Preventing employee misconduct in the insurance industry

Saiko Terada

10.Dec.2021

Nomura Research Institute, Ltd.

Executive Summary

Untoward incidents stemming from employee misconduct have been on the rise in recent years in Japan's insurance industry. It is crucial for insurers to detect early indicia of conduct risk in their employees' day-to-day activities and nip the risk in the bud before it manifests.

Saiko Terada

Senior Consultant

Global Financial Solution Business Department

FSA warns on conduct risk

Misconduct by insurance salespersons, ranging from failure to make required disclosures to mega-fraud, has garnered considerable public attention in Japan in recent years. Preventing such misconduct has become an urgent imperative for the insurance industry.

Until recently, the FSA had encouraged financial institutions to address conduct risk as they individually saw fit in light of their size and other attributes. It published case studies of best practices and shortcomings based on its conversations with major financial institutions but did not issue any specific rules or principles regarding the risk of misconduct not explicitly illegal.

However, at a July 2021 meeting between the FSA and the Life Insurance Association of Japan, the FSA brought up recent misconduct incidents and discussed conduct risk as an emerging but hitherto largely neglected risk. It stressed the importance of reducing conduct risk by identifying and responding to its early warning signs and asked the life insurers to do so. The FSA has not made the same request to any other types of financial institutions, suggesting it is most concerned about the insurance industry in particular.

Initiatives to prevent employee misconduct

NOTE

1) Motive, opportunity and justification are the three components of criminologist Donald R. Cressey's Fraud Triangle model, which was referenced in standards for addressing conduct risk in accounting audits published by Japan's FSA in 2013.

Employees putatively commit fraud only if they have a motive, an opportunity and a justification[1]. It is important to target preventive measures at these three elements and to foster a sound corporate culture as the cornerstone of such prevention. The insurance misselling incidents mentioned in the opening paragraph reportedly stemmed from overly ambitious sales targets imposed from above. The incidents' root cause was seemingly the sales targets or a top-down organizational culture

in which the sales force had no say, not a personal profit motive. Based on such a diagnosis, a wide range of companies are now taking action to mitigate conduct risk, including by instituting codes of conduct, raising awareness throughout their workforces, conducting training programs, revising compensation schemes and setting up internal whistleblower channels.

However, fostering a corporate culture takes years and no matter how much effort a company makes, conduct risk is virtually impossible to completely eliminate. It is therefore important for companies to operate under the assumption that misconduct will inevitably occur and have internal controls to nip it in the bud alongside various measures to prevent misconduct outright.

AI-powered early-warning detection tools

The Japanese insurance industry can learn a lot from Western financial institutions that were early adopters of technology to prevent employee misconduct. Western investment banks in particular are at the forefront in terms of technological safeguards against improprieties such as insider trading and conflicts of interest. A case in point is Jefferies Group, a global investment bank that has adopted an early warning detection system to mitigate conduct risk.

The system identifies behavior that fits patterns indicative of misconduct based on data, including text data (e.g., emails, chat transcripts) and voice data from telephone conversations and videoconferences, the latter of which have exploded in popularity amid the pandemic. Upon detecting suspicious conduct, the system automatically generates an alert. It screens for suspicious behavior using AI-augmented time-serial analysis of information such as the following.
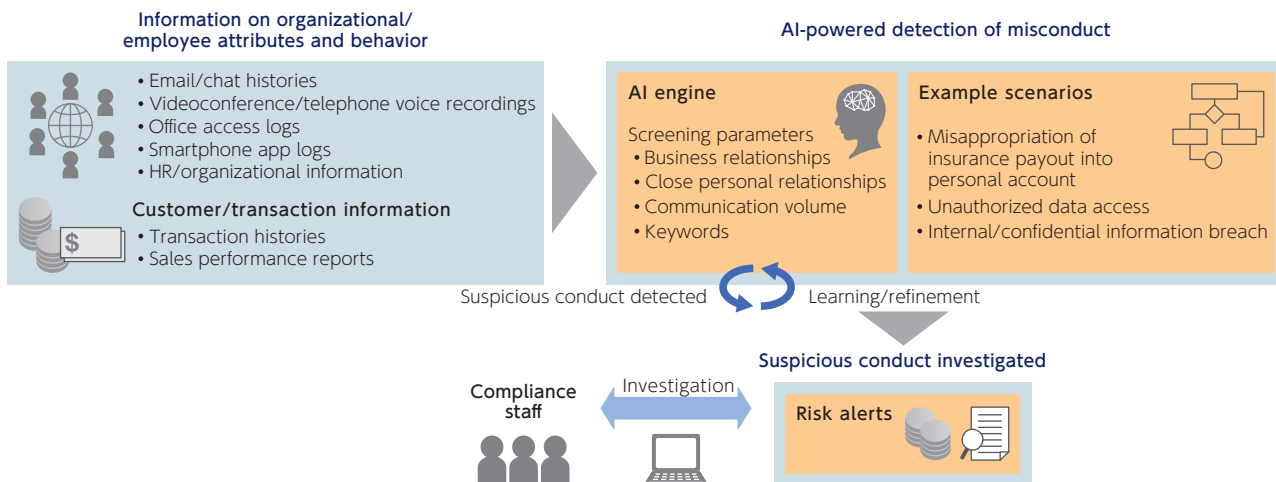
(1) Business relationships

Examples: emails with official/formal subjects and signatures, content of requests in emails, speed of reply

(2) Close personal relationships

Examples: conversations about personal interests, emails without subjects and/or signatures, casual language, timing and frequency of communication, etc.

How a misconduct early-warning detection system works

Information on organizational/employee attributes and behavior

- Email/chat histories
- Videoconference/telephone voice recordings
- Office access logs
- Smartphone app logs
- HR/organizational information

Customer/transaction information
- Transaction histories
- Sales performance reports

AI-powered detection of misconduct

AI engine

Screening parameters
- Business relationships
- Close personal relationships
- Communication volume
- Keywords

Example scenarios
- Misappropriation of insurance payout into personal account
- Unauthorized data access
- Internal/confidential information breach

Suspicious conduct detected   Learning/refinement

Suspicious conduct investigated

Compliance staff   Investigation   **Risk alerts**

(3) Communication volume

Examples: numbers/length of emails, chats, conversations, etc.

(4) Keywords used in communications

Examples: words indicative of divulgence of information, like "confidential" or "secret"

If, for example, the system were to detect a suddenly close relationship between two individuals with no history of prior communication with each other, an exchange of internal information and/or keywords indicative of an information breach, it would issue an alert. The AI can be refined by teaching it terminology and jargon specific to the, e.g., insurance industry. Additionally, the AI automatically improves its accuracy by learning the outcomes of investigations into its previous alerts.

Importance of employee buy-in

To deploy such technology in Japan, companies would have to be careful not to violate employees' privacy. There is a Japanese legal precedent that grants employees a limited right to privacy in the workplace, even with respect to information terminals furnished by their employer for business use[2]. Companies would need to take steps to address privacy concerns in utilizing monitoring technology.

As a first step, it is crucial to fully gain employees' buy-in before deploying the

2) Tokyo District Court decision of December 3, 2001 (*Rodo Jiken Saibanreishu* No. 826, p. 76).

technology. To do so, employers must adequately explain at least their policies with respect to the technology's use, the purpose of deploying the technology and the communication channels to be monitored. They must also make their entire organization aware that they will strictly limit access to employees' correspondence and conversations to authorized personnel and will not permit arbitrary access.

Another idea is to provide positive recognition to employees found to be complying with company regulations and procedures. By factoring such positive feedback into employees' compensation and/or performance evaluations, employers should accrue goodwill from employees for rewarding their previously overlooked day-to-day actions.

If companies fail to gain employees' buy-in, their employees may be inclined to find ways to circumvent monitoring and engage in misconduct. In addition to the steps suggested above, another key to successful adoption of misconduct early-warning detection systems is to make the system about more than just surveillance and detection so that employees personally appreciate its importance and effectiveness.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $4.9 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 13,000 employees.
For more information, visit https://www.nri.com/en