INSIGHT

Building Digital Security for Group Insurers

INTRODUCTION

Today's insurance industry consists of over 7,000 companies that collect more than $1 trillion in premiums each year. Its vast size contributes significantly to the incidence and cost of insurance fraud by providing more opportunities and larger incentives for bad actors to commit illegal activities. According to the FBI, the total cost of insurance fraud (in the non-health insurance sector) is estimated at $40 billion per year, which costs the average U.S. family between $400 and $700 per year in increased premiums.

For the past several years, insurers have been enhancing their digital presence to improve customer experience, increase speed of policy issuance or service, and reduce cost[1]. They accelerated this transition with the onset of the pandemic. The proliferation of digital self-service channels has presented cyber criminals with additional opportunities to commit insurance fraud. Insurers need to closely monitor and improve their online defenses, while evaluating existing solutions to either upgrade or replace them. This includes prioritizing technologies to achieve a delicate balance of comprehensive fraud management and a seamless customer experience for user satisfaction and an enhanced value proposition for all constituents.

THE DIGITAL OPPORTUNITY AND CHALLENGE

Over the past decade, insurance companies have been undergoing substantial digital transformation. Self-service portals for customers and agents, online loan applications, and electronic medical data are now all considered basic offerings. The pandemic rapidly accelerated this transformation with the migration of insurers, agents, and their customers to more digital experiences and remote work. The shift to a larger online presence for customer registration and claims submissions made it easier for criminals to create fake identities and perpetrate crimes. In addition, insurers' failure to prevent, detect, and respond to criminals or fraudulent activities has made this a lucrative activity for criminals. (See Figure 1, Life Insurance Accounts Created or Accessed Without Consent in the Past Two Years). To manage fraud comprehensively, insurers must remain alert to suspicious activity, and diligent in improving current measures by either enhancing existing defenses or developing effective alternatives.

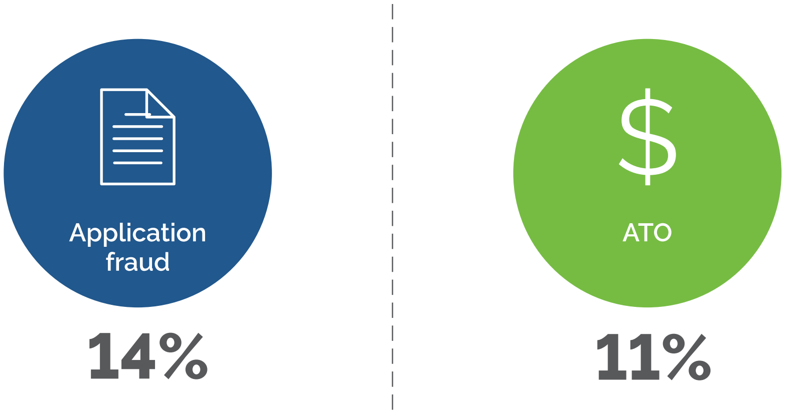
When firms establish a business relationship with a customer, they must also perform due diligence to verify their identity. Basic identifications such as their name, date of birth, and address may have sufficed in the past, but do not in the new expanded digital world.

INSURANCE FRAUD: THE FACTS

Insurance fraud, more specifically identity fraud, affects two separate parties: the victims who suffer financially and emotionally, and the organizations that serve consumers, who also bear the costs of identity theft and fraud.

Identity fraud reached extremely high levels in 2017 with over $17 billion stolen directly from U.S. consumers. The Coalition Against Insurance Fraud estimates that insurance fraud steals at least $80 billion every year from American consumers. The bigger costs, however, are in brand perception, damage to the customer relationship, and loss of productivity.

Figure 1: Life Insurance Accounts Created or Accessed Without Consent in the Past Two Years



ATO – Account takeover fraud
Source: Aite-Novarica Group's online survey of 8,653 U.S. consumers, December 2020

Insurance companies face additional complexities: insurers or brokers will need to identify the 'beneficial owner' who is acting on behalf of other people, businesses, partnerships, or trusts. Insurers can minimize the risk of insurance fraud only by establishing that they are transacting with the ultimate beneficial owner. Third-party service provider screening needs the same level of assurance and insight.

EFFECTIVE PREVENTION

Today's organizations are challenged to implement effective identity verification (IDV) without detracting from the customer experience. The National Institute of Standards and Technology (NIST) has provided guidelines in managing three levels of digital identity to prevent fraud:

- Level 1 (IAL1): There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the subject's activities are self-asserted or should be treated as self-asserted including attributes Credential Service Providers (CSPs) assert to a Relying Party (RP). Self-asserted attributes are neither validated nor verified.

- Level 2 (IAL2): Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically present identity proofing. Attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes. A CSP that supports IAL2 can support IAL1 transactions if the user consents.

- Level 3 (IAL3): Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained CSP representative. As with IAL2, attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes. A CSP that supports IAL3 can support IAL1 and IAL2 identity attributes if the user consents.

A suitable standard from the three NIST levels needs to be adopted based on the risk to the account. Security in layers using multiple factors (what you know, i.e., username and password; what you have, i.e., a token or authenticator app; and what you are, i.e., biometrics), device and location verification, and voice and keyboard analytics are some of the authentication technologies that insurers must deploy. It is imperative to establish a dynamic digital identity protocol with four key capabilities – an identity-based representation, secure resource access, continuous trust evaluation, and adaptive access control – for airtight security and to enable group insurer constituents' peace of mind.

CONCLUSION

As insurers continue their digital transformation to provide enhanced customer self-service, they have presented cyber criminals with expanded opportunities to commit insurance fraud. A seamless digital experience for all users is the goal of today's insurers, while recognizing the need for a system whose defenses will continually outpace bad actors. Impenetrable anti-fraud security measures are a must to ensure the security of all data and transactions, provide customer confidence, and protect company assets. With the help of NIST guidelines, companies can reduce the increased risk of insurance fraud, while providing the effortless digital experience today's customers demand.

ABOUT VITECH

Vitech is a global provider of cloud-native benefit and investment administration software. We help our Insurance, Retirement, and Investment clients expand their offerings and capabilities, streamline their operations, gain analytical insights, and transform their engagement models. Vitech employs over 1,600 professionals, serving the world's most successful insurance, retirement, and investment organizations. An innovator and visionary, Vitech's market leadership has been recognized by industry experts, such as Gartner, Celent, Aite-Novarica, and ISG. For more information, please visit vitechinc.com.

[1] "Insurance Fraud: Rethinking Approaches in the Digital Age," Aite-Novarica, September 2021, pg. 5