alessa

Build crime prevention into daily operations

Battling Insurance Agent Fraud

Introduction

Insurance fraud is a constant challenge to the industry and can take on many appearances, from fraudulent claims to elaborate scams and conspiracies created by agents themselves or working with complicit policyholders. The fraud can be small, amounting to an individual payment of a few dollars, or it could be a highly planned scheme worth millions.

The exact amount of insurance fraud is unknown globally, but a 2017 global survey by RGA suggests up to four per cent of all claims are fraudulent. The Insurance Information Institute in the United States reports fraud accounts for up to 10 percent of the property/casualty insurance industry's incurred losses and loss adjustment expenses each year, or about $30 billion. The Federal Bureau of Investigation says healthcare fraud, both private and public, is an estimated three to 10 per cent of total healthcare expenditures, or somewhere between $77- and $259-billion.

Case Study: Co-ordinated insurance fraud means big losses

In April 2019, U.S. federal prosecutors charged 24 people in a scheme to defraud Medicare in a $1.2- billion scheme that involved unnecessary prescriptions for medical equipment, kickbacks and bribes in a system that used offshore call centres to upsell unnecessary prescriptions and medical equipment to Medicare recipients.

The accused "concocted an elaborate scheme to exploit the U.S. health care system by targeting Medicare beneficiaries, paying doctors for prescriptions, paying kickbacks and bribes, and in turn selling these prescriptions to DME companies to ensure that they could line their pockets," IRS special agent Matthew Line said at the time.

The fraud saw 24 people charged, including those at the highest levels in five telemedicine companies, including their CEOs, COOs and associates; owners of durable medical equipment companies and three licensed medical professionals.

As part of the complex operation, doctors got kickbacks for prescribing unneeded back, shoulder, wrist and knee braces to elderly and disabled patients and charging the government's Medicare program.

While this example may be among the largest uncovered, many schemes are for hundreds of thousands of dollars. Policyholders who face higher premiums ultimately carry the costs.

Source: Department of Justice.

Agent fraud in insurance

This white paper is to help insurance providers focus on one specific area of fraud that often receives less attention than padded claims or intentional damages on property to collect insurance claims, and that is fraud conducted by agents themselves.

It outlines many different scenarios and gives real life examples of their prevalence in the industry. The fraud could be a rogue agent working alone to swindle clients of additional premiums or defraud the insurance company in other ways, or it could be a conspiracy involving agents, staff and/or clients themselves.

Combatting these schemes will not only see lawbreakers prosecuted, but it could help insurers improve their bottom line and customer confidence, preventing a loss of reputation. In many cases, discovering fraudulent activities will come from increased vigilance, while in others, it may be a simple matter of following your instincts – you could be saving your company thousands in stolen funds and ensuring your customers get the coverage they expect.

Scheme: Misdirecting settlement cheques

Agents can create a misappropriation of funds by misdirecting settlement cheques such as matured endowment or paid-up policies, to the branch officer, to their homes, or to fictitious addresses.

This is done prior to the settlement cheque issue date when the agent may change the company policyholder's address of record to either his address or a fictitious address. Once the cheque is issued, the address is then changed back to the previous address.

Detecting and preventing the scenario

- Build a monitoring report that generates address changes prior to settlement dates. Further investigate if there is a change back to the prior address.
- Further investigate if the address is in a location far from the first original address.
- Request signed documentation of the settlement in order to compare signatures for potential inconsistencies.
- Make verification calls to the policy holders.

Scheme: Pocketing insurance premiums

Case Study: Agent pocketing insurance premiums

A former licensed insurance agency owner faces more than 40 charges for allegedly stealing more than $620,000 in insurance premiums.

Orestes Valentin Rodriguez, owner of Blue Guard Insurance Group Inc., is accused of pocketing insurance premiums from a property management company representing a Miami homeowner's association and never paying the association's insurance.

In all, Rodriguez allegedly stole more than $620,000 in this fraud scheme. His insurance license has been revoked and he has been permanently barred from the insurance business in Florida. If convicted, Rodriguez could face up to 25 years in prison.

Source: Insurance Journal

An agent collects the premium, but does not remit the cheque to the insurance company, leaving the customer with no coverage.

Detecting and preventing the scenario

- Supervisors or a dedicated customer service unit could perform regular calls to verify the reason behind the premium collection. The call might reveal a fraudulent scenario.
- Send automated text messages or emails informing the customer for each amendment performed on the coverage. Ask customers to acknowledge/accept changes and follow-up with any changes that have not been accepted by the customer.
- Educate customers not to sign forms with blank spaces that can be filled in later.

Scheme: Fictitious payees

An agent or clerk can change the beneficiary of record to a fictitious person and subsequently submit the necessary papers to authorize the issuance of the cheque.

Detecting and preventing the scenario

- Build monitoring reports using logical filters that highlight results whenever a change in the customer data occurs around the time of a payment to the person added.
- Send electronic confirmations (SMS, email) to the insured for cheque authorizations.
- Make customer data changes an option available for head office staff only. Agents can request customer data changes only when submitting a form signed by the customer and the agency representative.

Scheme: Deleting policies

An agent might perform a policy deletion in the system without the customer's knowledge, after providing the customer with a printed policy.

Detecting and preventing the scenario

- Build a monitoring report that highlights cancelled policies that occur a short period after the policy is entered into the system.
- For each cancelled policy, perform verification checks with the agent, cross check the agent information with the customer.
- Have in place a cancellation form, detailing the reason for the cancellation, to be signed by the customer and the agent.
- Check all cancelled policies monthly. Group cancellations by agent and look for cancellations that deviate from the normal expected average.

Scheme: Fictitious death

An agent might obtain a fictitious death certificate and request a death claim cheque. The agent receives the cheque and cashes it.

Detecting and preventing the scenario

- Request official signed medical documentation along with the claim request.
- Crosscheck the potentially deceased records with the official data records issued by the authorities to verify the authenticity of the claim.

Case Study: Sell high, buy low insurance plans

Investigators say a licensed Miami insurance agent allegedly obtained and transferred more than 300 homeowner insurance policies without homeowners' knowledge or consent and pocketed nearly $476,000 from the policy premium differences.

According to a statement from Florida Chief Financial Officer Jimmy Patronis, Claudia Odila Romoleroux, owner of RND Insurance Corporation, is accused of fraudulently obtaining more than $877,000 in premiums for 307 homeowner's policies.

She is accused of using a portion of that money to pay for cheaper policies with inadequate coverage. If convicted, Romoleroux faces up to 25 years in prison.

Source: Insurance Journal

Scheme: False information

An agent may submit false information to obtain unlawful financial gain. For example, entering an improper date of birth to obtain a cheaper policy.

Detecting and preventing the scenario

- On new policy applications for existing customers, cross check the data input by the agent with the existing information in the customer's file or with information available through identity verification solutions.

Scheme: Fictitious policies

If a bonus incentive scheme is in place, the agent might try to inflate the number of policies sold by creating fictitious policies to bogus customers.

Detecting and preventing the scenario

- Build monitoring reports, which highlight inflated or unusual fluctuations from the historical activity of the agent.
- Analyse all the policies entered into the system on non-business days.
- Analyse the periods where the unusual fluctuations have occurred by crosschecking the sample with the additional information on the policies to verify the policy's authenticity.
- Perform on site visits to verify the accompanying documentation attached to the policies.
- Check official residential records issued by the state authorities to verify the data accuracy of the policyholders.

Case Study: Selling fake liability insurance policies

Authorities in Iowa recently charged an agent for selling fake liability insurance policies even after she no longer had a business relationship with the insurance company. The scheme was discovered after the policyholder tried to file a claim and found out the policy was fictitious. The agent was permanently banned from selling insurance in the state and could face up to 15 years in prison on charges of charges of fraudulent practice and fraudulent insurance claim submission.

Source: Ottumwa Courier

Scheme: Pocketing premiums

The agent keeps the premium without entering the policy details in the system and providing the customer with a fictitious policy.

Detecting and preventing the scenario

- Check the policies issued by the agents for any gaps in sequential policy numbers.
- Educate the customers about the formal policy details including (Sequential Policy Number, bar code).
- Educate the customers not to accept printed policies with blank sections.

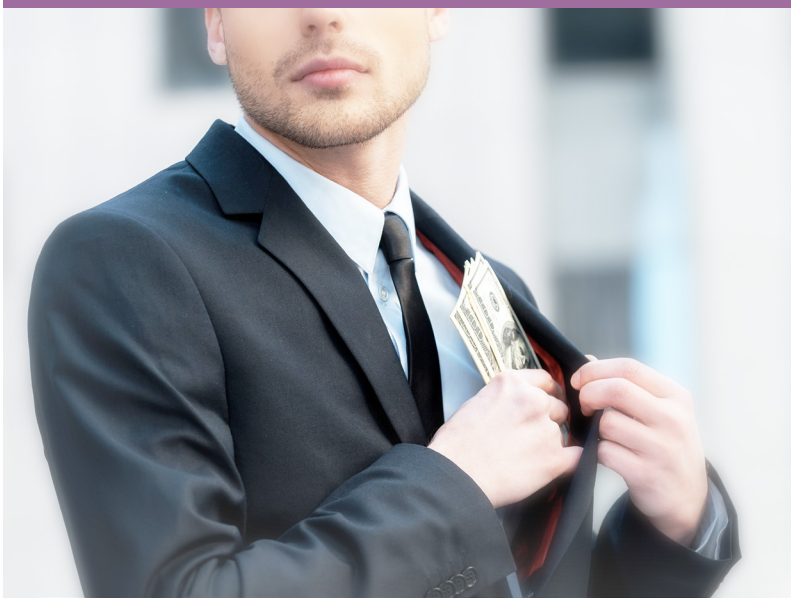
Case Study: Pocketing premiums from fictitious policies

In Fresno, California, unlicensed insurance agent Marlene Pineda, 34, was sentenced to 95 days in jail and five years of probation after pleading no contest to grand theft.

A consumer complaint received by the Investigation Division of the California Department of Insurance alleged Pineda stole $1,107 in insurance premiums from a client.

Investigators discovered that Pineda sold commercial and auto policies to an additional eight consumers, misrepresented their information on insurance applications and misappropriated premium funds for her own use. The total amount stolen from all victims was $28,707.12.

Source: California Department of Insurance



Scheme: Sliding

Sliding is the term used for including additional coverage in the insurance policy without the knowledge of the insured.

Detecting and preventing the scenario

- Use analytic reports to identify when existing insurance coverage is linked to the consumer on the same day as other insurance products.
- Use technology like anomaly detection and AI to find cases where the customer's profile does not fit with the type of the insurance product.
- Check if the time and date marked at the additional insurance coverage is not consistent with the existing insurance.
- For each additional insurance coverage product differing from the existing one, the customer's signature consent should be required.

Scheme: Churning

Dishonest agents might convince people to use the built-up value of their current whole life policy to buy a "better" policy even though their present life coverage is suitable. The agent gets a commission, but the policyholder must start over building up cash value.

Detecting and preventing the scenario

- Require that an agent provide a disclosure statement containing comparisons of the policies so customers can make informed decisions
- Require agent and applicant to sign a form which includes reason for change
- Review monitoring reports for agents/offices with high number of replacement policies

Scheme: Twisting

An agent may urge a client to change policies prematurely by "twisting" the truth about the downside. This could negatively affect a policyholder that has an illness, injury or other medical condition.

Detecting and preventing the scenario

- Require customers to sign off on any policy changes including extra coverage and charges

Scheme: Worthless investments

Customers may be urged to invest in insurance-like instruments such as life policies taken out on sick or terminally ill people. (e.g. Viatical investments or promissory notes.)

Detecting and preventing the scenario

- The investors will require a review of the seller's medical records to ensure the seller truly is a terminal patient. Have doctors review the records and actuarial charts.
- Fraudulent promissory notes are sometimes issued on behalf of fictitious companies; in this regard, documentation should be crosschecked with valid official records.

Case Study: Agents Issue policies to straw buyers

For example, New York officials and the FBI charged three insurance agents with a $100-million fraud scheme involving stranger-owned life insurance or STOLI. With stranger originated life insurance (STOLI) arrangements, a policy is bought with the intent to resell it to a third-party investor – there is no relationship with the people being insured. Many insurance companies will not allow the practice and some states have outlawed it. The agents were charged with conspiring to defraud major insurance companies into issuing life insurance policies to straw buyers, when the true owners of the policies were third-party investors and financiers. The agents received jail terms in 2014 ranging from 6-12 years.

Source: Forbes

Scheme: Internal conspiring

Fraudulent efforts to circumvent internal controls when there is collusion between the agent and other staff. Password sharing and weak IT controls can contribute to this problem.

Detecting and preventing the scenario

- Add another person from another department to authorize the contract or transaction by checking the physical documentation.
- Perform frequent staff rotations of the authorizers.
- Perform regular IT audits for unauthorized access, weak passwords etc.
- Run monitoring reports looking for cases where personal information of payout recipients are the same as agents or employees.

Case Study: Organized scheme to defraud insurance companies

Nine individuals and business owners face charges in a large-scale organized scheme to defraud insurance companies out of more than $600,000 in fraudulent insurance claims.

The joint fraud investigation was initiated after several insurance companies notified authorities of suspected fraudulent residential insurance claims in the South Florida and Tampa areas. Detectives believe that The Rubicon Group, a public adjusting company owned by Barbara Maria Gonzalez, committed organized fraud and grand theft.

Gonzalez allegedly utilized the services of unscrupulous Florida companies to commit the fraud, including water mitigation and restoration companies, insurance agencies and agents, appraisers, and willing homeowners, DFS said. The investigation remains open and ongoing and more arrests are expected, including 26 homeowners who have been identified as participating in the scheme. They will also face conspiracy charges and could face up to 30 years in prison.

Source: Florida Department of Financial Services

Additional measures for preventing agent fraud

Insurance companies want to ensure consumer and shareholder confidence by showing they are aware and actively searching for areas where agents or stakeholders could be conducting fraudulent activities. In addition to the above recommendations, there are a number of additional ways companies can show due diligence:

Case Study: Insurance Commissioner indicted in $2 million scheme for personal gain

Georgia Insurance and Fire Safety Commissioner indicted in $2 million scheme to pay for a rental property, credit card debt and taxes. The U.S. Attorney said Jim Beck is accused of using his experience in the insurance industry to create fake companies to defraud insurance companies of at least $2 million. Beck was indicted for creating shell companies to make fake invoices and redirect money given to him through other companies. The shell companies received money for home inspections and water damage mitigation, which they received from insurance companies using fake invoices.

Source: 11alive.com

Perform effective background checks

Perform background checks on every new agent or affiliate including using:

- **Credit Registry Checks** to identify possible unpaid loans
- **Black/High-Risk Lists Checks** to identify previous false claims and detected fraudulent attempts.
- **Criminal Record Checks** to identify possible risky individuals

Perform periodic onsite agent office visits and verification

- Frequent visits increase the perception of control and awareness of ethical conduct
- Conduct frequent training programs focused on maintaining standards
- Automate online verifications of data and transactions for a risk-based approach

Perform data accuracy verification to identify

- Double data entries or those left blank
- Data which falls outside the usual format for a particular entry (Example: ID – Letter, Number, Number, Number, Number, and Letter)
- Data which does not contain the required number of characters
- Data which follows sequential characters (Example: 123456789)
- Data which follows repeated characters (Example: 111111111)

Conclusion

Insurance agent fraud may be a small part of your insurance company's overall risk – but it is still something that requires your due diligence and an environment that makes it harder for agents to go rogue. Tier1 Financial Solutions offers a solution called Alessa to help screen transactions and ongoing business with agents and other insurance company staff.

Transaction monitoring and screening: Alessa offers the ability to identify potentially fraudulent insurance claims prior to payout. In these cases the claim management system sends the claims transactions to Alessa. Alessa then examines them using its anomaly detection engine and scores the transaction based on its attributes. If the transaction is considered high-risk then a message is returned to the claims management system, the status is updated to "At Investigations" and an alert is sent to the appropriate person(s). If after investigation the decision is made to deny the claim, the platform sends a new message to update the status to "Denied."

Investigation Tools: Alessa offers dynamic workflows to guide processes and investigations. Enterprise search capabilities allow for easy searching of data within internal and external sources, while case management offers a collaborative approach to investigations, compliance, and decision making.

Risk Scoring: Alessa uses data from various sources, including sanctions lists, to provide an assessment of the risks with transactions or of doing business with an individual or business. The solution also periodically reviews an organization's customer base and updates their risk level based on their activity and third-party data.

Configurable: With Alessa, organizations can select the functionality they need or the complete solution. Permission-based functionality allows different users to access only the information they need to perform their responsibilities, and data can be maintained in the cloud or on premise, ensuring compliance with regulations.

Data Management: Alessa accesses data from any platform, including ERPs, bespoke applications, and core business systems. The data is then cleansed and aggregated to increase its accuracy, and cross-referenced to reveal big-picture insights. Better data means better insights.

Metrics & Insights: Alessa offers configurable dashboards that track key metrics and allow compliance staff to drill down into the alerts. Advanced analytics allow for sound decision-making and actions to be taken based on comprehensive information and insights.

To learn more about Alessa can help your organization fight fraud and other forms of financial crimes, visit our website at **www.alessa..com.**

About Alessa

Alessa, by Tier1 Financial Solutions, is a compliance, controls monitoring and fraud prevention solution for banking, insurance, fintech, gaming, manufacturing, retail and more. With deployments around the world, Alessa allows organizations to quickly detect suspicious transactions, identify high-risk customers and vendors and decrease fraud risks that reduces profitability and increases costs. To learn more about how Alessa can help your organization ensure compliance to regulations, detect complex fraud schemes, and prevent waste, abuse and misuse, visit us at https://www.alessa.com/.

150 Isabella Street, Suite 800,
Ottawa, ON K1S 1V7, Canada

1-844-265-2508

alessa@tier1fin.com

www.alessa.com

alessa
by Tier1 Financial Solutions