This Happens Every Day - The Problem

A Member Services Rep (MSR) at Mesa Verde Credit Union takes a call from a member. The inbound phone number is indeed the member's registered number, the name of the member displayed on the MSR's screen. To be extra careful, the MSR asked the member to state the last four digits of the social security number and home address. Because the answers were correct, the MSR processed a wire transfer for $75,000 as a down payment on some property the member said he was buying.

But this was not a real member. In fact, this was a fraudster who stole mail and spoofed the member's phone number with a spoofing app. (*Note: Some fraudsters have password hacking software in case they need your password or PIN)*

Problem Cost

- Authentication time was costly because they ask so many questions of the member
- Within certain limits, the credit union likely covers the entire loss for the member, with only a portion refunded by insurance to the credit union. Some very large frauds require members to absorb costs depending on insurance level
- There is lost confidence in the credit union by the member and their friends and family.
- There is a lost reputation cost because the member likely claims on social media that the credit union does not do enough to protect member accounts.

Solution Statement

Now, the credit union can use "id-go", an identity authentication platform provided by Cozera. For an annual cost equivalent to less than one fraudulent action, that credit union protects member accounts in less than 3 seconds. Whether over the phone, in the branch, or online, the member does not need to use passwords or personal information to authenticate themselves. Now, they just use id-go and everyone wins.

How Does it Work?

Id-go is app-less for the member, meaning the member does not need to download a new app on their mobile device. Rather, the credit union pre-enrolls all their members. When a member contacts the credit union through any channel, a text message is sent to that member from the id-go platform. Once the member agrees to enroll, the platform loads a private digital key onto the member's mobile device. That key allows the phone to send a verification of biometric information back to the credit union via id-go. For compliance reasons, id-go does not see or store the biometric information because that information stays with the phone only. However, an encrypted message is immediately sent back to the credit union that essentially says "this is Joe Smith's face" or "this is Jane Smith's fingerprint" which securely ensures that the person communicating with the credit union is the real member and not a distant family member or some fraudster with stolen personal information.

It's that simple. The app-less version of id-go takes less than 1 hour to integrate and deploy for a credit union or bank. No programming required. Our low-code version integrates easily with call center and online banking software, making all transactions more secure. All this without requiring members to remember passwords or sharing personal information. It's all built into the phone, already. Id-go just uses existing technology to better ensure a customer's real identity.

Email us at sales@cozera.io for more information.