Aite PARTNER. ADVISOR. CATALYST.

Beat Life Insurance Fraud With Identity Verification and Authentication

This report provided compliments of:

JUNE 2021

Manoj Upreti

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACT POINTS

- This report examines the current practices and opportunities in identity verification, authentication, and fraud management in the life insurance industry. It is based on Aite Group's domain expertise and knowledge base, secondary research, briefings with industry players, a quantitative consumer survey in December 2020, and interviews with more than 20 experts at life insurance carriers and fraud-related industry organizations.
- Increased digital activities and the recent economic environment have increased the motivation, opportunities, and rationalization for fraud, mainly during onboarding and authentication. However, life insurers are behind other industries in managing fraud effectively.
- Both identity theft and account takeover (ATO) have increased, and customers are experiencing the impacts. An Aite Group survey in 2020 found that 14% of life insurance policy owners experienced identity fraud and 11% faced ATO.
- Fraud applies to many stages of the insurance value chain, and insurers need an omnichannel approach to detect, review, and prevent fraud in customer acquisition, underwriting, customer services, disbursements, and claims.
- High-maturity organizations are taking actions that include (a) strategic elements, such as multiyear roadmaps, centralized coordination, sharing and learning, and executive involvement; (b) process focus, such as fraud risk assessment, case management, and layered security; and (c) technology enablement via identity management, multifactor authentication, analytics, and enterprise orchestration.
- To maintain long-term strategic focus while keeping organization buy-in, insurers should take a multiyear, centralized approach to planning and execution, shift the narrative to building a better customer and agent experience, and reduce costs through commercially available technology solutions that can be scaled.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INTRODUCTION

The two most important tasks in managing fraud are to establish a person's identity and to have strong authentication in place. According to Aite Group estimates,[1] U.S. firms' losses due to identity theft increased in 2020 to US$712 million from US$502 million in 2019. That is about a 42% increase in just one year, primarily driven by unemployment-benefits-related identity theft during the pandemic.

In the past few years, the life insurance industry has been undergoing significant digital transformation. Online customer applications, electronic medical data for underwriting, and portals for customers and agents are now all considered table stakes. While technology has made it easier to do business, it has also created new opportunities for fraudsters. Data from insurers and consumers shows that the current business environment has led to increased vulnerability and fraud incidents. The industry must improve fraud management practices because fraudsters are constantly improving their methods and finding sophisticated ways to commit fraud. At the same time, insurers' onboarding and customer service experiences should be as frictionless as possible.

Historically, identity verification and authentication has been somewhat neglected in life insurance, and the practices are not as mature as in other financial sectors such as banking. However, insurers are now realizing that they need a long-term strategic viewpoint combined with the use of robust technologies to be prepared for a digital future.

This report examines the needs for identity verification, authentication, and fraud management in various parts of the life insurance value chain. It then explores practices and capabilities used by high-maturity insurance carriers, their level of adoption, and their impact on the success of fraud management. Finally, the report examines key considerations in selecting technology for identity management.

Life insurance executives and leaders in fraud management, risk, security, operations, technology, legal, and compliance functions can use this report as a starting point to brainstorm ideas and develop their fraud management strategy and action plans.

METHODOLOGY

This report is based on Aite Group's domain expertise and knowledge base, secondary research, briefings with industry players, a quantitative consumer survey in December 2020, and interviews with more than 20 experts at life insurance carriers and fraud-related industry organizations.

1. See Aite Group's report *U.S. Identity Theft: The Stark Reality*, March 2021.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

THE MARKET

The life insurance industry is going through a significant amount of digitalization, automation, and data transformation. These factors are changing the way agents and customers interact with the insurers and have created a need for superior customer experience as well as opportunities for fraud. The insurance companies are under pressure to balance fraud prevention with customer friction in their operating environment. Table A summarizes current market trends that are shaping the need for identity verification, authentication, and fraud management for life insurers.

Table A: The Market

Market trends	Market implications
Increased self-service onboarding	Although approximately 90% of life insurance policies are still sold by agents, the application and onboarding process is significantly digitalized. In many cases, agents initiate the buying process and customers might provide additional information or complete the second part of the application independently. In the drop-ticket process, agents only initiate the buying process, and the customer is approached later by a fulfillment center to complete the onboarding process. Such process adoptions have increased the need for identity verification when customers access the online application or call fulfillment centers.
Accelerated life insurance underwriting	Many insurers have increased their accelerated underwriting limit to US$3 million, up from US$1 million, due to difficulty in obtaining lab tests during the pandemic. Customer identity verification has become very important in ensuring the right alternative requirements, such as digital health data, to underwrite accelerated cases.
Carriers paying attention to customer experience and friction reduction	Life insurers are shifting the narrative to improving the customer and agent experience while managing fraud. That is helping prioritize technologies to balance fraud management while providing a frictionless customer experience. Layers of security, voice analytics, device verification, and data diversity available for authentication are some of the improvements many insurers are targeting to deploy.
Consumers' personally identifiable information exposure to high-data breaches in recent years	Organized fraud rings gather data on consumers in databases and strike many individuals when they have aggregated enough information to successfully impersonate consumers to take over existing accounts.
Infrastructure gaps to reliably authenticate customers	While banking and other financial institutions have adopted more strict authentication techniques, life insurance companies are behind in adopting new methods and technologies. This poses a significant financial risk to cash value accounts, annuities, and 401(k) accounts held by many life insurance companies.

Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

NEED FOR BETTER IDENTITY VERIFICATION AND FRAUD MANAGEMENT

The recent socio-economic environment has influenced all three components of the fraud triangle:[2] motivation, opportunity, and rationalization. Financial distress and unemployment have increased the motivation, the digital economy is providing higher opportunities and means than ever before, and difficult financial and health-related conditions help rationalize fraud-related actions.

Consumer studies often show the high incidence rate of identity theft and ATO in life insurance. In December 2020, Aite Group conducted an online quantitative survey of 8,653 U.S. consumers aged 18 and older. The responses were click-balanced to the U.S. census for age, gender, income, and region. Fourteen percent of the participants said that their personal information was used to buy life insurance or annuity without their consent within last two years. Eleven percent said that their account was accessed without their consent (Figure 1).

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

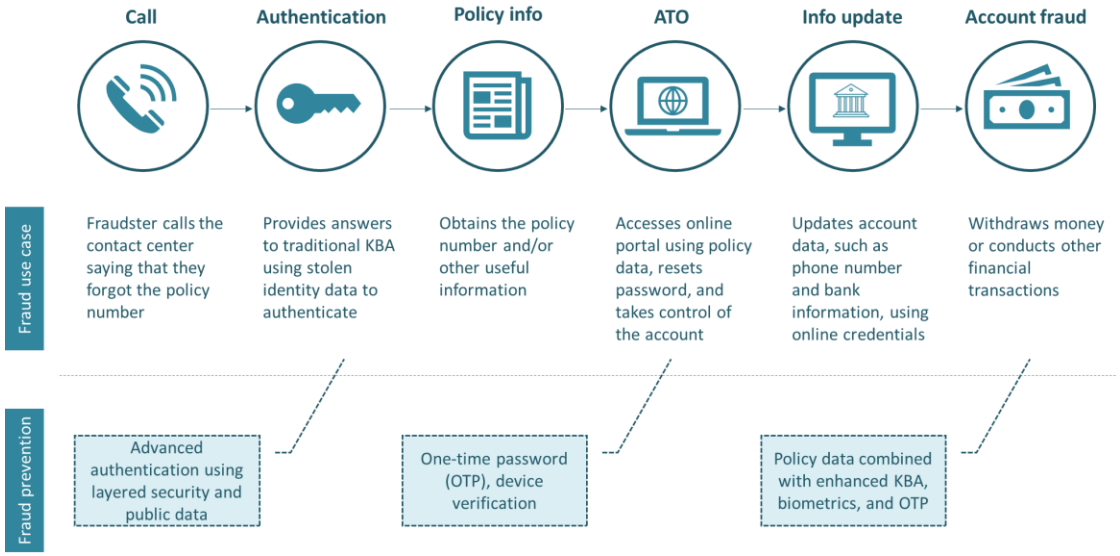
Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Most of the ATO fraud relates to cash-value life insurance or annuity products. Many ATO fraud cases start with a fraudster calling the customer service center with an assumed identity saying that they forgot their policy number. They prove their identity by answering questions based on traditional knowledge-based authentication (KBA) using stolen personal data, and then go online to reset the account password and ultimately assume the ownership of the account. Figure 2 demonstrates this typical use case and provides examples of the preventive actions, which are discussed later in this report.

2. "The Fraud Triangle," Association of Certified Fraud Examiners, accessed May 1, 2021, https://www.acfe.com/fraud-triangle.aspx.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 2: Typical Use Case for an ATO and Examples of Preventive Techniques



Source: Aite Group

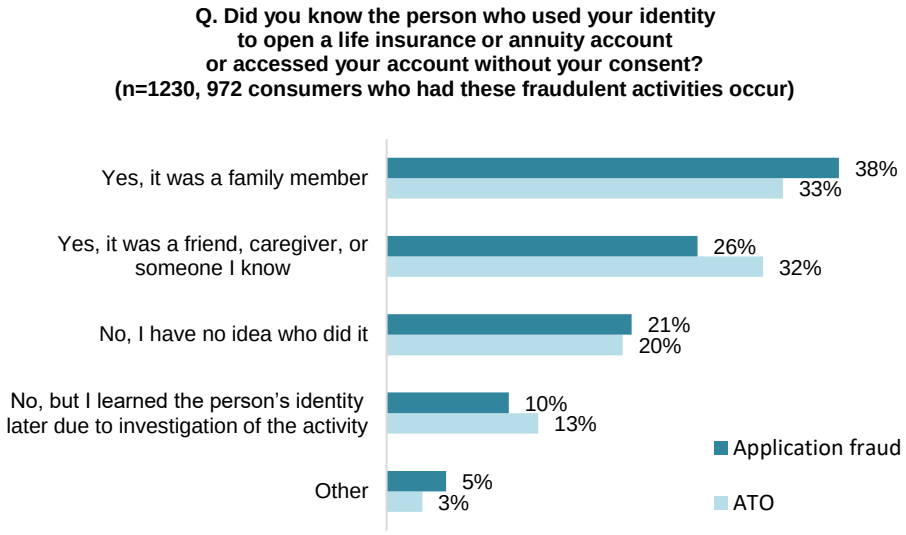
Both insurers' experiences and consumer data show that ATO fraud has increased in the last year, likely due to more digital and online activity. One other important finding from the above-mentioned consumer survey is that 58% more people say that they had a life insurance account fraud incidence in 2020 compared to those who said that fraud occurred in 2019.

Unfortunately, more than 60% of these fraud cases were committed by a family member, a friend, a caregiver, or someone known (Figure 3). Data for both application fraud and ATO show that trend. This is important because the solutions insurers deploy will need to be strong enough to be effective despite the information available to and accessibility of family members and close friends.

In about 20% of the cases, participants did not know who committed the fraud, which likely led to an unrecoverable financial loss in the case of the ATOs. Also, 10% of account-opening-related incidents and 13% of ATO incidents were discovered through insurance company investigations, indicating that more needs to be done to prevent and detect fraud.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 3: Identity of Fraudsters for Application Fraud and ATO



Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Insurers have also seen a spike in fraud-related incidences in the past year. Paperless applications and self-service portals, both for customers and agents, have increased online activity and use of digital data in life insurance sales and service. Life insurers' fraud management teams and special investigation units often find that fraud exists in different forms throughout the life insurance value chain (Figure 4). Not only do these fraud cases have economic impacts, but they also could result in reputational and regulatory consequences for insurance companies.

Figure 4: Examples of Fraud in the Life Insurance Value Chain

Acquisition, underwriting	Customer service	Claims, disbursements
Identity theft	ATO	Retirement withdrawals
Misrepresentation	Personal information theft	Annuity payments
Agent fraud	Elder financial abuse	Death claims
		Disability or health claims

Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IDENTITY THEFT

Identity theft is a common fraud scenario in the customer acquisition process. Many use cases include fraudsters buying life insurance policies on others by stealing their identities and assigning themselves as beneficiaries. As is consistent with the findings of the customer survey, insurers report most of this fraud as originating from family members or other people known to the victim.

MISREPRESENTATION

The increased use of digital process and accelerated underwriting have created opportunities for misrepresentation from the policy buyers themselves. The impact of such underwriting-related fraud may not be known for a few years until mortality analysis or claims experience is available.

AGENT FRAUD

Agents can instigate fraud at multiple points, from sales abuse, commission scams, other financial fraud, or even claims. Sometimes the source of information for fraudsters has been found through identities compromised from a single agent's book of business. Security and encryption of agents' devices, such as laptops, can also become an insurer's concern.

Distribution channels and product selection can be related to sales fraud. Insurers see more fraud originating from independent brokers than from captive agents and financial institution sales. Products with cash value or financial payout are a natural target for identity theft, and products such as index universal life policies have seen more fraud originating from foreign national customers.

ATO

ATO is by far the biggest concern for life insurers, and there has been an increase in ATO attacks on mobile and digital channels. Sometimes information gathered through call centers or compromised emails is exploited on online portals for account withdrawals or for stealing personal information.

ELDER FINANCIAL ABUSE

Another kind of fraud, elder financial abuse, is often uncovered during investigation. In the last two to three years, insurers have seen a spike in cases in which someone took advantage of an elderly person with diminished mental capacity or dependency and got access to that person's insurance, annuity, or retirement account. This is a hard-to-address fraud area because the victim may be coerced into requesting money and cannot be denied by the insurers. Some companies are working with regulators to develop better screening processes for financial transactions.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RETIREMENT AND ANNUITY PAYMENTS

Many fraud issues are seen for life insurance claims, annuity and retirement payments, and group benefit claims. 401(k) accounts collectively hold close to US$5.6 trillion in assets[3] and often do not have a strong authentication in place for withdrawals and transfers. An example of a retirement plan fraud activity is fraudsters using a stolen email access to obtain a one-time password (OTP) to log in to the retirement account and then change the bank account to their own, before making transfer requests.

DEATH CLAIMS

Payment to the right beneficiary is the most important concern for life insurance claims, and even though many cases are dismissed after investigation, the process still costs insurers significant time and money. Many insurers also report receiving a small quantity of false death claims each year.

3. John Sullivan, "401k Assets Totaled $5.6 Trillion in First Quarter 2020," 401(k) Specialist, June 17, 2020, accessed May 1, 2021, https://401kspecialistmag.com/401k-assets-totaled-5-6-trillion-in-first-quarter-2020/.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

MANAGING FRAUD: WHAT IS WORKING WELL

The most effective practices for fraud management can be placed in three categories: strategy, process, and technology. A combination of all three is needed for successful sponsorship, planning, and execution of fraud management. An assessment of life insurance carriers' adoptions and level of impact from these practices is discussed later in this report.

STRATEGY: COMMITMENT AND OVERSIGHT MAKE A DIFFERENCE

Organizations that have a long-term strategy in place to tackle fraud have created multiyear roadmaps and adopted a centralized coordination of activities. While fraud may be monitored and detected at each functional level of a company, centralized coordination through a dedicated fraud function is effective in establishing policies and procedures, training employees, sharing learnings, and continually adopting, evaluating, and improving technology.

Table B summarizes the key strategic elements adopted by high-maturity life insurers.

Table B: Strategic Elements

Practices	Details
Multiyear roadmap	A multiyear roadmap represents a long-term strategy to improve process, methods, and technology. This should be annually updated and approved by the leadership. Balancing fraud prevention with customer friction to deliver a superior experience has also become a key component of multiyear plans for some insurers.
Centralized coordination	This is a centralized coordination through a dedicated fraud function to ensure planning, execution, and governance of fraud management activities.
Sharing of learning	This includes sharing of new information, fraud-related learnings across organizational functions, and collaboration among business areas.
Fraud training and awareness	This is consistent training across the organization and tracking of successful completion. Regular updates on new information are provided.
Executive involvement	This is the role of a chief fraud officer or vice president of fraud.

Source: Aite Group

PROCESS: ORGANIZATION AND PLANNING FOR EFFECTIVENESS

Sound process management requires understanding and planning for the entire life cycle of fraud: awareness, adoption, implementation, operations, and enforcement of relevant policy and procedures, fraud data analysis, investigation, and reporting, and continual improvement of fraud countermeasures. Table C summarizes the process support that insurers find impactful for managing fraud.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table C: Process Support for Identity and Fraud Management

Practices	Details
Fraud risk assessment	Identifying risks and establishing plans and controls to address them is vital. Since fraud may also originate from agents, customers, vendors, partners, and employees, a holistic assessment of fraud is needed, at least annually.
Policies and procedures	These are policies and core responsibilities related to fraud management, signoffs, support for remediation, escalation, etc.
Case management	This includes the methods and tool for initiating, tracking, and monitoring fraud incidences. Mature organizations use common tools across business functions and for related processes, such as anti-money laundering.
Fraud risk scores	These scores help develop criteria for risk identification and escalation. Some organizations use a zero-to-100 scale to identify risk level and route transactions scoring over a certain threshold as referral for investigation. A solution set can evaluate and risk assess the vast array of meta data available in a digital session—from device fingerprint to behavioral biometrics to mobile device identifiers—to assess the risk associated with the session. When choosing risk-scoring solutions from a vendor, care should be taken to avoid considering a black-box solution that does not explain a complete methodology behind the scoring. The scoring method selected should be transparent, explainable, and defendable.
Threat inventory	High-maturity organizations often build a threat inventory through internal risk assessment and external data, and they continually manage and update it through new information from fraud attempts and any newly discovered vulnerabilities.
Layered security	This is the defining and adopting of multiple controls for a stronger defense. It often requires aggregating and analyzing data internally and combining it with external sources to improve the speed and accuracy of fraud detection while using minimum friction.
KPIs to manage fraud	Examples include numbers and the incident rate in new business, underwriting, customer service, and claims; financial impact such as ATO loss and number of cases or calls flagged; effectiveness of the prevention efforts, location of fraud detection, unit cost, customer experience, or any friction due to screening, such as impact on the call handling time.

Source: Aite Group

TECHNOLOGY: A KEY ENABLER

Technology can help execution of a fraud management strategy and can automate many process elements discussed in the previous sections (Table D).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table D: Technology Capabilities for Enabling Identity Management

Technology	Details
KBA	This is authentication by asking questions that only the true user should know, such as policy number, prior address, or credit bureau data. Traditional or static KBA often used by insurers is not considered very reliable anymore because personally identifiable information stored in their databases is most vulnerable to identify theft. Advanced KBA methods that combine a variety of data sources, such as public record, and provide limited time to respond can offer a reliable technique for onboarding identification and authentication.
Advanced identity management	Many commercially available solutions leverage data from many sources (including credit bureaus, public records, mobile phone carriers, devices, location, email, activity, etc.) to verify and authenticate identity by compiling a comprehensive picture of an individual. Such data diversity is important for establishing a layered security process, as described in the previous section.
Multifactor authentication (MFA)	MFAs such as OTPs require the user to provide two or more verification factors to access online accounts. Mobile app or email are commonly used to generate passcodes.
Bank verification	These services help verify account ownership and balance status before payment processing.
Fraud consortiums	Consortiums such as LIMRA's FraudShare or Evadata Protect's forum help carriers share incident information and prevent ATO attacks. Companies such as IDology also offer data from broader multi-industry consortiums.
Log analytics	This is an analysis of aggregated incidence logs to determine alerts and actions. It includes continual tweaking and tuning of settings based on transactional data results, trends, and changes in business requirements and behaviors, as well as fraud tactics observed. This is generally an initial level of analysis many organizations adopt before moving to more advanced predictive analytics.
AI/ML analytics	This is the use of artificial intelligence (AI) and machine learning (ML) to analyze the historical data on fraud occurrences, sources of fraud, and related activities to make predictions and establish standards and control mechanisms.
Enterprise orchestration	This includes building centralized data and functionality layers that use all available identity information from internal and external sources and a uniform fraud management capability, accessible to all organizational groups as a background process.
Link analysis	Link analysis tools sift through the data repositories and discover connections between customers and accounts, then graphically display them to facilitate investigation. For insurers, difficulty lies in linking data across product lines and getting access to activities external to the organization.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Technology	Details
Device verification	This is using characteristics of a device—such as the browser, make/model, IP address, and geolocation data—to identify abnormalities. Since familial fraud is common in life insurance, device-based verification such as fingerprint detection can help prevent fraud.
Voice biometrics	This is the use of voice recognition combined with other attributes such as phone number or passcodes to authenticate a caller. Similar to device verification, voice biometrics can help prevent fraud from friends and family, who often have access to customers' personal data.

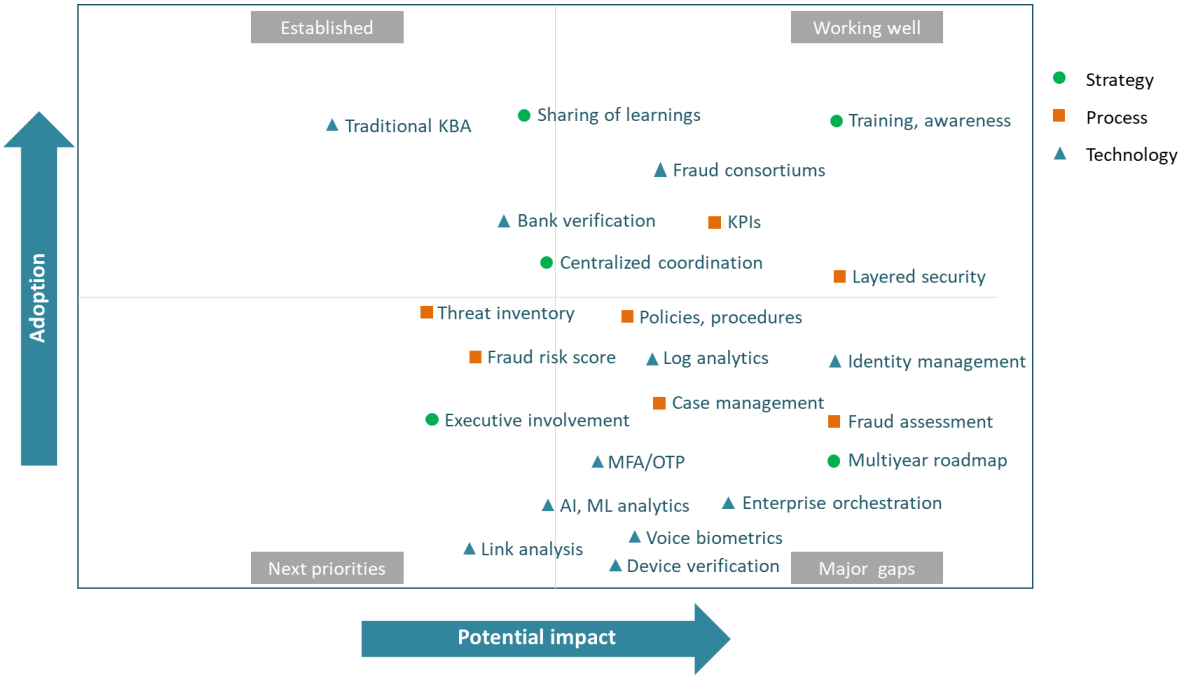
Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CARRIER ADOPTION AND IMPACT

Life insurers are at various levels of maturity in adopting the strategies, processes, and technologies discussed in the previous section. Figure 5 shows an analysis of input from carriers on the adoption of fraud management practices against their impact. In the upper two quadrants, a few practices and capabilities have strong adoption among insurers; many areas are shown to have medium adoption or have gaps that limit the effectiveness of fraud management. There are also areas needing attention, shown in the bottom right quadrant, labeled "major gaps." Many of these practices and capabilities are essential to combating the growing threats of identity theft, ATO, and other forms of insurance fraud.

Figure 5: Industry Adoption and Potential Impact of Fraud Management Practices



Source: Inputs from insurance carriers and Aite Group analysis

Some well-adopted practices that deliver value to the insurers include the following:

- Bank verification
- Enterprise training programs
- Fraud consortiums
- Layered security, in some form
- Metrics and KPIs
- Sharing of learning across functions

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Practices that have a high positive impact on fraud management but are not so well adopted are discussed in the following two sections.

HIGH PRIORITY

The highest-priority practices are those that provide a high impact but still lack adoption among life insurers. Identity verification and authentication, fraud risk assessment, multiyear roadmap, and enterprise orchestration are some of those practices, according to the high-maturity insurers.

IDENTITY VERIFICATION

Identity verification during onboarding is critical. With an increase in digital applications, the agent and customers are often not together, and they complete different parts of an application independently with the benefit of an agent present to verify customer identity. Since this is often the first interaction of the insurer with customers, there is no previously stored data to verify their identity. Use of public data sources, identity documents verification, and behavioral analytics is essential for customer acquisition without much friction in their experience.

AUTHENTICATION

Advanced authentication technologies can significantly reduce fraud losses and improve the speed and accuracy of results. Many insurers are using traditional KBA, which uses the customer's personal information stored in the company's systems. The more dynamic approaches include multifactor authentication, passwordless login, security keys, OTPs, and verification based on multiple sources such as location, email, activity, and devices; they offer step-up escalation as needed. Most organizations are using such methods in a limited capacity. For example, OTP is utilized in many insurers' online portals, but few have implemented MFA in their call centers. In contrast, many financial institutions, such as Vanguard,[4] offer multiple authentication methods as options.

FRAUD RISK ASSESSMENT

Many insurers include fraud risk in internal audits, but few have a dedicated annual fraud-based assessment to check the adequacy of controls and build action plans. Some smaller organizations have opted for external assessments on a less-frequent basis.

ENTERPRISE ORCHESTRATION

A handful of insurers are working on enterprise orchestration of fraud management. They are building centralized data and functionality layers that use all available identity information from internal and external sources, and a uniform fraud management capability is accessible to all functions as a background process. For example, a customer can be identified in a call center, and data from the customer's previous online activity or new business application can be linked

4. "Security at Vanguard," Vanguard, accessed May 1, 2021, https://investor.vanguard.com/security-center.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

to complete authentication. Such data from multiple sources creates an omnichannel identity of callers, thus requiring minimum additional information to authenticate.

MULTIYEAR PLANNING

One big challenge that fraud management functions often face is to obtain budget approval. Fraud managers find it difficult to prove cost-benefit analysis of investments to address the financial losses due to fraud. While the hidden costs of inadequate fraud and identity management should prove the benefits, those are often hard to quantify. The successful organizations have taken a multiyear approach, which helps them with better planning and support for ongoing needs of investments.

To demonstrate the benefits, carriers have shifted the narrative to improving the customer and agent experience by reducing the friction in their interactions while managing the fraud. That helps prove the cost-benefit analysis of fraud management investments and ensures that the program is aligned with customer-centricity and digitalization—often key strategic objectives for many insurers. A survey of trends in fraud mitigation management among 47 financial crime professionals at Aite Group's Financial Crime Forum in September 2020 reveals that 65% of respondents believe that improving client experience plays a greater role in getting investments funded today as compared to two years ago.[5]

NEED ATTENTION

Once insurers address the high-priority areas, they will need to turn their attention to the next group of practices that can help improve the effectiveness of fraud management programs. Centralized coordination, AI/ML analytics, executive role, voice biometrics, and case management fall in this category.

CENTRALIZED COORDINATION

A study by LIMRA in December 2020 found that three out of 10 carriers have a centralized fraud management program.[6] However, a much larger number (seven out of 10) have established fraud oversight committees that seek participation from new business, underwriting, contact centers, cybersecurity, access management, human resources, and distribution. Those that have adopted centralized fraud functions see benefits in efficiency, a better career path for fraud teams, a more effective regulatory response process, and agility in decision-making.

5. See Aite Group's report *Client Experience Trends in Fraud: Navigating a Busy Intersection*, December 2020.

6. Russ Anderson, "Financial Crimes Services and Fraud Prevention Study," Financial Crime Services, LIMRA, LOMA, and LL Global Inc., 2021.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

AI/ML ANALYTICS

Some insures have started using supervised and unsupervised ML models to find patterns in historical activities to identify meaningful variables and behavioral patterns that can improve the fraud prevention approach.[7] Solution providers may also offer ML methods that are closely coupled with active human expertise for pre- and post-verification fraud detection. That is important because existing rules might not detect any new techniques fraudsters have developed, and there is a need to anticipate fraud beyond solutions available through the existing technology. Still, the majority of life insurance companies find it difficult to perform advanced analytics due to a lack of reliable and centralized access to data.

EXECUTIVE ROLE

Few organizations have established a role such as a chief fraud officer or vice president of fraud. While some governance groups have been formed, at most executive committees, reporting of plans and progress is not common unless there is an ongoing serious issue. High-maturity organizations have created a formal fraud governance structure at the executive level and regularly report progress through dashboards and KPIs.

VOICE AND PHYSICAL BIOMETRICS

Authentication based on personal characteristics of a user, such as fingerprints, iris, voice, and face recognition are among the least-adopted technologies in the life insurance space. However, some organizations are piloting voice verifications for their call centers.

CASE MANAGEMENT

While most insurers adopt some level of case management, many still use an ad hoc process or Excel spreadsheets for this purpose. Life insurance is behind the other industries in using an automated workflow-based case management system that is centrally managed and enables alerts, tasks, communication, and reporting.[8]

7. See Aite Group's report *AIM Evaluation: Fraud and AML Machine Learning Platform Vendors*, March 2019.

8. See Aite Group's report *Aite Matrix: Case Management to Combat Global Fraud and Money Laundering*, September 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

TECHNOLOGY SELECTION: KEY CONSIDERATIONS

Technology can help execute strategy, plans, and processes better and faster, and in a cost-effective manner. The technology chosen should match the unique needs of life insurance business processes and governance models.

Many criteria can influence the selection of technology, including how it impacts an insurer's priorities, current multiyear roadmap progress, and plans. Table E provides some important considerations when selecting an identity management technology.

Table E: Criteria to Consider When Selecting Identity Management Technology

Criteria	Considerations
Layered security support	Layered security can combine public sources data with digital identity data sources such as location, email, activity, and mobile phone information. It should be able to create an omnichannel digital identity with verification of physical presence.
Data diversity	Solutions should access multiple data sources, such as public records, and not just be limited to credit bureaus.
Decision transparency	Identity attributes and verification decision-reasoning data should be transparent and actionable for further fraud and customer analysis. Regulators and thus insurers will increasingly need data on why specific decisions, such as for claims, are made. Such decisioning will need to be explainable and defendable to customers, regulators, and other stakeholders.
Locate rate	Leading solutions have a high locate rate for the users. Some insurers expect a 98% rate or higher from their fraud management systems.
Authentication features	Features such as multifactor authentication are standard and necessary for current security needs.
Built-in AI and ML analytics	Analytics should support supervised and unsupervised models, with the ability to ingest data from multiple sources. Hybrid approaches that incorporate dedicated fraud teams with ML-based analytics to identify potential incidences and novel fraud patterns help improve the model predictions.
Business process flexibility	Selected tools should be customizable based on industry, company, and business processes of the organization.
Technology compatibility	Technology should be compatible with the security policy, reporting needs, and existing technology, such as active directories and databases. Ease of installation and upgrades are also highly valuable to reduce ongoing IT support requirements.
Enterprise orchestration support	The solution should be able to facilitate the use of a common tool for multiple layers, escalation methods, and applications such as funds disbursement, onboarding, and customer service.

Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CONCLUSION

Life insurance organizations need to prepare themselves to meet the heightened threat of fraud arising from increasing digital activities and better means available to fraudsters. Their financial assets and reputation, as well as their customers' personal data and finances, are at risk. Some key action items for life insurance carriers include the following:

- Establish a centralized fraud management function for centralized coordination and form multifunctional teams to share learning, discuss approaches, and implement controls and solutions consistently across the organization.
- Create procedures with clearly defined responsibilities related to fraud management. High-maturity organizations perform periodic fraud risk assessments of fraud controls, identify weaknesses, and publish the results.
- Build a multiyear plan and continually refine it with assessment results, new developments inside the organization, externally available technologies, and analytics solutions. The roadmap should also address improvements to processes and technology adoption, and any need for resources.
- Develop scorecards and measurements that show the effectiveness of fraud management activities, controls, and results, and communicate those to the key stakeholders.
- Research, evaluate, and deploy technology for identity management and authentication. The solution should be flexible to adopt the organizational process, governance structure, and reporting needs, and it should be easy to integrate with existing technologies.
- Analyze incidence logs and other fraud-monitoring data to determine alerts and actions. Continually tweak and tune the settings based on transactional data results, trends, and changes in business requirements and behaviors as well as in fraud tactics observed.
- Start to build a plan for enterprise orchestration—a software system that can dynamically handle the complexities of the need for stakeholders, such as consumers and agents, that automatically applies the appropriate level of authentication and that is uniformly available to all business functions as a background process.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RELATED AITE GROUP RESEARCH

U.S. Identity Theft: The Stark Reality, March 2021.

Top 10 Trends in P&C and Life Insurance, 2021: Digital and Data Go to the Next Level, January 2021.

Fraud in Life Insurance: Technology Is the Shield, February 2019.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Manoj Upreti
+1.469.421.7145
mupreti@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com