# Financial Crimes Services and Fraud Prevention Study

May 2022

LIMRA®

*Navigate With Confidence*

# Financial Crimes Services and Fraud Prevention Study

## Contact Information

**Russell Anderson, CFE**
Head of Financial Crimes Services
Randerson@limra.com

**Sharyn Kessler**
Financial Crimes Services Program Owner
SKessler@loma.org

# TABLE OF CONTENTS

# Introduction

LIMRA's Financial Crimes Services (FCS) and Fraud Prevention study provides the life insurance and retirement industry with a collective look at the most current data and information related to their financial crimes services and fraud prevention programs. This report is an update of a 2021 report.

## Key Findings

- The number of fraud incident attempts across the industry continues to rise across nearly all types of fraud. While this doesn't speak to the success of those attempts, the industry must remain vigilant and continuously assess and enhance controls to mitigate and prevent fraud.
- There has been a trend towards centralizing the governance of fraud programs. Today, 5 in 10 companies have fully centralized programs, 4 in 10 are partially centralized, leaving just 1 in 10 fully decentralized.
- Six in 10 companies have formal oversight committees with an average of five areas participating. Larger companies are more likely to have such committees than smaller companies.
- While 4 in 10 companies most recently conducted a formal risk assessment of their financial crimes and fraud exposure in 2021, another 4 in 10 either haven't done so since 2018 or earlier or have never done so.
- There is a long and growing list of tools and services to help companies combat fraud in their businesses, including some they developed internally.
- When a customer contacts the company through one of many channels (e.g., phone, online, mobile app), the company needs to ensure that person is who they say they are. Companies accomplish this through authentication, using both traditional and, increasingly, more sophisticated methods. Mobile apps and websites appear to utilize more sophisticated methods than interactive voice response (IVR) systems or call centers.
- Running a financial services business today has become a balancing act between protecting customer accounts and providing a good customer experience. Companies continue to offer customers the ability to perform self-service transactions via customer websites, though are more likely to allow them to make changes to their accounts than to initiate withdrawals online.
- Looking towards the future — topping the list of 2022 areas of focus is the authentication process and control enhancements; the most common exposure of concern to companies is account takeovers; and the top two biggest challenges facing companies in 2022 are technology-related and resource-related, both financial and human.

### METHODOLOGY

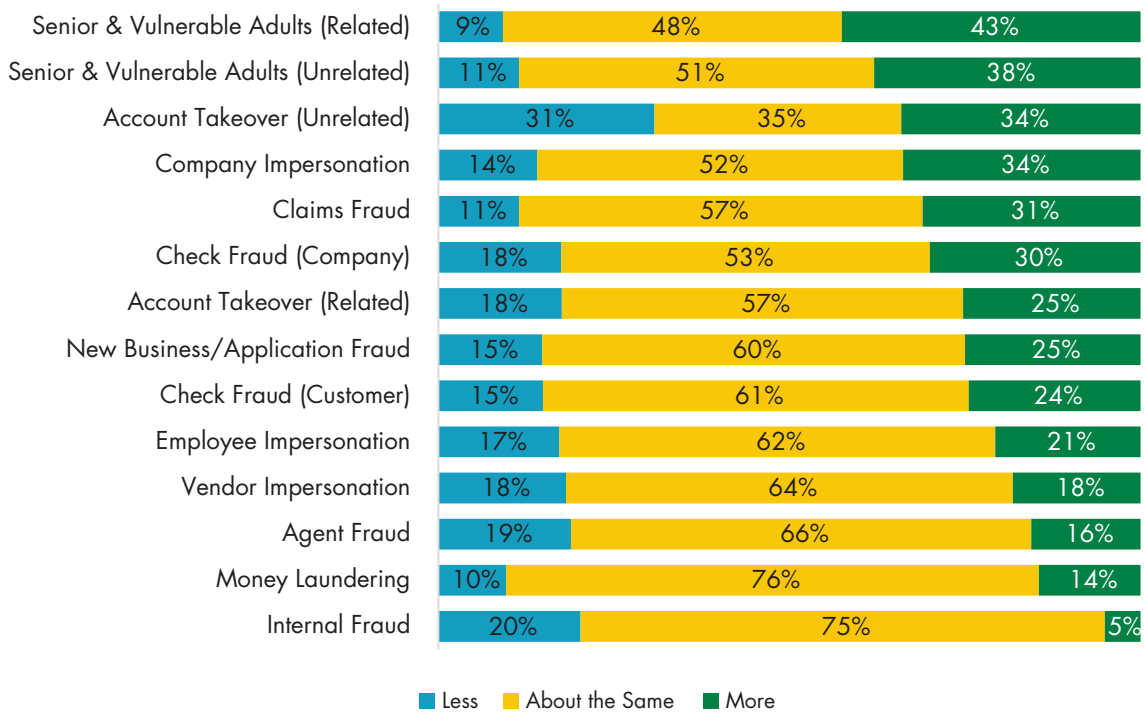
The study was fielded in January and February 2022. Follow-up interviews were conducted with select companies to obtain supplemental data and insights.

Responses were received from 56 companies, with varying levels of participation at the question level.

# Fraud Trends

Fraud continues to challenge the industry, as the tendency for fraud incidents increased last year in all but two categories of fraud. It is important to note that a fraud incident speaks only to the attempts and does not indicate whether those attempts were successful.

## Confirmed Fraud Incidents in 2021 Compared to 2020

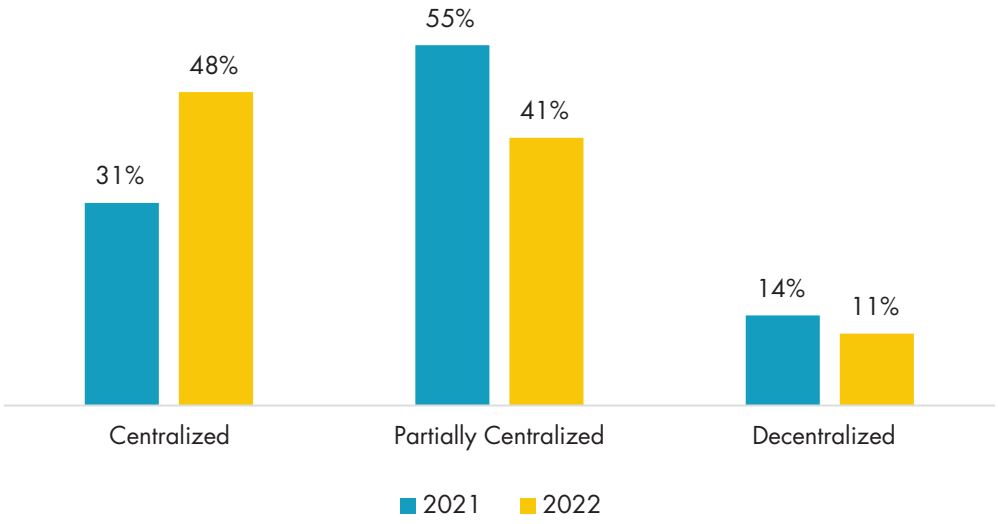



Notes: Companies could also indicate N/A. Those responses have been excluded from this chart to show the trend for companies where each type of fraud is relevant. See Appendix A for definitions of fraud types.

# Program Organization

Nearly half (48 percent) of companies have a fully centralized financial crimes and fraud management function. This is higher than the 3 in 10 reported a year earlier. An additional 41 percent of companies have a partially centralized function, leaving just 11 percent fully decentralized. These results are consistent regardless of company size or complexity (such as the number of business lines or distribution channels).

## Fraud Program Organization



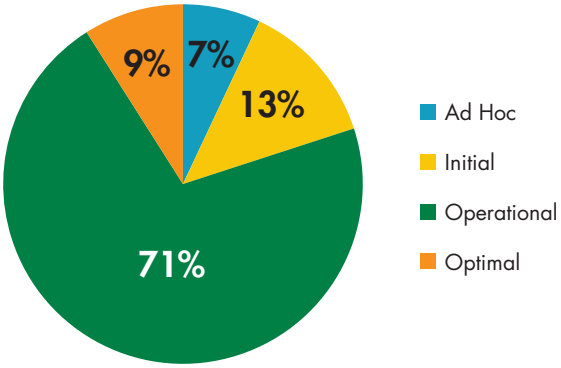

Regardless of how a program is organized, on average, nearly seven teams across the company play an active role in it. However, primary responsibility typically falls in either compliance, a special investigation unit (SIU), or a team created specifically to manage financial crimes and fraud operations.

## Team With Dominant/Primary Responsibility

# Program Maturity

As with last year's study, a small number of companies consider their programs to be optimal. Maturity is consistent across different size companies, whether measured by admitted assets or employees.

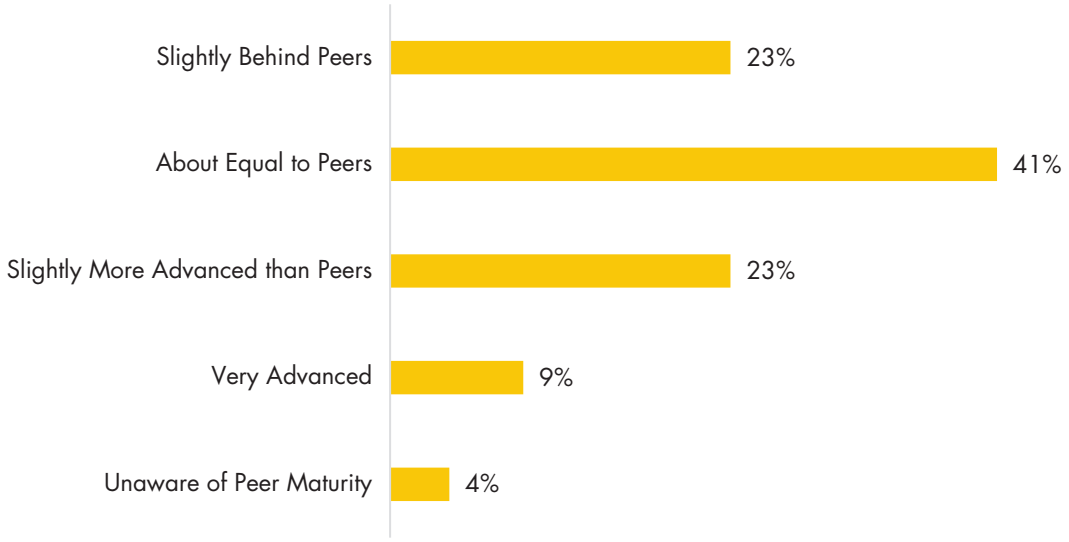
## Program Maturity




Note: See Appendix A for program maturity definitions.

Interestingly, more companies feel their programs are ahead of rather than behind their peers. Compared to last year, fewer companies believe their programs to be on par with their peers (41 percent this year versus 61 percent last year).

## Program Comparison



# Governance

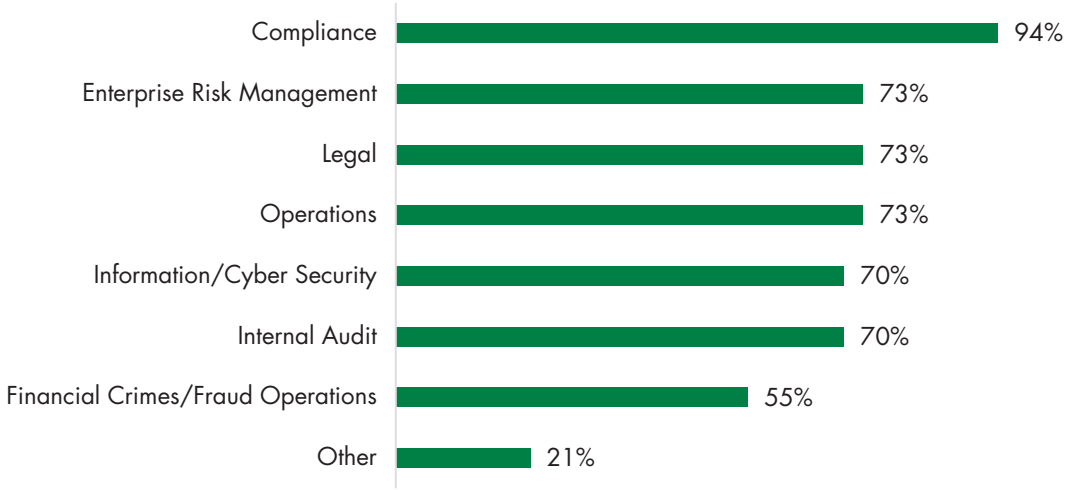
Six in 10 companies have a formal oversight committee or group tasked with overseeing their programs, down slightly from 7 in 10 reported last year. Larger companies are much more likely to have a formal oversight committee than smaller companies. For example, just 4 in 10 companies with less than $5B in admitted assets have committees compared to 9 in 10 companies with more than $100B. An average of five areas participate on these committees.

Three in 4 companies provide regular management reporting to board members/audit committees, executive management, and/or senior management. One in 3 provide reporting to middle management, and 1 in 4 to unit/front line management.

**"Holding fraud awareness meetings with front line management helps maintain a heightened sense of fraud awareness and helps drive accountability for maintaining appropriate fraud controls."**

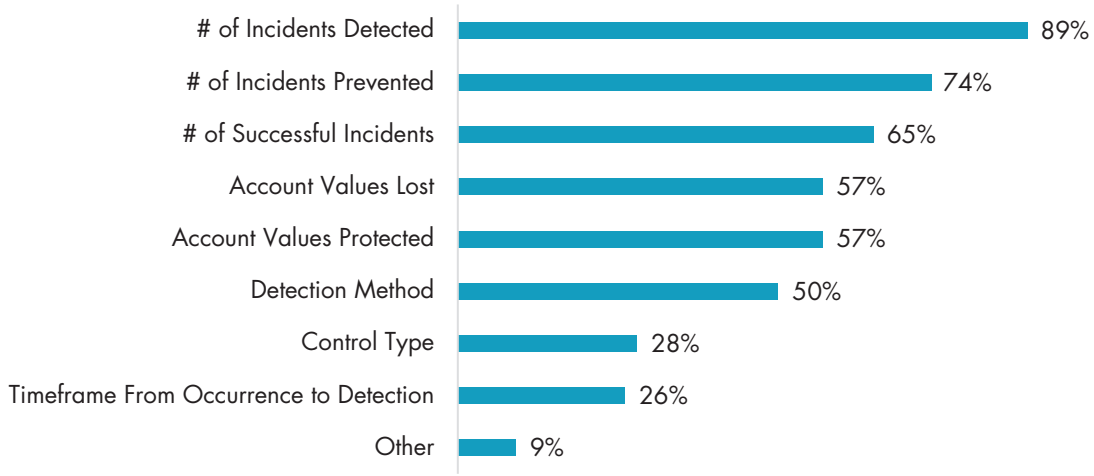
**Ryan Schwoebel, CFE, CAMS**
**SIU Director**
**Protective Life**

## Areas Participating on Oversight Committees



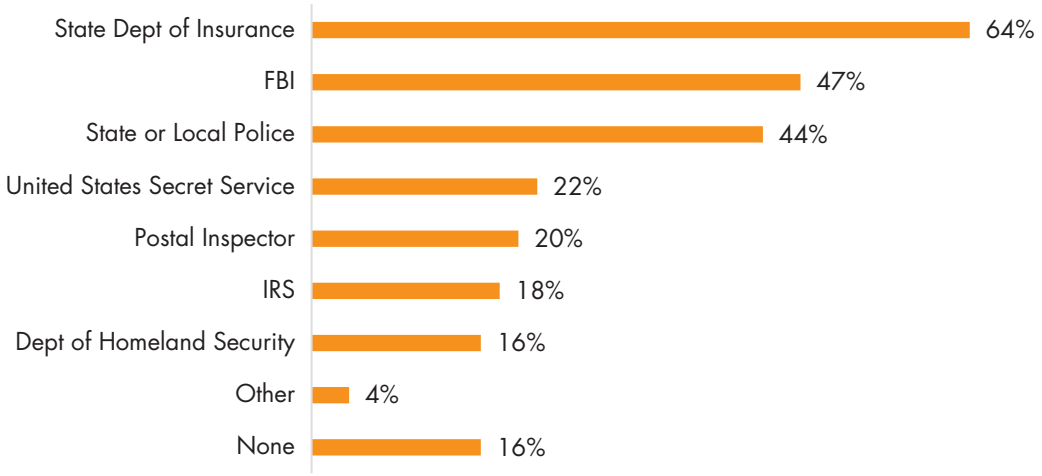

Companies employ a variety of metrics to determine the success of their programs. The most common metrics are related to incidents detected, prevented, or are successful.

## Metrics



Most all companies have a standing relationship with one or more law enforcement or government agencies. Companies also report fraud-related information to various organizations. Nearly all (91 percent) provide mandatory reporting to state insurance departments, and 4 in 10 provide discretionary reporting. Seven in 10 companies submit Suspicious Activity Reports (SAR) with the Financial Crimes Enforcement Network (FinCEN), and just 1 in 5 submit filings to the Internet Crime Complaint Center (IC3).

## Relationships With Law Enforcement



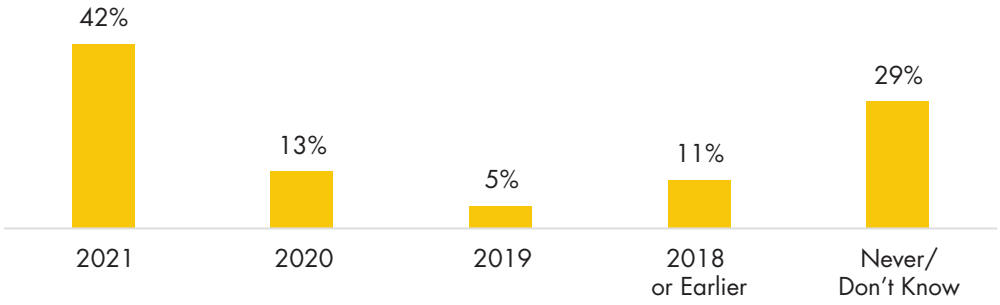

# Risk Assessments

Seven in 10 companies have conducted formal risk assessments of their financial crimes and fraud exposure. Of those that have, most did so in the past year, and just over half have made adjustments to their programs as a result, down from nearly 9 in 10 in last year's study. Fully half of smaller companies (with less than $5B in admitted assets) said they've never conducted a risk assessment or they don't know. On the other hand, half of larger companies conducted one in 2021.

**"Annual Fraud Risk Assessments are a critical component of your fraud prevention strategy. While the output is valuable, getting operational teams to think about fraud risk and controls on a regular basis is especially valuable. It promotes a broader sense of fraud risk and control ownership."**

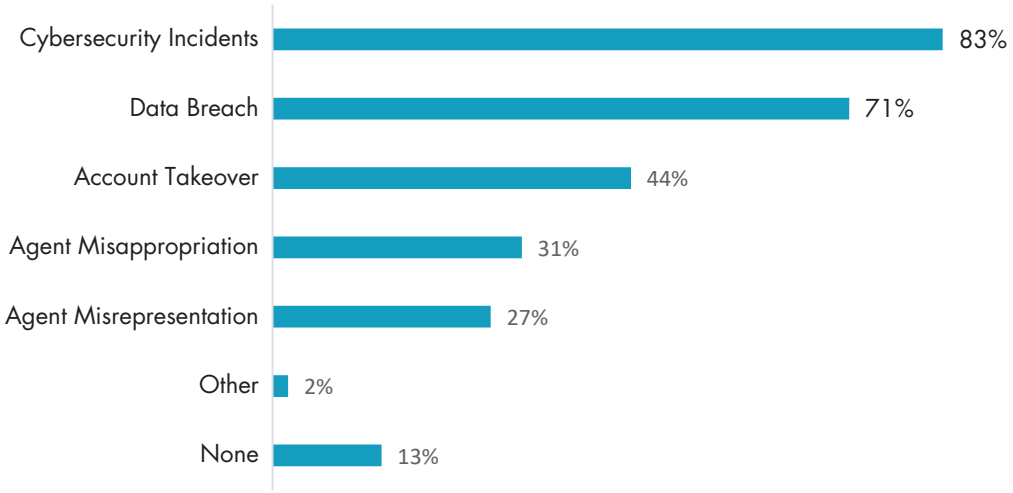
**Ken Elder**
**VP Enterprise AML Officer**
**Lincoln**

## Year of Last Risk Assessment




Six in 10 companies have a defined risk appetite, and it is likely that slightly more based the level of risk on a dollar amount, rather than reputation and brand. Risk appetites can be set by many parts of an organization, but usually involve compliance and/or risk management. Most companies mitigate their risk by purchasing one or more types of insurance.

## Commercial Insurance Coverage



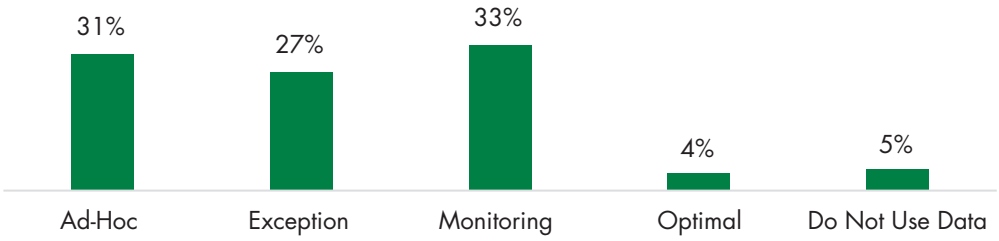
# Program Tools and Technology

Companies use a combination of people, processes, and technology to detect and prevent fraud. As in last year's study, when it comes to using data for this purpose, companies admit there is room for improvement. Smaller companies (with less than $5B in admitted assets) are more than twice as likely as larger companies to answer "Ad Hoc."

**"There's no silver bullet — if there were, everyone would be using it. It takes the right mix of internally developed and third-party tools working in combination to protect your online portals, call centers, and disbursement teams from ongoing attacks."**

**Mike Kennedy**
**Senior Director, FIU**
**Equitable**

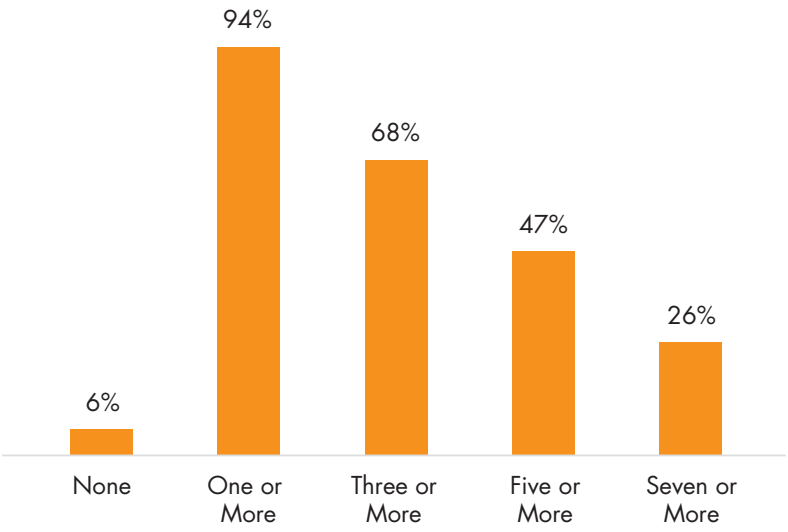
## Maturity of Use of Data in Fraud Detection and Prevention




Note: See Appendix A for definitions of data maturity categories.

The survey asked companies which of 28 tools or services they use to help authenticate customers and identify and investigate fraudulent activity. Companies collectively wrote in more than 15 additional tools, demonstrating the variety and number of tools available. Companies employing at least one tool use an average of five. Six in 10 companies are considering an average of two additional tools.

## Number of Tools Used to Identify and Investigate Fraud Activity




## Top 10 Tools Used

| | |
|---|---|
| LexisNexis Accurint | 66% |
| FraudShare | 62% |
| Refinitiv GIACT | 45% |
| Splunk | 32% |
| Tools developed in-house | 32% |
| FS-ISAC | 19% |
| Pindrop Protect | 19% |
| Fiserv Financial Crimes Risk Manager (FCRM) | 17% |
| Thomson Reuters Clear | 17% |
| TransUnion TLO | 17% |

Nearly 9 in 10 companies use one or more case management tools to manage and analyze incidents. One in 3 companies use tools they developed in-house. Other popular tools, used to a lesser degree, include Archer, SalesForce, and Service Now. One in 3 companies are considering additional tools for case management, down from nearly half a year earlier.

# Spend

Nearly all companies maintained (64 percent) or increased (32 percent) spending on fraud prevention and/or authentication capabilities in 2021 compared to 2020 and similarly plan to maintain or increase spending in 2022. Most companies that spent more in 2021 than 2020 also plan to spend more in 2022 than 2021. There is also tendency for larger companies (>$5B in admitted assets) to say they're spending more. Staffing levels for financial crimes and fraud prevention management programs correspondingly increased from 2018 through 2021. However, companies expect 2022 staff levels to remain consistent with 2021. It appears that those planning to spend more are doing so by investing in additional tools and services and not necessarily staff.

# Authentication

Companies have a wide range of available methods to choose from in authenticating customers and/or agents/advisors to their IVR systems, call centers, websites, and mobile apps, or when a user forgets their username or password. These methods may use more traditional sources such as standard identifiers (e.g., name, Social Security number, date of birth, policy or contract number) and knowledge-based questions. Or they may use more sophisticated methods that include sending one-time passcodes to a phone or email, use of an authenticator app, tools that identify the user's device as being their device, a government ID scan and selfie, analytics on user behavior patterns, technology-enabled anomaly detection, voice biometrics, and more.

## Level of Authentication Sophistication*

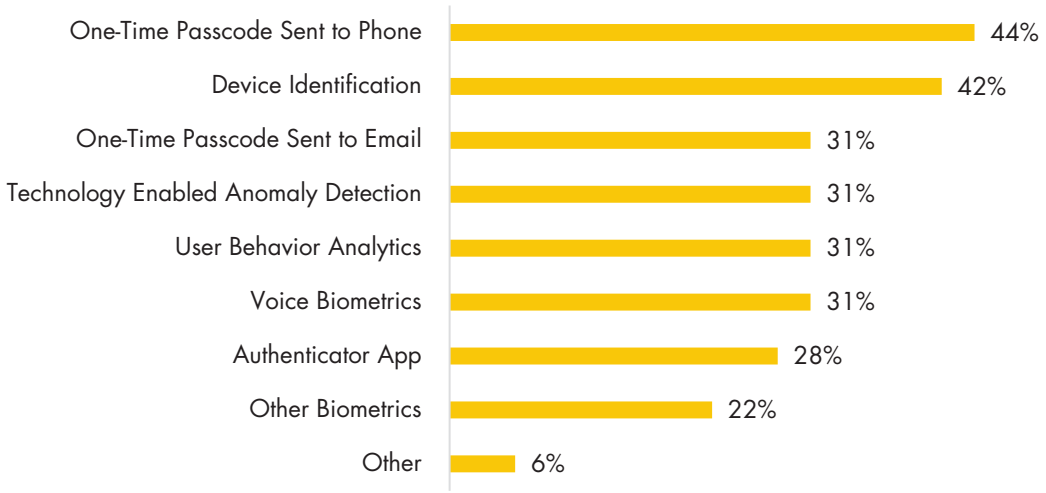
| Who | Accessing | Traditional Only** | Sophisticated** |
|---|---|---|---|
| Agents/Advisors | Mobile app | 14% | 86% |
| Customers | Mobile app | 22% | 78% |
| Agents/Advisors | Website | 29% | 71% |
| Customers | Website | 31% | 69% |
| Customers | Forgotten username or password | 43% | 57% |
| Customers | Initial registration | 47% | 53% |
| Customers | IVR | 65% | 35% |
| Customers | Call center | 69% | 31% |
| Agents/Advisors | Call center | 73% | 27% |

* Companies that do not offer access to an IVR, call center, website, mobile app, etc. are excluded above.
** As defined in above paragraph.

There is room for increased sophistication, especially when authenticating at the IVR or call center, though in the latter the company representative can play a role in watching for fraud. Multifactor authentication (MFA) is often used for access to websites and mobile apps, which accounts for a significant portion of the increase in the proportion of companies being labeled as "sophisticated" in Table 2. It's curious to see the level of sophistication when a customer first registers their online account as being somewhat lower than when customers access the website at a later date.

Many companies are considering adding sophisticated authentication capabilities. Most common are MFA and device identification. Biometric technology has also had significant advancements in recent years, and many companies are considering voice and other biometrics, including fingerprint, facial, palm print, and retinal scans.

## Authentication Capabilities Under Consideration




Companies increasingly are enabling customers to perform various transactions online. Currently, companies appear more comfortable with customers making changes (address, bank account, beneficiary) to their accounts than requesting withdrawals. Similarly, companies are more likely to be adding the ability for customers to make changes than to take withdrawals.

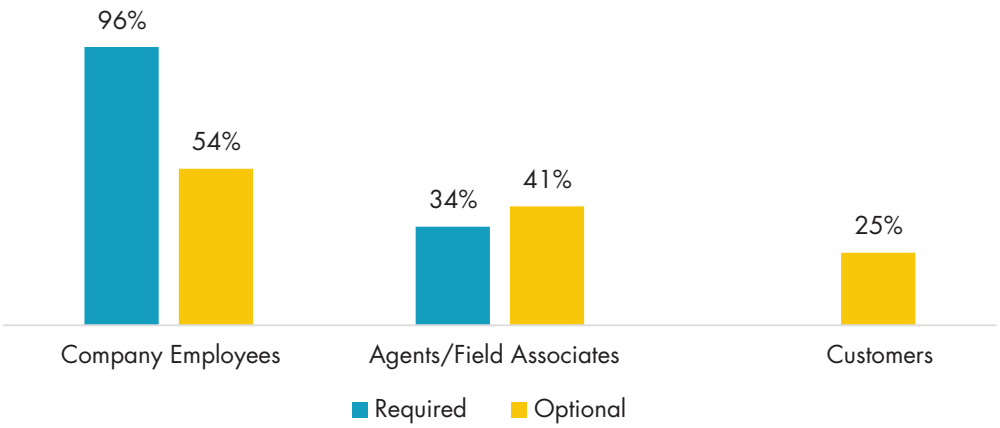
## Online Transaction Capabilities

| | Current | Anticipated |
|---|---|---|
| **Changes to ...** | | |
| **Address** | 67% | 38% |
| **Beneficiary** | 46% | 45% |
| **Bank Account (Incoming Payment)** | 46% | 30% |
| **Bank Account (Outgoing Withdrawals)** | 35% | 25% |
| **Withdrawals** | | |
| **Check (Under a Certain Amount)** | 29% | 21% |
| **EFT (Under a Certain Amount)** | 27% | 26% |
| **Check (Any Amount)** | 21% | 19% |
| **EFT (Any Amount)** | 23% | 19% |
| **None of the Above** | **29%** | **45%** |

# Training and Awareness

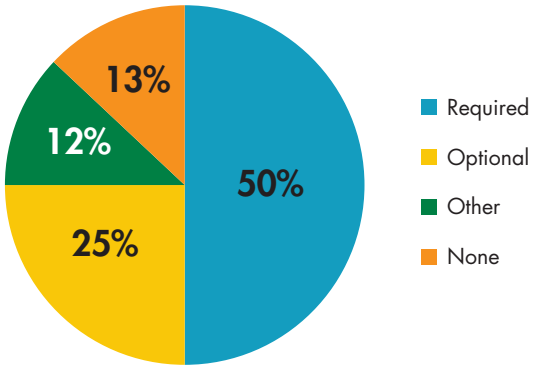
Nearly all companies require training for company employees, and 1 in 3 require it for agents/advisors and/or field associates. Companies may otherwise provide optional training for all or for those not required to undergo training on financial crimes and fraud awareness. Just 1 in 4 companies offer regular training or educational materials to customers, including policy/contract owners, plan participants, and/or plan administrators and sponsors. A few companies will require training for other organizations that have access to customer data, including vendors, contractors, and third-party administrators. Training provided to employees and agents/agent support staff is most commonly no more than five hours per year.

## Required or Optional Training Provided




Beyond standard training, most companies provide impromptu training after a significant fraud event has occurred to ensure staff are aware of new fraud schemes and how to watch for red flags.

## Impromptu Training After Fraud Events



# Challenges and Outlook

A company cannot simply build a fraud prevention and management program and then sit back and let the program do its thing. There is always room for improvement, and, more importantly, companies must remain vigilant as bad actors continue to think of new ways to commit fraud.

## Top Areas of Focus for 2022

| | Top Priority | One of the Top Three Priorities | Overall Rank |
|---|---|---|---|
| Authentication Process and Control Enhancements | 39% | 65% | 1% |
| Digital Fraud Process and Control Enhancements | 15% | 41% | 2% |
| Training and Education for Employees | 11% | 48% | 2% |
| Technology — Internal Solutions | 6% | 26% | 4% |
| Disbursement Process and Control Enhancements | 4% | 24% | 5% |
| Centralizing the Organizational Structure | 7% | 15% | 6% |
| Governance Model | 7% | 13% | 6% |
| Technology — External Solutions | 4% | 15% | 8% |
| Training and Education for Agents/ Field Representatives | 2% | 13% | 9% |
| Enhancing Management Reporting | 2% | 9% | 10% |
| Update Your Current Fraud Risk Assessment | 0 | 17% | 10% |

Note: Overall rank was determined by assigning 3 points to a top priority, 2 points to a second priority, and 1 point for a third priority.

The survey asked companies to list their top three exposures and challenges in 2022. Exposures mentioned most frequently are: account takeovers, claims fraud, and agent misconduct. Top three challenges are technology, resources, staying current. Continuing to prevent account takeovers and claims fraud are the top areas companies are concerned about potential exposure and continue to face challenges with effectively implementing technology and garnering the resources — both financial and human — to ensure their fraud protection and management programs remain strong.

A slight majority of companies believe the insurance and retirement services industry is keeping pace with other industries with it comes to utilizing tools and technologies to combat fraud. Those who feel otherwise suggested actions the industry could take to better combat fraud. Top themes include 1) more and faster collaboration across the industry, 2) better leveraging of technology, including use of artificial intelligence and behavioral analytics, along with transitioning away from legacy systems, and 3) implementing more cost-effective solutions.

## Top Exposures and Challenges of 2022

| Exposures | Mentions | Challenges | Mentions |
|---|---|---|---|
| Account Takeovers | 24% | Technology | 24% |
| Claims Fraud | 11% | Resources | 20% |
| Agent Misconduct | 8% | Staying Current | 15% |
| Elder Financial Exploitation | 8% | Authentication | 10% |
| Cybersecurity Incidents | 7% | Education | 8% |
| Familiar Fraud | 5% | Employee Turnover/Vigilance | 8% |
| Application Fraud | 5% | Customer Experience | 6% |

Note: Companies mentioned a total of 132 exposures and 79 challenges. The numbers in the table represent the percent of mentions in a given category.

# Appendix A — Definitions

## Fraud Categories

**New Business/Application Fraud —** Agent or customer intentionally providing false information, or omitting or understating material information to obtain an insurance policy or securities account that would not have been approved during the policy underwriting or account application processes if accurate and/or complete information had been provided.

**Agent Fraud —** Any fraudulent activity undertaken by the agent to increase their compensation or receive funds and/or misrepresent product or service terms or conditions for personal gain.

**Account Takeover (Related) —** Unauthorized attempt to access a customer account by a related party (e.g., family member, friend, caregiver, etc.) impersonating the customer to fraudulently obtain data or funds.

**Account Takeover (Unrelated) —** Unauthorized attempt to access a customer account by an unknown and unrelated third-party impostor to fraudulently obtain data or funds.

**Senior and Vulnerable Adults (Related) —** A person with functional, physical, or mental inability to care for self or someone who is unable to protect themselves against harm or financial exploitation perpetrated by a known or related individual (e.g., family member, friend, or caregiver).

**Senior and Vulnerable Adults (Unrelated) —** A person with functional, physical, or mental inability to care for self or someone who is unable to protect themselves against harm or financial exploitation perpetrated by an unknown or unrelated party. Example: A fraudster contacts or befriends the victim and executes a confidence scam (e.g. romance, IRS, help desk, or lottery).

**Vendor Impersonation —** Impersonations of a company vendor or supplier to obtain company funds or data. Example: A fraudster submits bogus invoices or updates legitimate invoices with their bank information to redirect payments to an account they control.

**Employee Impersonation —** Impersonation of an employee to obtain the employees data or to redirect payroll or expense reimbursements. Example: A fraudster impersonates an employee and contacts the HR department to update the employee's banking information to an account the fraudster controls.

**Company Impersonation —** Impersonations of company or associated party (employee, agent, vendor) to obtain information or funds from an individual or company that may or may not be a customer or employee of the company. Example: A fraudster calling random people impersonating your company to obtain their personal data and\or account information.

**Check Fraud (Company) —** Intentionally forging check signatures or endorsements, altering check payees, or creating unauthorized checks for the purpose of fraudulently obtaining company funds. Example: A fraudster creates counterfeit checks using your company's name and banking information and uses them to purchase goods from someone they met on social media.

**Check Fraud (Customer) —** Forging check signatures or endorsements or altering check payees for the purpose of fraudulently obtaining customer funds. Example: A fraudster obtains a legitimately issued check payable to a customer and alters the payee's name in order to cash it.

**Money Laundering —** Engaging in acts designed to conceal or disguise the true origins of derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins and constitute legitimate assets (only confirmed).

**Claims Fraud —** Intentionally submitting false or misrepresented information to generate or support a claim (all life, health, disability, annuity, and retirement services products).

**Internal Fraud —** Fraudulent acts perpetrated by employees or contractors to obtain company or customer data and/or funds.

## Program Maturity

**Ad Hoc —** Fraud events handled in a reactive and ad hoc manner at the local level with minimal documented policies or procedures.

**Initial —** Fraud events are handled in a reactive manner at the local level with some enterprise-wide coordination, policies and procedures are documented. Fraud controls are mainly detective and risk assessment process is ad hoc (if existent).

**Operational —** Fraud events are handled in a coordinated manner with documented policies and procedures. Fraud controls are documented and consist of both detection and prevention. There is an enterprise perspective with at least some governance and risk.

**Optimal —** A defined governance and risk assessment process drives the Financial Crimes and Fraud prevention program with an enterprise perspective. Procedures, policies and controls are well documented with a focus on prevention and continual improvement.

## Data Maturity

**Ad Hoc —** Basic reporting provides raw data for human analysis

**Exception —** Alerts generated based on known exceptions or threat indicators

**Monitoring —** Alerts generated based on trend and pattern analysis that detect unusual interactions and\or transactions

**Optimal —** Program utilizes advanced analytics to identify or predict fraudulent activity in near real time

# Appendix B — Participating Companies

Allianz Life Insurance Company of North America

American Family Life Insurance Company

American Farmers & Ranchers Mutual Insurance Life Company

American Savings Life Insurance Company

Athene Annuity & Life Company

Brighthouse Financial

Catholic Life Insurance

Catholic Order of Foresters

Catholic United Financial

Charles Schwab & Co., Inc.

CMFG Life Insurance Company

CNO Financial Group, Inc.

ELCO Mutual Life & Annuity

Equitable

Equitrust Life Insurance Company

Everlake Life Insurance Company

Farm Bureau Life Insurance Company of Michigan

Foresters

Gleaner Life Insurance Society

Global Atlantic Financial Group

Guardian Life Insurance Company of America

Guggenheim Life & Annuity

Homesteaders Life Company

Illinois Mutual Life Insurance Company

Jackson National Life Insurance Company

John Hancock Financial Services, Inc.

KSKJ Life, American Slovenian Catholic Union

Lincoln Financial Group

Loyal Christian Benefit Association

Massachusetts Mutual Life Insurance Company

National Farm Life Insurance Company

National Life Insurance Company

Nationwide Financial

New York Life Insurance Company

Northwestern Mutual Life Insurance Company

Ohio National Life Insurance Company

OneAmerica Financial Partners, Inc.

Pacific Life Insurance Company

Polish Falcons of America

Protective Life Insurance Company

Prudential

Sammons Financial Group

Securian Financial Group

Southern Farm Bureau Life Insurance Company

Standard Insurance Company

Sun Life Assurance Company of Canada (US)

Symetra Financial

T. Rowe Price Group

Talcott Resolution Life Insurance Company

Tennessee Farmers Life Insurance Company

The Canada Life Assurance Company

Thrivent Financial for Lutherans

Transamerica Life Insurance Company

Venerable Annuity

Voya Financial, Inc.

Western & Southern Financial Group

# Maximize the Value of LIMRA Research

Access our research findings to develop and execute effective business strategies for engaging today's ever-changing markets. You can identify growth opportunities and monitor key trends with our unbiased quantitative and qualitative research.

***Additional ways you can take advantage of research capabilities include:***

### RESEARCH FOLLOW UP

Do you have a question about the research? Contact our researchers directly for additional insight, data runs and analysis, and/or implications.

### CUSTOM RESEARCH

Has the research raised new questions that could be answered by a customized study, or do you have other research projects? For additional information, contact Dararith Ly at DLy@limra.com or Lynn Ferris at LFerris@limra.com.

### CONSULTATION

Are you wondering how to integrate the findings into operational and/or marketing strategies? For more information, contact your Client Relationship Manager.

### WEBINAR

Would your company benefit from a presentation by the researcher? You can meet virtually with the researcher or other topical experts to discuss findings and answer specific questions.

### INFOCENTER REQUESTS

Searching for additional material on a topic? The InfoCenter staff is available to help you. Contact infocenter@limra.com.

***Connect With LIMRA***




0550-2022 50700-10-730-10007