuine car insurance broker, acting as the negotiating point between a driver and insurance companies.[7] There are several ways a ghost broker can target an unsuspecting motorist for instance, they might forge entire insurance documents, or change a driver's details to reduce the price of the policy significantly. Moreover, they could change your occupation, your age, or the length of time you've owned the vehicle. This has an impact on your insurance, and because it's incorrect information, it invalidates your policy.

Another ghost broking tactic is for the so-called broker to set up a genuine policy, only to cancel it later, reclaiming the refund for themselves and leaving the victim completely unaware that they're no longer covered.

Cybercrime risk

Data breaches at insurance companies over the last few years have exposed the personal information of over 100 million people.[8] A major data breach that happened in this industry was in 2015 on Anthem Inc. Hackers broke into health insurer Anthem's servers and accessed 80 million company records.[9] These data breaches can further create a financial risk for the companies, as stolen data can be further used to carry out illicit activities.

[7] Rac.co.uk
[8] Cybersecurity issues in Insurance Industry
[9] Anthem Data breach

False claims fraud

False claims fraud happens when a claimant makes up information or exaggerates it in an attempt to get the money guaranteed by their insurance policy. The scammers may stage accidents, or break-ins in order to claim a large sum of money. This results in an increase in rates, inflated policy prices for your clients and huge taxes.

Health insurance fraud

In this fraud, scammers provide fake or misleading information to a health insurance firm in an attempt to have them pay unauthorized benefits to the policy holder, to some party, or the institution providing services. The fraud can be committed by the insured individual or the provider of health services. Such frauds can lead to hefty losses for the insurance service providers and it further causes an impact on the health insurance advantage for genuine customers.

Cybercriminals use various types of malware to attack insurance companies[10], such as:

- **Ransomware:** Thes attacks block a company's access to its systems and data until a ransom is paid.

[10] Firm Guardian

- **Trojan horse:** Malwares such as Emotet and Trickbot, originally designed to break into banking systems, are now a growing threat to insurance companies.

- **Phishing attacks:** They are used to trick users into disclosing confidential information, typically by clicking a link in an email or by responding to a text or phone call.

Increasing Threat of Money Laundering

Insurance products, particularly life insurance, provide a very attractive and simple means of laundering money for criminals. The Financial Action Task Force (FATF) considers this sector as potentially vulnerable to money laundering because of its size, the easy availability, diversity of its products and the structure of its business.

A few years ago, a global US Customs Service investigation exposed the widespread use of insurance products for laundering by international drug traffickers. The investigation revealed that around $80 million in drug money was laundered through life insurance policies issued[11] in the Isle of Man, a few British islands, Florida, and other locations. The drug traffickers allegedly purchased more than 200 life insurance policies through brokers, naming cartel members, and family members as beneficiaries. Policies were paid for using cheques and wire transfers purchased with drug money.

How it happens?

There are several ways that criminals can use insurance products for money laundering.[12] Some of the red flags which may indicate money laundering includes:

- Paying a massive "top-up" into an existing life insurance policy Making a claim request after a few days of purchasing a general insurance policy

[11] Money laundering & Insurance Industry

[12] World Check

- Making a claim request after a few days of purchasing a general insurance policy.
- To purchase a policy using payments from a third party.
- Payment of premiums into one policy, from different sources.
- Channeling payments via offshore banks.
- The funds coming from another country, particularly high-risk jurisdictions.

KYC and AML Guidelines for Insurance Companies

With the growing threats of financial crime and frauds, the regulatory authorities have placed strict regulations for the insurance sector as well.[13]

Know your customer (KYC)

Customer due diligence/Know your customer is intended to ensure that life insurance companies or intermediaries ascertain the true identity of each customer, beneficial owner, and beneficiary of the policy and assess with an appropriate degree of confidence the types of business and transactions the customer is likely to undertake.

Consistent with applicable law, the life insurance company or intermediary‟s procedures should include procedures to:

- Identify and verify the identity of each customer before or during establishing a business relationship.
- Identify the beneficial owner of the customer, and take reasonable measures to verify the identity of the beneficial owner such that the life insurance company or intermediary is satisfied that it knows who the beneficial owner is.

[13] FATF

- Identify and verify the identity of the beneficiary of the life insurance contract at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy. Normally, and in the absence of indicators of higher risk, the anti-fraud checks regarding the identity of the beneficiary at the time of payout would be adequate.

- Obtain appropriate additional information to understand the customer‟s circumstances and business, including the purpose and the expected nature of the relationship. Relevant Customer Due Diligence information should be periodically updated as part

FATF also allows a life insurance company to rely on intermediaries such as brokers or other third parties to perform some elements of the CDD process, provided that certain measures are in place. These measures are:

- Immediately obtain from the intermediary or other third party the necessary CDD information.

- Satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available upon request without delay.

- Satisfy itself that the intermediary or other third party is regulated and supervised and has measures in place to comply with all the CDD requirements and record-keeping obligations.

- Rely only on those intermediaries or other third parties in countries which apply adequately the FATF standards.

- Recognize that the ultimate responsibility for customer identification and verification remains with the insurance company. However, intermediaries should also be made responsible for the validity of this information.

Anti-money laundering (AML)

The anti-money laundering regulations for this sector are more or less the same, with minor changes depending upon the laws in different regions. If we look at the AML laws in the US, the insurance companies must develop a written, risk-based AML program addressing the covered insurance products, and comply with Bank Secrecy Act/anti-money laundering (BSA/AML) program requirements.[14] At a minimum, the program must consist of the following features:

- A designated compliance officer responsible for effectively implementing the program.

- Ongoing training of appropriate persons, including insurance agents and brokers.

- Policies, procedures and internal controls tailored to the AML risks of the institution.

[14] RSM AML Compliance

- Independent testing to monitor ongoing compliance, including testing for compliance of insurance agents and brokers.

Along with implementing an adequate BSA/AML program, insurance companies are subject to suspicious activity reporting (SAR) requirements. Companies are required to submit a SAR to the Department of Treasury's Financial Crimes Enforcement Network. Insurance companies must obtain relevant customer information from agents, brokers and any other sources to report such transactions.

Areas of concern to review

Insurance companies face the challenge of developing an AML program that incorporates insurance agents and brokers, and effectively covers the risks proportionate to its specific products offered. Any areas of concern can be addressed by conducting the following reviews:

- **Policies and procedures:** Evaluate policies and procedures to determine adequacy given the institutions' risks and current industry regulatory requirements.

- **AML risk assessments:** Assess the inherent and residual AML risks related to products, services, customers and geographic exposure.

- **Independent audits:** They are used to trick users into disclosing confidential information, typically by clicking a link in an email or by responding to a text or phone call.

- **Training:** Review staff training programs to ensure adequate coverage of relevant responsibilities under the program.

- **Risk-based review:** Determine and assess the total effectiveness of AML-related processes and internal controls in relation to the specific products, services, customers, and geographies of the company.

- **Independent/outsourced due diligence and sanctions screening:** Identify beneficial ownership structures, negative news, and sanctions screening for customers, vendors and transaction parties.

Digital KYC to Ensure Fraud Prevention

Advanced digital KYC solutions just like Shufti Pro, conduct verifications of individuals effectively in seconds helping organizations to identity fraud entities easily. Powered by advanced technologies like Artificial Intelligence (AI), these solutions flawlessly analyze the identification data of customers, establishing that they are actually who they claim to be. Furthermore, they employ OCR technology embedded in them and can extract relevant information from the government-issued documents and verify identities within a few seconds. They can verify individuals from anywhere in the world.

DID YOU KNOW

Shufti Pro provides a recorded video stream, sequence of images, and 24/7 access to customer data, ensuring that its customers are always in control of the identification services they acquired.

Digital KYC can prove to be a valuable tool for various frauds including application fraud. The process of verifying a person who wants to acquire a policy through digital KYC include:

- Filling out relevant information like name, address, and date of birth, etc.
- After submitting, the customer would be redirected for verification.
- Customers would present proof of identity documents in front of the camera.
- The system checks the documents for signs of tampering or forgery.
- The picture is matched with the face of the person and the data is matched with the provided data that the customer submitted initially.

Furthermore, Digital KYC can also help insurance companies in catering to regulatory compliance needs. By fulfilling the regulations the businesses can secure themselves from penalties and credibility loss that could be huge in some cases.

DID YOU KNOW

Shufti Pro has a massive data bank compiled from 1000 checklists and 3000 databases, enabling organizations to forecast and identify financial risks and frauds. The data bank gets updated every 15 minutes.

Video KYC - Another Approach for Fighting Frauds

Video KYC is another quick and convenient process for verifying individuals in the insurance sector. This method replaces all the traditional verification processes and verifies individuals through video interviews performed by a KYC expert.

The video KYC process undergoes the following steps:

- The customer is asked to fill in the registration form.
- After registration, the KYC expert connects with the customer for live verification.
- Identification is performed via video interview, and real-time presence of customer is ensured through liveness detection.
- KYC expert takes consent from the customer to collect data for identification purposes and to proceed forward.
- The customer is then asked to show (both sides) an ID document.
- The AI-based verification technology verifies the ID document, performs facial recognition, and AML screening.

DID YOU KNOW

Shufti Pro has a massive data bank compiled from 1000 checklists and 3000 databases, enabling organizations to forecast and identify financial risks and frauds. The data bank gets updated every 15 minutes.

Why video KYC is good for insurance businesses

Video KYC ensures regulatory compliance for businesses by keeping a balance between digital security and customer experience. The following are some benefits of video KYC for insurance platforms:

- **Saves time and money:** It's a quick and cost-effective solution for insurance platforms to perform digital identity verification.
- **Improves Digital Security:** Video KYC reduces the risks of fraud and bad actors that use fake identity credentials and documents to get insurance premiums illegally.
- **Complying with KYC requirements:** With live video identification, insurance firms can meet the requirements of regulatory bodies to prevent financial crimes.
- **Enhanced customer experience:** Customers can verify their identities by showing identity documents to the camera and answering a few questions asked by the KYC expert.

- **Instant verification:** The information provided by the users can be verified instantly with document identification and facial recognition.

Conclusion

With frauds, financial crime, and money laundering threats looming around the insurance sector the companies need to perform KYC and AML checks before giving services to any individual or business. It will help them curb the increase of revenue losses and damage to their reputations. Such organizations must adopt enhanced verification solutions like Digital KYC and Video KYC. Being technologically advanced, such solutions can perform verifications quickly and ensure increased security.

Want to integrate Shufti Pro Digital KYC in your system?

Contact Our Experts

Or test our services yourself for 15 days

Get a free trial

www.shuftipro.com

sales@shuftipro.com

Shufti Pro

Shufti Pro True Identity Builds Trust

Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from 3000+ ID templates and business entities from 200 million companies data.