NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement

Client Insights & Intel, part 3: Fidelity Investments combats fraud to protect the business and its customers

Brett Beranek | Vice President & General Manager, Security & Biometrics

23 June 2020

The volume of fraud attacks has increased tremendously over the previous few weeks – with increases ranging from 200% - 400%, depending on the industry. While fraudsters are persistently changing and adapting their tactics during the pandemic, organizations like Fidelity Investments are finding the balance between nefarious activity and legitimate transactions, while continuing to deliver superior customer service.

As part of our "***Client insights and intel***" webinar series, I recently had the pleasure of interviewing Mark DiMarzio, VP Risk of Fidelity Investments, during a virtual fireside chat. Mark spoke about business practices to address increases in fraud volume, thinking through fraud verification and alert processes, and how to help his team understand patterns of activity so they can better identify legitimate calls verse fraudsters.

During our conversation, Mark touched on working remotely, social engineering, identify theft, watch lists, voice biometrics, and other timely topics in the changing landscape of COVID-19. Leveraging Nuance's biometric and fraud miner solution, Fidelity "lets their agents do their job." Implementing both real-time and offline fraud detection, Mark covered a variety of the technology's features and benefits. When asked about the value and issue fraud detection, and prevention technology solved both on the customer and fraud side, Mark responded: "Anytime I can have technology implemented that is for the purpose of customer service, but also affords me the ability to be better at my job and preventing fraud, I will give my blessing and get out of the way."

With so many great topics, we, unfortunately, were not able to get to all the questions. However, two that I felt were important to address, and which Mark was kind to answer post-webinar:

1. **[Client Question]** Mark, do you have a different approach for retail account clients vs. institutional clients (i.e., an authorized person acting on behalf of an entity)?

[Response from Mark DiMarzio] We do. The risk is managed differently in a couple of ways. For institutional clients who are authorized to act on behalf of one of their clients/employees, they are given their own separate website to transact, a separate service team to work through if they prefer to interact over the phone, and each has its own login/authentication. The other way we manage the risk is by controlling what the authorized individual(s) are allowed to do in a discretionary manner. For example, in our 'workplace' business unit, authorized individuals are not allowed to move money.

2. **[Client Question]** Mark, can you comment on the importance of doing enrollment, authentication or fraud detection in the course of a conversation between advisors and customers?

[Response from Mark DiMarzio] I view authentication as the most important thing. It's comparable to an ID / Password in an online channel, in fact, depending upon what types of transactions may be allowed over the phone that aren't allowed on the web, it may be more critical than ID / Password. For us, we've defined high-risk transactions both online and in the phone channel, where we require something above and beyond 'standard' authentication. It's user choice as to whether you consider enrollment as a high-risk transaction. As I mentioned on the call, we assume a little risk because we'd rather enroll 999 customers and get one fraudster vs. making it too difficult and only enrolling 500 customers (numbers made up). I don't believe it's fair to ask an associate answering an 800# to do fraud detection. I'd teach them some red flags and an escalation procedure, and mitigate the risks in other ways.

Tags: Fraud prevention, Fraud prevention, Customer success story, Voice biometrics

About Brett Beranek

Brett Beranek is responsible for overseeing the security and biometric line of business at Nuance, a Microsoft company. In this role for the past 12 years, Beranek has brought Nuance to a leadership position in the biometric authentication and biometric fraud prevention space. A thought leader in the field of biometrics, Beranek is a frequent contributor in industry events and the media on the topic of AI technology and it's use by the fraud community, and how society can mitigate against these evolving threats. Prior to Nuance, he held various leadership positions in the biometrics and security industry. He has earned a Bachelor of Commerce, Information Systems Major, from McGill University as well as an Executive Marketing certificate from Massachusetts Institute of Technology's Sloan School of Management. Beranek is also a certified Master Fraud Prevention Black Belt professional.

View all posts by Brett Beranek