NICSA

An Asset Management Association For All

Best Practices in Fraud Prevention

RESEARCH NOTES

By NICSA's Compliance & Risk Management Committee

Social Engineering Recognition and Response

NICSA explores how asset managers and other financial institutions are implementing new initiatives, developing businesses responses, and crafting best practices in the fraud prevention arena.

Best Practices in Fraud Prevention

By NICSA's Compliance & Risk Management Committee

Social engineering can be described as a combination of social and psychological information gathering techniques that are used to manipulate people for nefarious purposes. Social engineering exploits the natural human tendency to be helpful, and as such has made its way to the front lines of the financial services industry: the contact center.

Asset managers and other financial institutions are looking for innovative ways to protect themselves from social engineering and other types of fraud. Fraud is becoming more complicated, more sophisticated, and more prevalent, making the development of best practices increasingly challenging. Weak security measures can put fraudsters in a position to exploit vulnerable shareholders.

Contact centers have the opportunity to be part of the solution through rigorous training, ongoing communication and industry-wide collaboration. This report is offered as a framework to asset managers and service providers to evaluate their best practice guidelines as they pertain to fraud prevention, recognition and response.

COMMITTEE OVERVIEW

The **NICSA Compliance & Risk Management Committee** serves as a resource for the NICSA community by providing access to information and education focused on regulatory compliance and the management of risk in the fund industry.

COMMITTEE MEMBER FIRMS:
ACA Compliance Group
American Century Investments
American Funds
Amundi Pioneer Asset Management
Citi
Deloitte
DST Systems, Inc.
DWS
Eaton Vance Management
Ernst & Young LLP
Fidelity Investments
FIS
Franklin Templeton Investments
MFS
Northern Trust Company
OppenheimerFunds
Putnam Investments
PwC
State Street Corporation
T. Rowe Price
Thrivent Financial Investor Services
Vanguard Group, Inc.
Voya Investment Management

Know the Landscape

There are many examples at the state and federal level of legislation supporting the limitation of fraud within the asset management industry. States in particular, with the help of the North American Securities Administration Association, have been proactive in creating fraud awareness training and protections over the last few years. The federal government is also getting more involved in fraud prevention, particularly in the area of elder exploitation. For example, FINRA recently amended Rule 4512 to require member firms to make reasonable efforts to obtain contact information for trusted persons from shareowners opening accounts. More recently, FINRA Rule 2165 became effective, permitting firms to place holds on disbursement for shareholders over the age of 65 if exploitation is suspected. Further, to support asset managers in this same context, the SEC recently granted no action relief permitting funds and their transfer agents to delay disbursements as well. It is critical for executive teams across the asset management industry to not only understand the impacts of state and federal regulations on their lines of business, but to understand the role of financial institutions in the fight against fraud.

Define the Target

One of the first steps in preventing fraud is recognizing the target. Asset management industry participants need to clearly define what a "vulnerable shareholder" may look like for their business (be it senior investors, lost shareholders, etc.). Identifying the key characteristics for "at risk clients" is essential, as is assessing these vulnerabilities on an ongoing basis.

In addition to documenting all policies and procedures, regular training sessions should be held with front-line staff in order to stay up-to-date on trending types of abuse and scams targeting vulnerable shareholders. New employee training as well as ongoing processes where information about fraud trends is shared in real time can be effective tools against fraud.

Balance Service with Skepticism

Contact centers are trained to provide the highest level of personalized service. As a result, bad actors have homed in on contact centers to exploit that customer service attitude. Social engineering fraudsters are adept at manipulating the psychological human tendency to be sympathetic—via contrived time pressures or emotional circumstances—which may lead to agents bypassing internal protocols in an effort to be helpful. A key hurdle in the fight against fraud, particularly where social engineering is concerned, is the inherent conflict between training contact center agents to provide a premier level of service, while at the same time asking them to be skeptical

and inquisitive.

Knowing the red flags can be critical in managing the conflict between service delivery and risk mitigation. Creating a culture where there is a balance of service with skepticism can help agents to move into a place of inquisitiveness.

Provide an Avenue for Escalation

Training agents to recognize the patterns of account activity that can add up to fraud over time (for example, multiple inquiries to the contact center coupled with a recently established online log-in, a recent address change, an update of banking information, and/or the addition of e-delivery to the account) can be an essential best practice in fraud prevention. Agents need to be well positioned, via training and information sharing, to recognize these combinations and patterns.

Once suspicious patterns are identified, having a clear avenue of escalation is key. Providing contact center agents with a process to escalate suspicious activity can have a significant impact on fraud prevention success rates. Some industry participants report having multiple levels of agents, including top-level specialists trained to address suspicious requests. This type of structure can funnel all suspicious activity through a smaller group of more experienced employees who are well versed on the latest fraud trends.

Explore Technology Solutions

The deployment of new technologies has, in many respects, opened the door to greater opportunity for fraud. Deployment and testing phases can be particularly prone to enhanced risk. Technology can, however, play an essential role in developing effective end-to-end fraud prevention processes. Tech applications are increasingly being utilized to combat the fraud epidemic, and can be a vital tool in the fight against social engineering.

Source: Nuance Internal Customer Research 2016

Biometrics is one such example. One of the most prevalently used forms of biometrics in the contact center is voice biometrics. Often deployed in initial live conversations with agents, a voice biometric engine can create a voice print for shareowners opening an account. Typically used in conjunction with legacy authentication processes, a voice biometric engine can help to validate the shareholder's identity on future calls. Beyond the contact center, behavioral biometrics can help to validate the identity of individuals behind electronic devices – such as smart phones, tablets, laptops and desktops. While cost/benefit analyses of deploying technology solutions may differ by firm, evaluating evolving technological capabilities can help firms make informed decisions when it comes to developing the systems to secure their financial services across customer care channels.[1]

Support Industry Collaboration

Internal information sharing is critical to ensuring that contact center agents recognize red flags and understand firm policies around fraud response. Encouraging staff to share live examples in real time is key. To that end, many firms are creating internal working groups around fraud, engaging executives across business disciplines.

Industry wide collaboration, however, can be more challenging. However, many NICSA member firms agree that information sharing across firms is necessary in order to effectively develop predictive mitigating controls around fraud. Several industry programs exist that act as forums for this type of exchange. Further, some large BPO organizations within the industry are reporting plans to sponsor client working groups in order to engage on best practice development.

Investor fraud is an industry issue, and should not be viewed solely from a single-firm perspective. There are a multitude of opportunities to get an understanding of what other companies are doing to protect vulnerable shareholders—including continuing education via conferences, webinars and networking events across the industry. Communicating about effective solutions among industry participants can help the industry succeed in protecting assets and shareholders.

As an industry trade association, NICSA hopes that the sharing of best practices and evolving technologies aimed at combating this issue sparks constructive dialogue and furthers the ability to fight fraud across the industry.

NICSA supports a wide variety of topic committees, allowing our members to have impactful participation, make meaningful contributions, and have their voices be heard. This briefing spotlights NICSA's Compliance & Risk Management Committee and the productive work that team is doing. Join the conversation today. Contact NICSA to see how to become a member in any of the following committees:

Compliance & Risk Management | Data Analytics | NextGen | Product & Distribution

Retirement | Technology & Innovation | Transfer Agent | UIT

Tel: 508.485.1500 • NICSA.ORG

[1] Source: Information obtained from Nuance, a provider of multi-modal biometric authentication.