BioCatch

Case Study

Top U.S. Credit Union Disrupts Cybercrime Network and Realizes 95% Reduction in Residual Zelle Fraud Losses in Two Months

Problem

A top U.S. credit union became the target of an advanced cybercrime network soon after launching Zelle payments for its mobile banking members in August 2019. They immediately saw a spike to 700 basis points of fraud which means 7% of their total Zelle transaction volume was fraud. They reacted by putting in additional multi-factor authentication (MFA) and other controls, such as limits on Zelle transfer amounts, which helped reduce fraud considerably. However, this caused a big impact on customer experience as members' access to the payment network and its full functionality were limited.

Solution

After realizing how customer experience was impacted by these new controls, the credit union realized that they needed a long-term solution that could significantly reduce fraud to acceptable levels while giving them the confidence to provide customers with full access to the Zelle payment network. They implemented behavioral biometrics on top of the controls they had in place and immediately saw a significant reduction in residual fraud losses and gained deep insights into the cybercrime gang that had been targeting its members. The solution provided an effective control from day one.

Results

95%

Reduction in residual Zelle fraud losses in only two months

0.02%

Achieved best-in-class fraud levels for Zelle payments at only 0.02% of $ volume sent via Zelle

In addition to reducing fraud losses, the credit union also realized significant operational cost savings due to a significant **decrease in call center volumes.**

New Services, New Risks

Since its launch in 2017, the Zelle payment network has experienced rapid growth in the United States offering consumers the convenience of free and fast peer-to-peer (P2P) mobile payments. While consumers have embraced it, banks soon realized the greater risks of online fraud that P2P payments expose. Institutions that have already launched Zelle—ranging from the top five U.S. banks to small credit unions—report highly targeted fraud campaigns and an adaptive race with clever cybercrime rings who are quick to respond to new controls. In fact, by now Zelle fraud is one of the fastest growing areas of account takeover (ATO) fraud in the U.S. banking sector.

A top U.S. credit union realized the risks soon after launching Zelle in August 2019 within its mobile banking platform. Almost immediately, the credit union saw fraud jump to 700 basis points, or simply put, 7% of total Zelle transaction volume was fraud.

They implemented stop gap controls including additional MFA for all new enrollments and beneficiaries. These controls brought fraud down by nearly two-thirds to around 2%, but it was not a sustainable solution or an acceptable level of fraud risk.

Other controls that were implemented included reduced limits for payments. For example, about 75% of new enrollees into the Zelle network had to wait 90 days before they could access the full transfer limit amounts. While this measure further reduced fraud losses, it also had a significant impact on customer experience, frustration with lack of functionality, and an increase in customer service calls to support the payments that couldn't go through Zelle. The credit union's senior executive team wanted a solution that would eliminate this friction for its members.

Taking a Coordinated Cybercrime Gang Head On

Even after implementing the initial controls, the credit union had to continue to bring down payment limits to keep fraud levels under control. After several months of investigation, they learned that they were not up against a small group of cybercriminals, but rather a coordinated gang who were well-scripted and very familiar with the credit union's policies and process. What was actually happening?

This cybercrime gang had purchased or gained access to extensive personal information on dark markets, including account numbers, Social Security numbers, date of birth and even member location. However, in order to access a member's account, they would need to have access to the SMS one-time passcode (OTP) that is commonly used as a way to authenticate a user logging in from a new device or location.

The gang started to initiate calls to members from a number matching the one on the back of the credit union's debit card using a phone spoofing service. Acting as a representative of the bank, the cybercriminals were able to establish authenticity by confirming personal information on the member that they had secured from fraud forums.

The cybercriminal would pose as a member of the fraud team, declare suspicious card transactions or online banking access had occurred from a remote location, and direct the member to perform a password reset. The cybercriminal would initiate the reset so the SMS OTP would be sent to the member's phone. The member would be asked to provide the OTP and then it was game over. The member was locked out of their account allowing the cybercriminals to change the email and phone number on record and enroll in Zelle to initiate fraudulent payments.

After deep investigation, the credit union learned they were being targeted by coordinated gangs throughout the U.S. identified to be coming or centered around college campuses. The gang was very well-scripted, highly familiar with the bank's process and believed to have experience in call center enviornments based on the sophistication of the attack. In some cases, social engineering tactics were so effective the cybercriminals even got members to divulge their usernames and other details needed to access their account.

Case Study

Going Beyond Device with Behavioral Insights

The advanced social engineering schemes associated with the account takeover attack had been able to circumvent MFA controls. The credit union required a solution that could provide behavioral insights to identify patterns in real-time indicative of a cybercriminal inside the member's account.

Upon deploying BioCatch behavioral biometrics, common patterns related to account takeover using social engineering emerged almost instantly. The access to the member's account showed lack of familiarity with the member's details, which is an indication of criminal use. While the fraudsters were highly familiarity with the flow of Zelle enrollment, they displayed behavior consistent with someone who doesn't know the data such as segmented typing indicating working off a list, pasting certain elements and multiple deletions. The length of time it took to conduct certain actions within user sessions was correlated to social engineering ATO. With the use of MFA codes, a member being coerced would need to read an MFA code to the cybercriminal which takes more time.

Behavioral biometrics data elements also show differences in the way cybercriminals and genuine operate their devices. Those elements became important to the risk scoring model developed by the credit union.

The solution proved to be effective from day one. The BioCatch technology immediately spotted differences between genuine and cybercriminal access even without any prior user history which was very important to the credit union. There was simply no time to wait and build profiles. The result was an immediate reduction in fraud losses in the mobile banking channel.

Within two months of deploying BioCatch, the credit union saw a 95% reduction in residual fraud losses, virtually eliminating all fraud associated with Zelle payments and disrupting a sophisticated cybercrime network. Today, **only 0.02% of Zelle payments is fraud.** BioCatch is now being implemented across other areas of exposure to help improve ATO fraud detection performance.

The credit union has been recognized as best-in-class for maintaining such low levels of Zelle fraud and continue to stay well ahead of their competitors in managing the risk. The cybercrime gang has since taken their business elsewhere, and the fraud team at the credit union gets regular calls from their peers who are now experiencing similar attacks to seek advice on mitigation strategies.

BioCatch

BioCatch pioneered behavioral biometrics, which analyzes an online user's physical and cognitive digital behavior to protect users and their data. Today, customers around the globe leverage BioCatch's unique approach and insights to more effectively fight fraud, drive digital transformation and accelerate business growth. With nearly a decade of data, over 50 patents and unparalleled experience analyzing online behavior, BioCatch is the leader in behavioral biometrics. For more information, please visit **www.biocatch.com**

www.biocatch.com

E: info@biocatch.com

@biocatch

in /company/biocatch