NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement

How to create and maintain the optimum fraud prevention solution for your business

Nuance Guest Blogger

12 February 2019

To make the most of Nuance fraud prevention solutions, you need to consider a variety of issues related to your business and the types of fraud to which it's exposed. Nuance guest blogger, Iam McGuire, explores characterizing your organisation's attitude to fraud, assessing your fraud landscape, weighing the benefits of offline and real-time fraud detection, understanding the fraud attack cycle, maximising the value of alerts and management information - including optimising watchlist management, analysing your data and prioritising alerts, and capturing the richest possible metadata – and evolving your defences in line with changing fraud behaviour.

Personal identity numbers (PINs), passwords and security questions have had their day. A constant barrage of data breaches has led to widespread compromise of personal data and user credentials, causing many businesses to rethink their approach to customer authentication and fraud prevention within their customer care channels.

As a result, increasing numbers of enterprises are turning to solutions such as Nuance Security Suite to replace these credentials with voice biometrics and other characteristics that are much harder for fraudsters to compromise. To make the most of these solutions, you need to consider a variety of issues related to your business and the types of fraud to which it's exposed.

Characterising your organisation's attitude to fraud

It might seem obvious that any fraud prevention solution would aim to minimise an enterprise's losses due to fraud. But different organisations can have widely differing attitudes to the levels of fraud they're willing to accept in order to balance security and the customer experience.

If you implement extremely tight security controls, this will often create an unfriendly customer experience that can negatively affect your brand. Whereas, making the customer experience as simple as possible may leave gaps in your defenses for which you'll have to accept a certain level of losses. You'll therefore want to implement a solution that achieves the optimum balance between minimising fraud losses while not impinging customer service.

Assessing your fraud landscape

Many organisations have a wildly inaccurate understanding of their 'fraud landscape', and so find it very difficult to make fraud-related decisions based on sound financial information. Establishing a clear picture of this – including the levels of fraud and nature of the attacks you're experiencing – allows you to sanity check the scale of your fraud problem; whether the cost of fraud is acceptable; how and where Nuance can help you reduce the attacks and losses you're suffering; and the implications of your risk appetite when it comes to striking the right balance between security and quality of the customer experience.

Weighing the benefits of offline and real-time fraud detection

Understanding the nature of your fraud landscape will let you determine whether improving your 'front door' security through voice biometrics authentication will help, how much, and also whether you need real-time detection or if the fraud you're experiencing can be managed offline.

Many enterprises have achieved rapid reductions in fraud losses through offline fraud detection. This is also typically the easiest to deploy, so you may choose to implement an offline solution while looking to roll out real-time detection and authentication through a strategic deployment plan.

Understanding the fraud attack cycle

Fraudsters tend not to perform a single attack on an organisation, but do so repeatedly, with each attack having multiple steps. Another way of thinking about reducing fraud losses is therefore through this 'fraud attack cycle' of data acquisition, reconnaissance, setup, cash out, laundering and access to cleaned funds.

Nuance FraudMiner™ can detect fraud during the reconnaissance, setup and cash out phases; and offline detection can also be used during reconnaissance and setup, thereby reducing the need for real-time detection at the point of cashing out.

Maximising the value of alerts and management information (MI)

While the initial focus of data gathering is to enhance understanding of the fraud landscape, once offline and/or real-time fraud detection has been implemented, this then switches to MI dealing with the specific threats to which your business is exposed – including optimising watchlist management, analysing your data and prioritising alerts, and capturing the richest possible metadata.

Evolving your defences in line with changing fraud behaviour

Nuance Security Suite delivers omnichannel security and fraud prevention across digital, telephony and self-service channels. But as consumers and enterprises increasingly adopt these solutions, fraudsters will inevitably divert their attention to trying to compromise the biometrics involved. This is why Nuance is constantly developing new technologies to mitigate and prevent these attacks.

To find out more about how to create and maintain the optimum fraud prevention solution for your business, see a recent *Wall Street Journal* article on fraud prevention at Royal Bank of Scotland

Ian McGuire *joined Nuance in 2012 as a Business Consultant. He provides insight and strategic guidance to clients regarding their deployment of natural language call steering, speech self-service and, in particular, authentication solutions. Ian's skillset covers the whole spectrum of speech technologies, but in recent years he has been focused on voice biometric authentication and counter-fraud solutions. He has worked with government agencies, major banks and leading telecom providers, to develop customer experience, security and communication strategies for the successful deployment of their voice biometric solutions. Notable highlights include the launch of voice biometric authentication for HMRC, HSBC Group, Natwest, Lloyds, Coutts, and TalkTalk.*

Tags:

More Information

Want to find out more about solutions in Financial Services?

Get our latest resource: download the White Paper "Fraud prevention best practice toolkit" on how to create and maintain the optimum fraud prevention solution for your business, using practical steps and best practices based on the experiences of leading financial organisations

Learn more