Aite Novarica

SEPTEMBER 2021

INSURANCE FRAUD

RETHINKING APPROACHES IN THE DIGITAL AGE

MANOJ UPRETI
MIKE TRILLI
STUART ROSE

Presented by:

LexisNexis®
RISK SOLUTIONS

IMPACT REPORT

TABLE OF CONTENTS

LIST OF FIGURES

IMPACT REPORT

SEPTEMBER 2021

INSURANCE FRAUD

Rethinking Approaches in the Digital Age

MANOJ UPRETI
MIKE TRILLI
STUART ROSE

LIST OF TABLES

IMPACT POINTS

- This report is based on 132 respondents from U.S. carriers with 2020 premiums of US$500 million or more, with knowledge of fraud management strategies across underwriting, customer servicing, and claims.
- Life, personal lines, and small commercial insurance leaders in compliance, customer experience, digital experience, digital transformation, information security, IT, operations, and risk can use these insights as a guidepost to evaluate the opportunity to layer in fraud mitigation and identity verification capabilities for underwriting, customer service, and claims.
- This report first introduces the major market trends related to insurance fraud and then provides the findings from the survey in the areas of digital activities, corresponding increase in fraud incidences, solutions adopted, and benefits obtained by the insurers.
- Since early 2020, consumers' digital activity with carriers has dramatically increased compared to pre-pandemic levels, and these accelerated levels of digital activities are expected to continue.
- As digital activity has increased, so has the number of fraud incidents, and carriers need to rethink their digital transformation approach to include appropriate levels of fraud management.
- Like digital activity, fraud is expected to continue its trajectory, and increased business and customer loss from fraud threatens to dilute carriers' benefits from their customers transacting digitally.
- The increase in fraud will require carriers to evaluate their current fraud applications and the breadth of solutions needed to improve fraud mitigation without creating unnecessary friction in the customer experience.
- Key drivers of rising fraud at carriers include increased use of online portals, reduction in face-to-face encounters with customers and agents/advisors, increased coordination among groups of fraudsters using stolen and synthetic identities, and the increased use of alternative underwriting methods at the point of quoting and application.

- A multilayered approach to fraud mitigation and identity verification capabilities requires implementing solutions that apply the appropriate level of security based on the fraud risk levels and that escalate in rigor as necessary. However, more advanced fraud management solutions, such as fraud risk scores or link analysis, lack adoption compared to more common solutions, such as multifactor authentication (MFA).

INTRODUCTION

The pandemic has accelerated the migration of insurers, agents, advisors, and their customers away from face-to-face interactions toward more digital experiences. Carriers have been offering these digital capabilities for years, yet the adoption has been slow. The recent mass adoption of digital platforms and processes, driven by the pandemic, presents a double-edged sword of sorts to insurers. On the one hand, it helps improve customer experience, increases speed of policy issuance or service, and reduces cost. On the other, digital transformation expands the means and opportunities for fraudsters to steal identities and commit financial fraud.

Insurers need to make sure that their fraud mitigation and identity verification capabilities appropriately guard against fraudulent activities and match the strength of the advanced methods fraudsters may use. The approach should be to apply continual improvement by evaluating defenses and then identifying the solution needs, either to enhance an existing solution or implement a new one. The insights from this report can be used to support insurers in this evaluation and to embrace a multilayered fraud mitigation and identity verification approach. This report is intended for life, personal lines, and small commercial insurance leaders in compliance, customer experience, digital experience, digital transformation, fraud management, information security, IT, operations, and risk.

The report begins with an overview of key market trends. Then it provides a measure of increases in digital activity and corresponding rising fraud incidents during the first year of the pandemic as well as an analysis of the impact of those trends on the insurers. Finally, it looks at fraud solutions and their adoption as well as the benefits of a multilayered approach to fraud management.

METHODOLOGY

LexisNexis Risk Solutions—a data, advanced analytics, and technology firm in identity fraud prevention—commissioned Aite Group to conduct an online quantitative survey in May 2021. The survey is of 132 U.S. subject-matter experts and decision-makers of fraud prevention strategies at insurance carriers. Target carriers had at least US$500 million in 2020 premium revenue. To create an adequate representation of industries, business functions, and subject-matter expertise, the respondents were distributed across following areas:

- Life insurance, personal lines insurance (auto, home), and small commercial lines insurance carriers
- Underwriting, claims, and service as knowledge base
- Roles in the following departments: customer experience, fraud or special investigation units, claims, compliance, underwriting, new business, digital transformation, information security, IT security, operations, and risk

The data have a margin of error of approximately 8 points at the 95% confidence level. Statistical tests of significance, where shown, were conducted at the 90% level of confidence.

THE MARKET

Like customers in banking and other industries, insurance policyholders are adversely impacted by identity theft. The perpetrators of this type of theft are often associated with organized crime rings. Data breaches are perhaps the most common example, yet a family member or friend fraudulently buying a policy or accessing an account is also a frequent use case. This identity theft trend is viewed in conjunction with more policyholders and agents interacting digitally with carriers in lieu of more traditional face-to-face encounters. The implications of these trends point to carriers needing to evaluate the effectiveness of their current fraud mitigation and identity verification strategies and capabilities, as the number of fraud incidents is on the rise. This sober evaluation is also important as insurers try to achieve business goals tied to digital transformation (Table A).

TABLE A: THE MARKET

MARKET TRENDS	MARKET IMPLICATIONS
Insurance has an identity theft problem.	An estimated 18% of life insurance and personal lines policyholders fell victim to identity theft (account takeovers or application fraud) in 2020, and this data point represents a call to action for insurers to take stock of their current fraud prevention strategies and the level of defense they are providing.[1]
Consumers' personally identifiable information (PII) has been exposed to many 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 and take over existing accounts, creating a need for insurers to adopt more advanced identity verification tools.[2]

[1] See Aite Group's report U.S. Identity Theft: Consumer Trends in Health, Life, and P&C Insurance, June 2021.

[2] See Aite Group's report Beat Life Insurance Fraud With Identity Verification and Authentication, June 2021.

MARKET TRENDS	MARKET IMPLICATIONS
Carriers are at an inflection point relative to digital interactions with consumers.	Carriers saw increases in digital activity across underwriting and claims functions when compared to pre-pandemic levels, and this pace of digital activity is expected to continue. Although customers are increasingly shifting to digital activities, they still expect their policies, accounts, and transactions to be protected against fraud. Therefore, carriers cannot overlook fraud at the expense of achieving business goals.
Carriers see an increase in consumer digital activity, which increases their fraud risk and results in more fraud.	The increase in digital activity has brought about an influx of digital newbies who tend to be more susceptible to social engineering and identity theft. Carriers reported an increase in fraud rates across underwriting and claims functions when compared to pre-pandemic levels, and there is no indication this pace will slow. This places a greater onus on insurers to upgrade, augment, and replace existing fraud management tools and systems, and to integrate elevated data and intelligence.
Fraudsters are taking opportunities across underwriting, claims, and servicing.	Underwriting is a focus area in life insurance as a potential fraud entry point, yet this area receives less focus in property and casualty (P&C) insurance than customer service and claims, despite its emergence as a fraud entry point. It will be incumbent on carriers to increase fraud defenses across underwriting, customer service, and claims to keep up with advances being made by fraudsters.

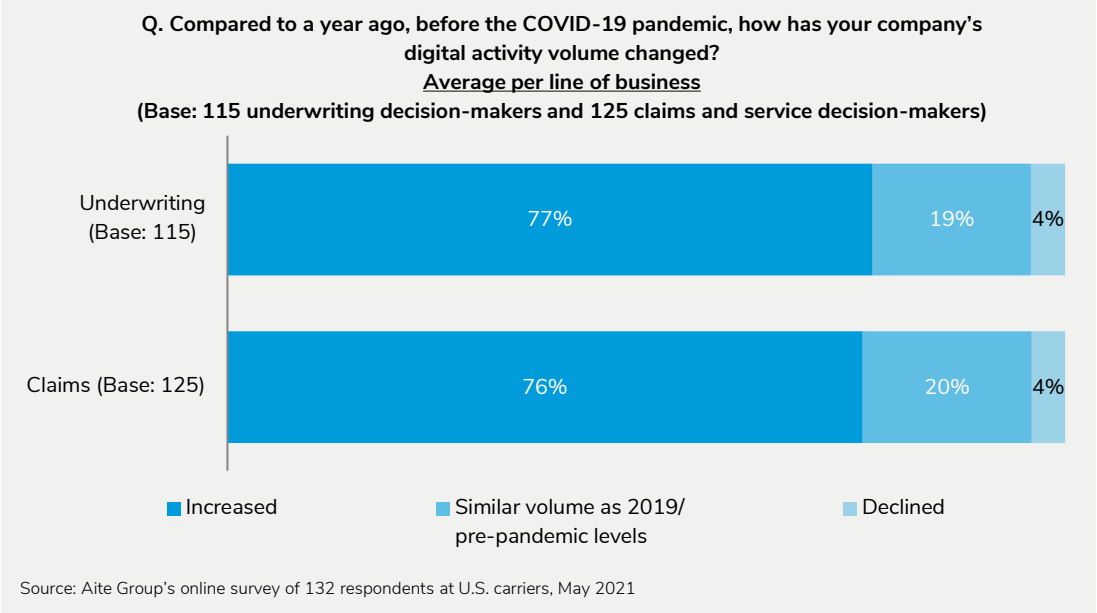
Source: Aite-Novarica Group

INCREASED DIGITAL ACTIVITY: THE NEW NORMAL IN INSURANCE

Most carriers saw an increase in digital activity by their customers in 2020 across both underwriting (77%) and claims (76%) during the pandemic (Figure 1). One factor driving higher digital activities in underwriting was quote requests. Life insurers were more likely to see a doubling of digital interactions in this area than before the pandemic.

On the claims side, 76% of carrier respondents saw an increase in digital activities. Two areas driving this trend for P&C carriers were claim initiation and claim payments. Carriers leaning on automation for first notice of loss and outbound disbursements are key contributors for this increase in digital activity levels.[3]

FIGURE 1: CURRENT DIGITAL ACTIVITY LEVELS AT CARRIERS

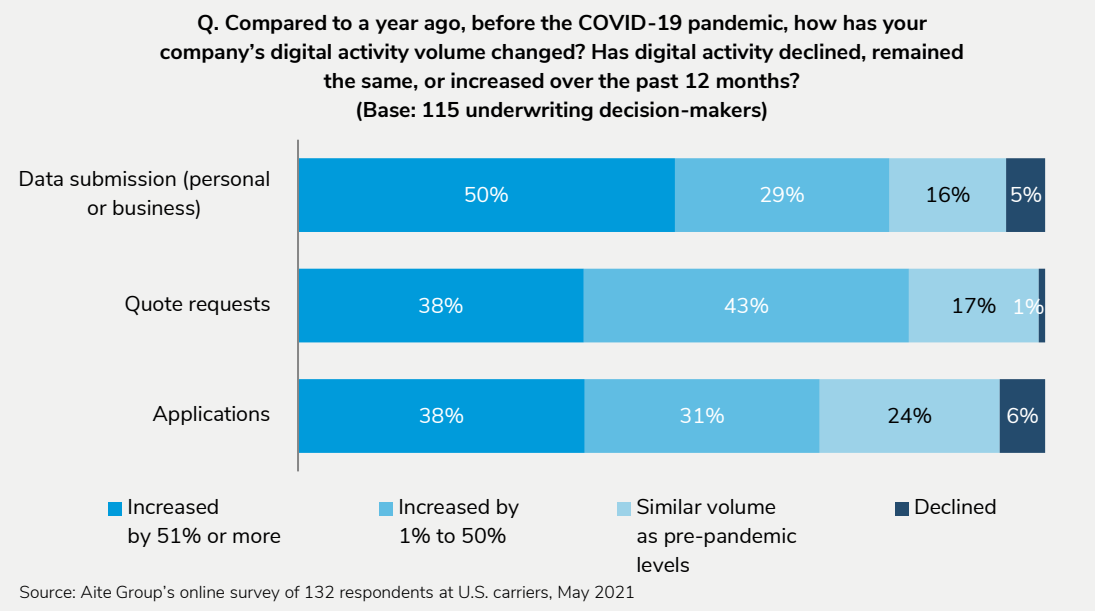


Source: Aite Group's online survey of 132 respondents at U.S. carriers, May 2021

As carriers seek to scale their digital assets, data submission—data provided either by the insured or a third party to help with the underwriting decision—is one underwriting-related area seeing significant online activity growth. Half of the respondents say it has increased by more than 50% compared to a year ago. In many cases, the underwriting decision is being made using alternative, or automated, methods (Figure 2).

[3] See Aite Group's report A Digital FNOL Market Overview: First Impressions Last, July 2021.

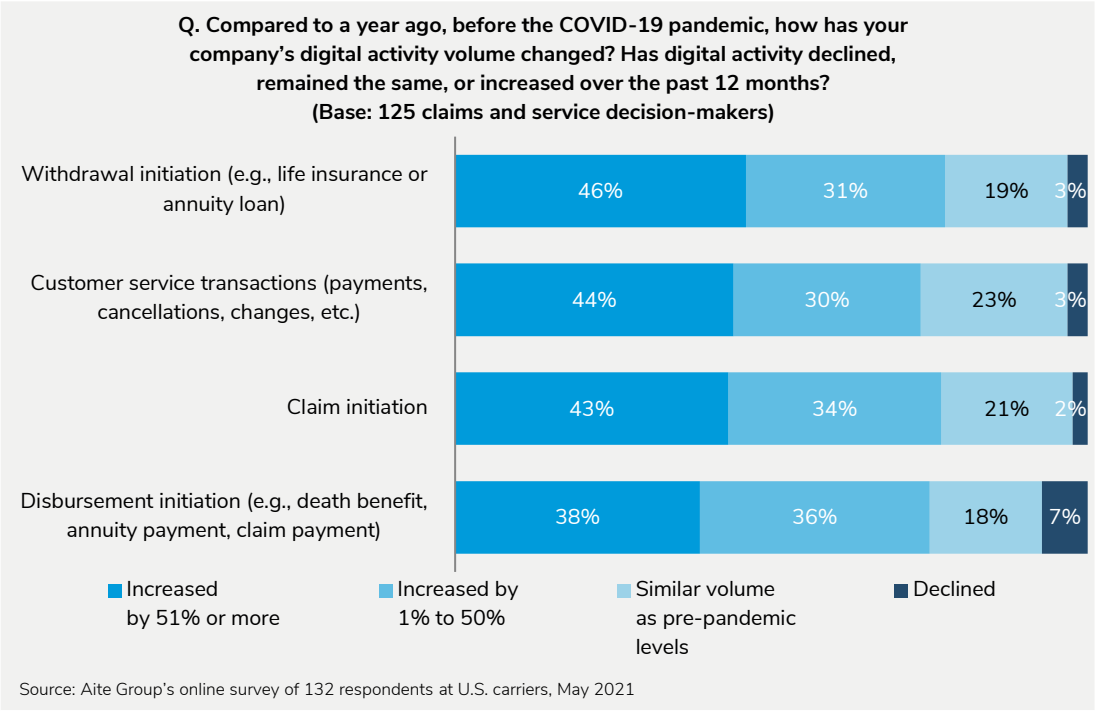
FIGURE 2: UNDERWRITING ACTIVITIES WITH INCREASED VOLUME DURING THE PANDEMIC



Source: Aite Group's online survey of 132 respondents at U.S. carriers, May 2021

Further downstream, policy life cycle processes, such as claims and withdrawals initiation, are driving a significant amount of digital consumer activity (Figure 3). Digital newbies are more likely than most to be susceptible to social engineering, scams, and coercion, as they are less likely to practice sound security practices. Increasing digital adoption often triggers increased proliferation of stolen PII.

FIGURE 3: CLAIMS AND SERVICE ACTIVITIES WITH INCREASED VOLUME DURING THE PANDEMIC



Source: Aite Group's online survey of 132 respondents at U.S. carriers, May 2021

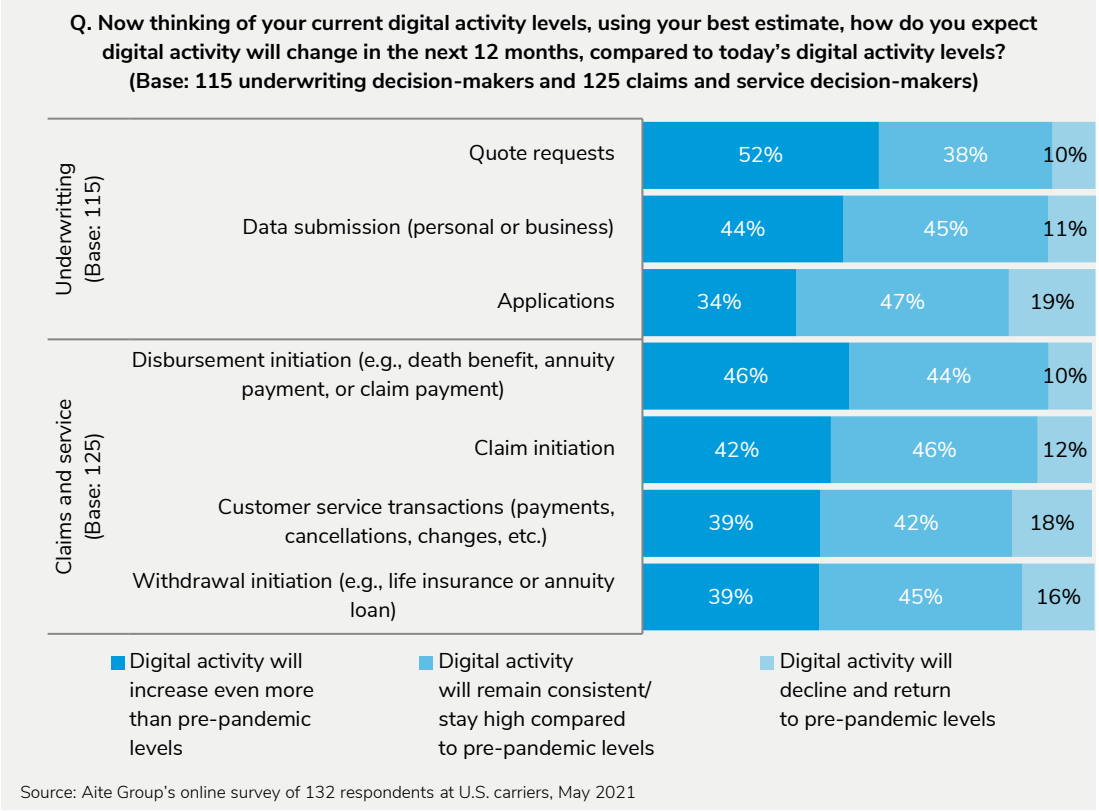
DIGITAL TREND EXPECTED TO CONTINUE

According to 42% of the survey respondents, insurance carriers can expect this digital trend to continue at levels higher than those occurring prior to the pandemic, ushering in a new normal for carriers. The biggest drivers for this increase in digital activities are consumers continuing to opt for convenience and younger buyers increasingly purchasing their policies online. In addition, consumers' digital behaviors during the pandemic, such as familiarity with digital tools and greater comfort with remote and virtual interactions, will also generate traction toward online activities.

Carriers have their hand in this increase as they make use of digital processes in greater numbers within their portfolios and leverage data to simplify and automate underwriting and claims workflows. Thirty-four percent to 52% of respondents expect digital activities for underwriting and claims to grow even further than pre-pandemic levels in the next 12 months (Figure 4). For example, the adoption of electronic health records in life insurance underwriting has changed the behaviors of agents and customers, and that trend is expected to continue in the future. For personal lines, claims trends include

the adoption of remote virtual inspections and the use of artificial intelligence to assess the damaged property or vehicle and to determine the next steps in the claims workflow.

FIGURE 4: ACTIVITIES DRIVING FUTURE DIGITAL INTERACTIONS



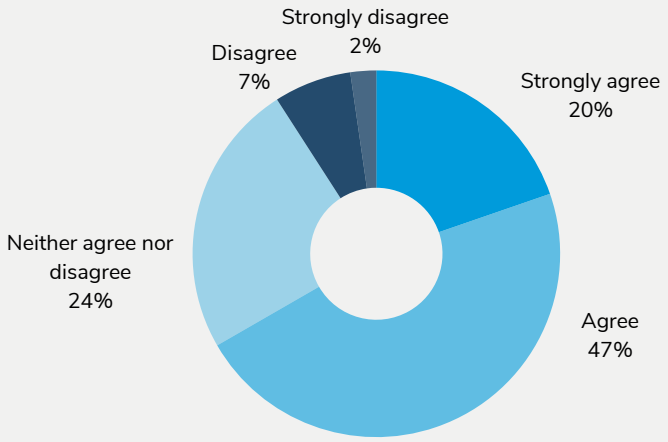
Source: Aite Group's online survey of 132 respondents at U.S. carriers, May 2021

ENHANCED CUSTOMER EXPERIENCE COMES AT A PRICE

The increase in digital interactions is enhancing the customer experience and creating a path for carriers to deepen customer relationships over the life of a policy and not just at the time a claim is filed. With benefits come risks, and carriers are faced with challenges as this digital explosion is occurring in conjunction with a persistent threat of identity theft and fraud incidents. As proof, 67% of respondents either agreed or strongly agreed that the increase in digital transactions has resulted in higher fraudulent activity (Figure 5).

FIGURE 5: IMPACT OF DIGITAL ACTIVITY ON FRAUD

Q. To what extent do you agree or disagree with the statement "An increase in digital activity has resulted in more fraud or a higher fraud risk"? (Base: 132 claims and service or underwriting decision-makers)



Source: Aite Group's online survey of 132 respondents at U.S. carriers, May 2021

Carriers experiencing increased fraudulent activities are seeing this occur, almost evenly, across three entry points: underwriting or at the point of application, customer service or at the point of account access, and claims or at the point of payment. It is worth noting the increases in fraud across underwriting and claims functions have exceeded pre-pandemic levels for most carriers (Figure 6). A common theme that emerged among respondents who experienced higher fraud incidences last year is that the rate of increase in fraud can be characterized as higher than their typical year-over-year rise. Insurers' experiences confirm that fraud increases in the last year are likely due to more digital and online activity. Following are the most common examples of fraud incidences cited by the insurers:

- Account takeover (ATO) concerns for life insurers have exacerbated as they offer the new digital service model. Digitalization combined with the lack of advanced identity security at customer call centers can offer new opportunities to fraudsters.[4] Most ATOs start with a fraudster calling customer service with an assumed identity saying that they forgot their policy number. They prove their identity by answering

[4] See Aite Group's report Improved Customer Experience, Reduced Fraud and Cost: Contact Center Solutions, December 2020.

questions based on stolen personal data and then go online to reset the account password and ultimately assume ownership of the account.

- P&C carriers are on heightened alert to cybercrime due to the increased digitalization of the underwriting and claims processes. A significant proportion of claims fraud is perpetrated through illegally obtained policies. Insurance companies need to acquire a holistic view of the insured and the electronic devices interacting with their systems to not only minimize application fraud but also mitigate the number of fraudulent claims initiated and paid.

FIGURE 6: CHANGE IN FRAUD ACTIVITY AT CARRIERS

Source: Aite Group's online survey of 132 respondents at U.S. carriers, May 2021

The drivers of fraud activities most carriers experienced can be traced back to three main areas:

- The assets tied to their digital transformation efforts, such as online portals, alternate underwriting, and claims automation
- The availability of consumer data to fraudsters due to data breaches
- The pandemic's impact on changing consumer behaviors/lifestyles

Insurers need to make sure their fraud mitigation and identity verification capabilities are conducive to removing consumer friction within digital workflows. However, insurers need to guard against fraudulent activities and protect against advanced fraudster methods using stolen information or synthetic identities. As carriers perform this ongoing evaluation of their capabilities, they should assess the following, as many have been accentuated during the pandemic and provide motivation for the fraudsters:

- Impact of increased use of online portals to purchase a policy, create a new account, or access an existing account
- Impact of increased coordination among groups of fraudsters to use false information to submit a fraudulent application or take over an existing account
- Impact of and gaps in current safeguards around the use of alterative underwriting methods and data—for example, medical records for life insurance or aerial imagery to find property location for P&C in the claims process
- Impact of and gaps in the understanding of the electronic devices interacting with carrier systems due to the reduction in face-to-face interactions between customers and agents/advisors

FRAUD MITIGATION AND IDENTITY VERIFICATION CAPABILITIES

An increase in fraud rates, and fraud risk, is a signal for insurers to ensure that their capabilities are guarding well against fraudulent activities and matching in strength to the advanced methods fraudsters may use. If they are not already doing so, insurers should consider a multilayered approach to improve their mitigation efforts. This layered approach works across two dimensions. The first dimension is functional, as carriers address the prospects of fraud across underwriting, customer service, and claims. The second dimension is capabilities, as carriers assess strengths and gaps across those functional areas, implementing a suite of solutions.

Table B shows insurers' investment focus on service, claims, and underwriting functions. Life insurance companies have a greater focus on service, likely due to high ATO risks. Personal and small commercial insurance carriers face a greater claims fraud risk, and that shows in their relatively higher investment focus in claims.

TABLE B: CARRIER INVESTMENT FOCUS FOR FRAUD SOLUTIONS BY INSURANCE TYPE

FUNCTIONAL AREA	PERSONAL LINES (BASE: 51)	LIFE INSURANCE (BASE: 42)	SMALL COMMERCIAL (BASE: 39)	TOTAL (BASE: 132)
Service	49%	57%	36%	48%
Claims	37%	19%	44%	33%
Underwriting	14%	24%	21%	19%

Source: Aite Group's online survey of 132 respondents at U.S. carriers, May 2021

Many types of solutions have emerged over the past several years for protecting online identity and accounts—for example, identity verification, email address profiling, document identification, MFA, password-free authentication, fraud scoring, link analysis, and behavioral and physical biometrics such as voice analytics. Table C provides a list of common capabilities considered or implemented by many insurance carriers for identity verification and authentication and examined through this survey.

TABLE C: COMMON FRAUD MITIGATION AND IDENTITY VERIFICATION CAPABILITIES

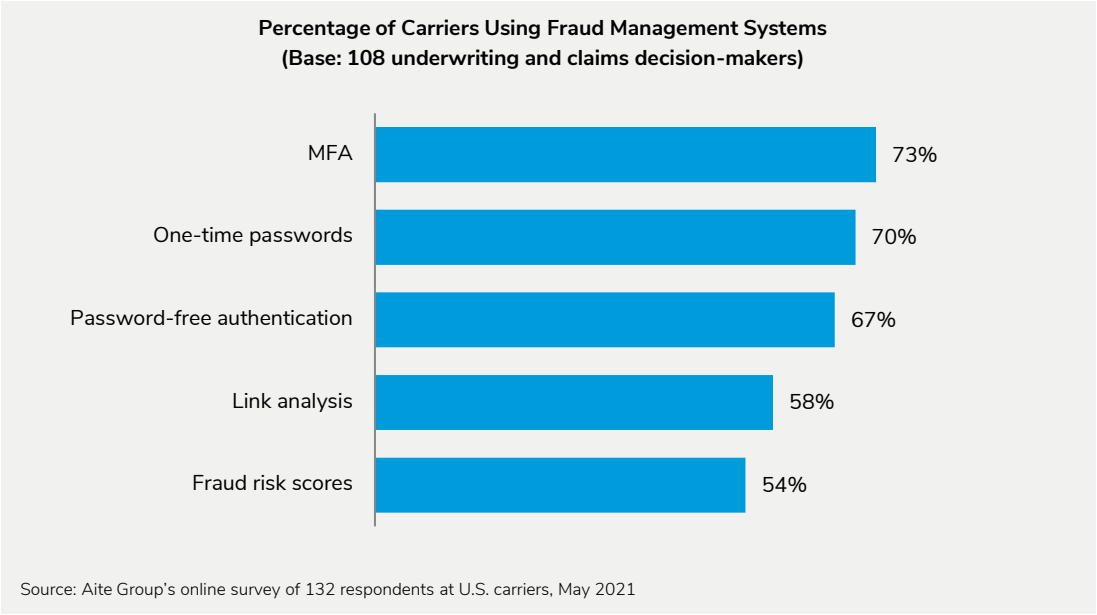
FRAUD MITIGATION SOLUTION	DETAILS
MFA	Many forms of authentication require two or more forms of evidence for users to log in. Examples include a one-time password (OTP), a push notification on mobile devices, and token cards.
OTP	OTP is a type of MFA in which a passcode is sent to users—for example, through mobile text or email—and is used in addition to the login credentials for authentication.
Password-free authentication	Several solutions no longer require a password as part of the authentication, such as simple clicks on magic links, facial recognition, and fingerprint-based authentications.
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 to route transactions scoring over a threshold as referral for investigation. A solution set can evaluate the vast array of metadata available in a digital session—from device fingerprint to behavioral biometrics to mobile device identifiers—to assess the risk associated with the session.
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.

Source: Aite-Novarica Group

Carriers' adoption of capabilities varies (Figure 7). MFA is the leading solution implemented across carriers of personal lines, life, and commercial insurance, for all premium revenue sizes and for both underwriting and claims functions.

More advanced solutions to mitigate fraud, such as digital fraud risk scores and link analysis, remain underpenetrated overall to complement other customer-facing solutions. However, small commercial carriers are more likely to be using fraud risk scores for claims than are life insurance or personal lines carriers.

FIGURE 7: CURRENT ADOPTION OF FRAUD SOLUTIONS



Source: Aite Group's online survey of 132 respondents at U.S. carriers, May 2021

ADOPTING A MULTILAYERED STRATEGY TO OBTAIN BENEFITS

Carriers could benefit by identifying and adopting multiple solutions, or by taking a multilayered approach, for a stronger defense. This requires merging data from multiple sources, combining fraud solutions to validate identity verification and authentication, and escalating the security controls based on the level of internal and external information available about the user. No single technology will detect and prevent all fraud, but rather a combination of solutions and coordination across functional areas will bolster defense throughout the policy life cycle.

Table D provides five key benefits experienced when using various fraud management solutions. Increased accuracy is the most cited benefit, whereas carriers struggle with ease of deployment and with realizing efficiency benefits. A summary of the benefits carriers see for each of these solutions follows:

- Increased accuracy is the most cited benefit, and 45% to 65% of respondents saw that as a benefit provided by most of the fraud management solutions. While some form of identity management and authentication has always been in place via

traditional methods such as knowledge-based authentication, more advanced solutions help mitigate risks better while avoiding false positives.

- Fifty-one percent or fewer respondents selected reduced fraud as a benefit across all solutions. OTP is viewed as more effective in claims compared to other solutions. Fraud risk scores were viewed as most effective in reducing underwriting fraud. Overall, the findings suggest that carriers view their traditional methods as equally effective in managing fraud but find these advanced solutions beneficial in other ways, such as improved accuracy.
- Ease of compliance is another common benefit these solutions deliver. Regulators and thus insurers increasingly need data on why specific decisions, such as for claims, are made. Such decisioning needs to be explainable and defendable to customers, regulators, and other stakeholders. MFA surfaces and is seen as helping with compliance by 52% of respondents.
- Ease of deployment was seen as a benefit by only 33% or fewer respondents. Solutions such as fraud risk score require developing standards, establishing a threshold, and integrating with existing solutions. Only 13% believed the deployment of risk scores to be easy for claims, and 16% for underwriting.
- Operational benefit is another area not yet matured, as shown by a small number of respondents selecting increased efficiency as a benefit. MFA surfaces in this category (31% for underwriting and 30% for claims), likely driven by its wider adoption compared to other solutions.

TABLE D: BENEFITS EXPERIENCED WITH FRAUD MANAGEMENT SOLUTIONS

SOLUTIONS	INCREASED ACCURACY	LESS FRAUD	EASE OF COMPLIANCE	EASE OF DEPLOYMENT	INCREASED EFFICIENCY
OTPs (Base: 88)	65%	51%	39%	33%	30%
MFA (Base: 92)	61%	40%	52%	27%	35%
Link analysis (Base: 70)	53%	49%	49%	26%	21%

SOLUTIONS	INCREASED ACCURACY	LESS FRAUD	EASE OF COMPLIANCE	EASE OF DEPLOYMENT	INCREASED EFFICIENCY
Fraud risk scores (Base: 63)	51%	46%	44%	17%	24%
Password-free authentication (Base: 82)	45%	46%	41%	30%	16%

Source: Aite Group's online survey of 132 respondents at U.S. carriers, May 2021

CONCLUSION

Insurance carriers have many opportunities to mitigate and prevent fraud. At the same time, they need to make it easy for customers and agents to interact digitally and strengthen relationships, with the goals of retaining their customers and growing their business. Here are some recommendations for carriers as they evaluate their fraud strategies and capabilities across underwriting, customer service, and claims:

- **Realize the new normal is here.** Carriers' investment in digital assets and the impact of the pandemic on consumer behaviors have driven increased digital activity between carriers, agents, and consumers—this is the new normal.
- **Do not overlook fraud as a side effect of digital transformation.** While insurance carriers experience this digital revolution, they cannot overlook the increase in fraud rates and fraud risk that is occurring in parallel, which threatens to dilute benefits due to higher claims costs and strain the operations and consumer relationships they are investing to develop.
- **Close the capability gap.** Many carriers have invested in some fraud capabilities, yet the majority are still on the fence with implementing more advanced solutions, creating a notable capability gap for insurers in the current high-fraud-risk environment in which cases are increasing.
- **Adopt a multilayered approach.** No single technology will detect and prevent all fraud. Carriers need to identify and adopt multiple solutions or take a multilayered approach for a stronger defense.
- **Balance investment across functional areas.** Servicing remains a prime area of investment, and this should be a priority. But it is necessary to demonstrate an investment discipline and execute a strategy that extends throughout the policy life cycle.

RELATED AITE-NOVARICA GROUP RESEARCH

U.S. Identity Theft: Consumer Trends in Health, Life, and P&C Insurance, June 2021.

Beat Life Insurance Fraud with Identity Verification and Authentication, June 2021.

P&C Underwriting Fraud: A Market Overview, April 2021.

Rethinking Life Insurance Underwriting: Leapfrog Competition, Delight Customers, February 2021.

ABOUT LEXISNEXIS RISK SOLUTIONS

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

LexisNexis Risk Solutions
+1.800.458.9197
insurance.sales@lexisnexis.com

Media Contact
Rocio Rivera
+1.678.694.2338
rocio.rivera@lexisnexisrisk.com

ABOUT AITE-NOVARICA GROUP

Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, markets, and operations to hundreds of banks, payments providers, insurers, and securities firms as well as the technology and service providers supporting them. Our core values are independence, objectivity, curiosity, and a desire to help all participants in financial services create better, more effective strategies based on data, well-researched opinions, and proven best practices. Our experts provide actionable advice and prescriptive business guidance to our global client base.

CONTACT

Research and consulting services:
Aite-Novarica Group Sales
+1.617.338.6050
sales@aite-novarica.com

Press and conference inquiries:
Aite-Novarica Group PR
+1.617.398.5048
pr@aite-novarica.com

For all other inquiries, contact:
info@aite-novarica.com

Global headquarters:
280 Summer Street, 6th Floor
Boston, MA 02210
www.aite-novarica.com

AUTHOR INFORMATION

Manoj Upreti
+1.469.421.7145
mupreti@aite-novarica.com

Mike Trilli
+1.617.398.5058
mtrilli@aite-novarica.com

Stuart Rose
+1.984.263.9783
srose@aite-novarica.com