The Experts Weigh In

AML Insight, Advice and Best Practices for Insurance Companies

fiserv.

It's been more than a decade since the Financial Crimes Enforcement Network (FinCEN) labeled certain insurance products "vulnerable" to money laundering and required insurers develop anti-money laundering (AML) programs. Still, insurance companies have not yet attracted regulators' attention in the same way as other financial services industries.

However, that seems to be changing. Insurers are seeing increased scrutiny and enforcement actions globally. They are understandably concerned about risks to their reputation as well as the potential for suspension, censure, fines and criminal prosecution. One of the primary challenges is how to balance regulatory requirements with efficiencies in operations and technology to help reduce rising compliance expenses.

Experts in AML for the insurance industry are ready with answers to some of the most pressing questions, including:

- How do insurance companies address the burden of AML mandates, evolving regulations and rising operational costs?
- How can compliance departments gather the intelligence to channel limited investigative resources where they are most needed?
- What are the hallmarks of an effective financial crime management solution?

Today, FinCEN establishes agreements with state insurance regulators to assess insurance or annuity issuers' AML programs as part of regular examinations.

How AML Compliance Is Changing in the Insurance Industry

Despite the role insurance products can play in facilitating money laundering schemes, there are fewer AML "best practices" in the industry than in banking or other financial services. The insurance industry's inconsistent approach to AML is due in part to the decentralized regulatory guidance and enforcement. That creates a problem for insurance companies as they navigate the increasingly complex challenges presented by money launderers and fraudsters.

"Absent such guidance, many insurance companies face the unenviable prospect of determining the effectiveness of their AML program in a vacuum," said Vicki Landon, president of Landon Associates, a consultancy specializing in anti-money laundering and terrorist financing in the insurance industry.

Previously, FinCEN tasked the IRS with evaluating the AML programs of insurers and annuity providers. Today, FinCEN establishes agreements with state insurance regulators to assess insurance or annuity issuers' AML programs as part of regular examinations.

The scope of such AML-related examinations varies by state. When examiners uncover problems or deficiencies, they provide that information to FinCEN and the IRS. Landon predicted regulators will get better at uncovering evidence of money laundering.

"As state examiners become more accustomed to scrutinizing AML programs, and providing their findings to the federal government improves," she said, "we'll likely see more insurance companies and annuity providers subject to the fines and penalties that come with noncompliance."

Inevitably, for many, confusion reigns regarding what constitutes enough compliance. Despite the best intentions of compliance executives, insurance companies face the real prospect of over- or under-investing in AML compliance. Yet striking the right balance in AML compliance is important because most insurers lack sufficient budgets and resources to spend on less than optimal programs.

"In addition to mixed signals stemming from a lack of regulatory activity and the delegation of law enforcement by the federal government to state insurance regulators, insurance companies must contend with legacy technology systems that make the extraction and analysis of data a challenging undertaking," said Andrew Davies, vice president of Financial Crime Risk Management for Fiserv.

With the specter of increased oversight by state insurance regulators on the horizon, insurers are struggling to optimize their approach to financial crime management while simultaneously looking for ways to minimize their compliance costs.

"An AML scenario focused on customer activity may uncover agent activity indicative of fraud."

- Pierre Isensee, Business Consultant, Financial Crime Risk Management, Fiserv

You Can't Detect Crime Without the Right Detection Scenarios

Effectively detecting money laundering, or any form of financial crime related to insurance products, depends on access to a technology solution purpose-built for the insurance industry and tailored to an individual company's tolerance for business risk. That includes providing access to industry-proven scenarios and the flexibility to evolve detection strategies as dictated by changes in the business and risk environment.

When companies employ a risk-based approach to financial crime management, they direct precious resources where they can accomplish the most good and generate the highest return on investment, said Pierre Isensee, a business consultant with Financial Crime Risk Management at Fiserv.

"Risk-based compliance," he said, "also helps companies avoid the need to hire large teams of investigators to monitor unfiltered and often innocuous suspects that arise from false positives."

While the acceptable level of false positives varies by company, inundating investigators with an excessive number of suspects is never the goal.

"Yet ultimately," Isensee said, "companies, not the technology provider, need to decide where their tolerance for risk and false positives lies."

Davies said he also sees the merits of a risk-based approach.

"The development of risk scores allows investigators to channel their efforts toward the management of the greatest risk," he said, adding that an AML technology solution should address insurance products' unique challenges, including terminology specific to those products and markets.

AML and other types of fraud detection rely on similar data and processes, so insurers can generate efficiencies by centralizing those programs.

"An AML scenario focused on customer activity may uncover agent activity indicative of fraud," Isensee said.

Consequently, when insurance companies invest in a financial crime management solution rather than technology designed to unmask only money laundering, they generate a much more compelling return on investment.

Still, Isensee advised insurance companies to proceed with caution as they develop scenarios to uncover money laundering or fraud.

"It takes time to create a scenario that reflects a company's risk tolerance, proves effective in detecting suspicious activity and produces the desired false-positive rate," he said.

Depending on the complexity of a new scenario, Isensee said, development takes one to two days to discuss and document, one to two days to implement and four to six weeks of testing to optimize before the new scenario enters production.

He also offered guidance for insurance companies regarding the number of scenarios to employ.

"Generally, insurance companies utilize 15 to 20 scenarios, leaving room to add well-thought-out additions," Isensee said.

With respect to the split between customer and agent risks, he said he typically sees insurance

companies use 10 to 15 scenarios to examine customer risk, with the remaining five to 10 scenarios focused on agents and agencies.

A Modern Approach to AML Compliance Can Ease the Burden

So how do insurance companies create a new program, or improve an existing one, to combat money laundering and fraud?

"A modern approach to AML and fraud detection starts with a technology provider that knows how to position your company to stay in compliance and stay one step ahead of criminals," Davies said. "A provider needs expertise related to the extraction and aggregation of data from existing systems and mapping of data into the technology solution. The provider should also have a comprehensive understanding of the insurance industry and how scenarios align with your company's risk assessment."

Yet he acknowledged the inherent challenges insurance executives must overcome as they tackle financial crime.

"Many insurance companies maintain multiple technology platforms," Davies said. "Data is often organized at contract level rather than client level, which complicates the application of analytical techniques to uncover money laundering schemes. Sometimes, the data is just missing or unreliable."

As a result, he stressed the need for a technology solution that can import data from disparate sources and conduct analytics to determine the integrity of the data.

As it relates to how a financial crime management solution functions, Davies said, the hallmarks of an effective platform include the flexibility to monitor the activities of an agent, an employee, a policyholder and related parties. So, whether activity involves AML, fraud, market abuse, product suitability or vulnerable-adult abuse,

"Data is often organized at contract level rather than client level, which complicates the application of analytical techniques to uncover money laundering schemes. Sometimes, the data is just missing or unreliable."

– Andrew Davies, Vice President, Financial Crime Risk Management, Fiserv

compliance departments can target the solution as needed.

In addition to flexibility, Davies said, the right solution includes a library of detection scenarios and techniques, created specifically for the insurance industry.

"AML solutions oriented toward depository institutions do not include specific scenarios for insurance products," he said. "As a result, they fall short of delivering an effective approach to AML and fraud detection as well as market abuse and product suitability."

Further, a solution must include typologies around investment products. They involve a low volume of transactions, and, therefore, require a different type of analysis.

When it comes to assessing the effectiveness of efforts to combat financial crime, a solution should produce metrics, including reports on the relationship between policies, alerts, cases and suspicious activity, as well as an analysis of the false-positive ratio. That type of reporting lets insurance companies demonstrate their commitment to compliance to regulators.

"In the absence of consistent regulatory guidance, many insurance companies struggle to determine what constitutes an acceptable approach to financial crime risk management," Davies said. "Using a technology solution custom-built for the insurance industry, in concert with a risk-based approach to detection, can help detect suspicious activity involving employees, agents and policyholders quickly and with minimal customer friction."

Meet the Experts

Pierre Isensee

Business Consultant, Financial Crime Risk Management, Fiserv

Isensee has more than 15 years of experience in technology business consulting. He is an industry expert on the current anti-money laundering requirements. As a Fiserv business consultant, he is focused on supporting Fiserv clients and defining and building risk and regulatory frameworks specific to their business.

Vicki Landon

President, Landon Associates, Inc.

Landon is the founder of Landon Associates, Inc., which provides AML and fraud services to life insurers.

Experienced in delivering independent AML audits, risk assessments, AML/fraud consulting services and AML transaction management solutions, Landon has more than 25 years of industry experience, including senior and executive positions with Aquilan, IBM and Continuum (now DXC).

Andrew Davies

Vice President, Global Market Strategy, Financial Crime Risk Management, Fiserv

Davies has 25 years of experience in financial services and risk management, with particular focus on AML, fraud, risk management, settlement risk and payment processing. He is responsible for working with Fiserv customers around the world to design and deploy effective financial crime risk management solutions. Davies has experience working for and with organizations such as Nomura, the Federal Reserve Bank of New York, the Continuous Linked Settlement Bank, ING, Sun Life, Manulife Financial, Citizens Bank, Deutsche Bank and the Bank of Tokyo-Mitsubishi.

Connect With Us

For more information about detecting and preventing financial crime, call 800-872-7882, email getsolutions@fiserv.com or visit www.fiserv.com.

About Fiserv

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today. Visit fiserv.com and fiserv.com/speed to learn more.

Fiserv, Inc.
255 Fiserv Drive
Brookfield, WI
53045

800-872-7882
262-879-5322
getsolutions@fiserv.com
www.fiserv.com