

# Top 5 U.S. Bank Launches Behavioral Biometrics to Stop Account Takeover Attack Using Zelle Payments

## Launch New Digital Products and Services With Confidence

### Problem

A top U.S. bank was experiencing a sustained account takeover attack in which cybercriminals used social engineering tactics to trick customers into sharing their online banking credentials. Once inside the account, cybercriminals would proceed to enroll the customer into Zelle, set up new payees and initiate real-time fraudulent payments.

### Solution

The bank was already using BioCatch to detect account takeover fraud. The BioCatch behavioral biometrics solution implementation was extended to login, user dashboard and high-risk activities such as Zelle enrollment and payments. During the massive Zelle attack, the BioCatch risk score provided a deeper layer of visibility to identify fraudulent activity and eventually deflect the attack.

### Results

# 100%

Fraud Alert Accuracy

# 300+

Zelle enrollment fraud cases flagged in weeks with no reported false positives

# \$300,000

Saved in first 3 weeks of attack

The US banking industry made a significant leap forward when the Zelle real-time P2P payment network was launched in 2017. In only three years, Zelle took off announcing in November 2020 that it reached more than 1 billion payments in a 12-month period and has more than 1,000 banks and credits unions currently contracted to participate in its network.

The rapid adoption of Zelle by consumers in the U.S. have made it a hunting ground for cybercriminals primarily due to speed. Payments are completed within minutes making it difficult for banks to detect or disrupt a transaction. The move to faster payments in other countries has proven to cause a rapid increase in fraud. In the UK, it caused online banking fraud losses to triple within three years<sup>1</sup>, despite the implementation of controls including hardware and SMS-based multi-factor authentication.

## Detecting Anomalies in Zelle Enrollments

The launch of faster payments requires fraud and risk management teams to make decisions in real-time, and the fraud solutions and controls they implement must do the same. Behavioral biometrics provides immediate visibility and insights into risk for faster payments. This is especially true at the enrollment stage before a payment can be initiated.

When a customer initiates a Zelle enrollment, the BioCatch system looks at three elements: user behavioral anomalies (i.e. the user does not behave in a normal way), criminal behaviors (i.e. the anomaly looks negative and associated with past fraud behavioral patterns), and non-behavioral risk indicators.

In the following example, user behavioral anomalies in the Zelle enrollment process are evident:

Navigation	Session Value	User %	History Value
Arrows	65	3%	0.38
Keyboard Navigation Methods	Session Value	User %	History Value
Delete	20	2%	0.58
Keyboard Navigation Methods	Session Value	User %	History Value
LeftShift	94	8%	0.14

The data in the table indicates the following **high-risk behavior**:



**Scrolling preference anomaly:** The genuine user normally scrolls up and down using the mouse wheel. In this session, however, they used the Arrow key 65 times in order to navigate up or down.



**Excessive deletion:** The enrollment process contains information that the user is supposed to know. In past sessions, the user used the Delete button only once every 2 sessions on average (0.58 per session). In this session, the Delete button was used 20 times. This anomaly suggests lack of familiarity with data which is present in 64% of confirmed account opening and enrollment fraud cases, according to BioCatch research.



**Cognitive choices:** There are many elements that a user might frequently utilize or generally avoid. Specifically, this user rarely uses LeftShift. In the past, LeftShift was used in 1 out of 7 sessions (0.14 per session). In this session, LeftShift was used 94 times.

The BioCatch platform analyzes over 2,000 behavioral risk indicators in real-time. This specific case of a Zelle enrollment was confirmed as fraud, and BioCatch was able to detect it by seeing anomalies in the user's regular behavior, cognitive choices, interaction patterns and navigation habits. The anomalies were further classified as negative by using the criminal behavior model which leverages past fraud events to predict likely fraud scenarios. Additional non-behavioral risk indicators in this session included signs of access from a virtual machine and a time zone mismatch.

## Behavioral Biometrics Provides Immediate Impact

By adding the BioCatch platform to their fraud controls, the bank was able to stop over \$170,000 in fraud attempts within the first weekend of the attack. By the end of the month, BioCatch alerted on a total of 312 Zelle attack sessions with no false positives reported. In total over a three-week period, the BioCatch platform prevented over \$300,000 in fraud losses.

The move to faster payments and P2P platforms is a big win for consumers, especially among the younger generation. Among those 18 to 24 years of age, 82% have used P2P payments<sup>2</sup>. Banks who are looking to remain competitive in a digital-first world know that adoption of these platforms is critical to retain existing customers and attract new ones. However, these platforms expose banks to increasing risk which is why it is important to have strong fraud controls at the enrollment process, such as behavioral biometrics, to ensure consumers are able to enjoy the full functionality and convenience of the service.

<sup>2</sup> Source: Payments Journal, "Debit Cards and P2P Payments are Important to the Payment Ecosystem," March 2020



BioCatch is the leader in Behavioral Biometrics which analyzes an online user's physical and cognitive digital behavior to protect individuals and their assets. Our mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease seamlessly co-exist. Leading financial institutions around the globe use BioCatch to more effectively fight fraud, drive digital transformation and accelerate business growth. With over a decade of analyzing data, over 60 patents and unparalleled experience, BioCatch continues to innovate to solve tomorrow's problems. For more information, please visit [www.biocatch.com](http://www.biocatch.com)

[www.biocatch.com](http://www.biocatch.com)

**E:** [info@biocatch.com](mailto:info@biocatch.com)

**T:** [@biocatch](https://twitter.com/biocatch)

**L:** [/company/biocatch](https://www.linkedin.com/company/biocatch)