Nasdaq Verafin

BioCatch
Stay Safe.

Next-Generation Fraud Detection for Banks and Credit Unions

Revolutionizing Prevention with BioCatch and Nasdaq Verafin



Colin Parsons

VP Fraud Product Strategy,
Nasdaq Verafin



Justin Hochmuth

Manager, Threat Analytics – Partners,
BioCatch

Poll

How familiar are you with BioCatch?

- Currently using BioCatch
- Used to use BioCatch
- Familiar with BioCatch but have never used it
- Never heard of BioCatch

BioCatch is the leader in next-gen fraud prevention

Company

Founded in 2011

Pioneer and leading provider of **behavioral intelligence**

Trusted by **leading financial institutions** around the world

Work closely with customers to identify **cutting-edge solutions** to new attack vectors

Team

Global presence with headquarters in NY and Tel Aviv

Industry-leading experience: Unit 8200, RSA, L-1, ThreatMetrix, Cyota

Deep domain expertise coupled with advanced data science and machine learning

Products

Spans the **digital account lifecycle** from onboarding to login to payment

Analyzes a user's physical and cognitive digital behavior to make banking safer every day

Generates **actionable insights** empowering customers to determine the appropriate response

>535M	>90	>16B	$3.7B
global users protected	global patents granted	sessions protected per month	estimated fraud prevented in 2024

New York • Tel Aviv • Boston • London • São Paolo • Santiago • Mexico City • Melbourne • Mumbai • Singapore

Trusted by the largest global banks...



...and >190 of your peers.



Nasdaq Verafin

BioCatch Stay Safe.

Markets

Protect financial institutions of all sizes across the globe

Data

Best-in-class transactional, behavioral and device intelligence

Beliefs

Fighting fraud and financial crime requires unique data and a collaborative approach

Nasdaq Verafin

BioCatch Stay Safe.

Our Partnership

Initial Phase

Unlock Insights

Integrate BioCatch alerts and risk insights into the Nasdaq Verafin platform.

Co-Design

Combine best-in-class transactional, device and behavioral insights to deliver innovative fraud solutions.

Collaborate

Fight fraud at an industry level, joint research, thought leadership.

Fighting Fraud More Effectively



725M
Counterparties



2600
Financial
Institutions



3000
Unique
behavioral and
device-related
datapoints

Fraud is a $486B global problem.

Source: Nasdaq, 2024 Global Financial Crime Report at https://www.nasdaq.com/global-financial-crime-report

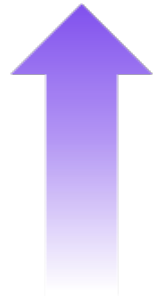


Rapidly Evolving Scams & Threat Vectors



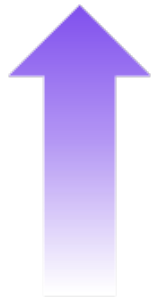
60% increase

in **AI-related fraud** & scam cases
(2022-2024)



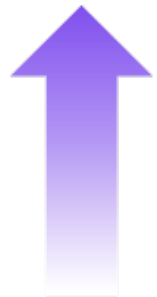
80% increase

in **crypto-related fraud** cases
(2023-2025)



60% increase

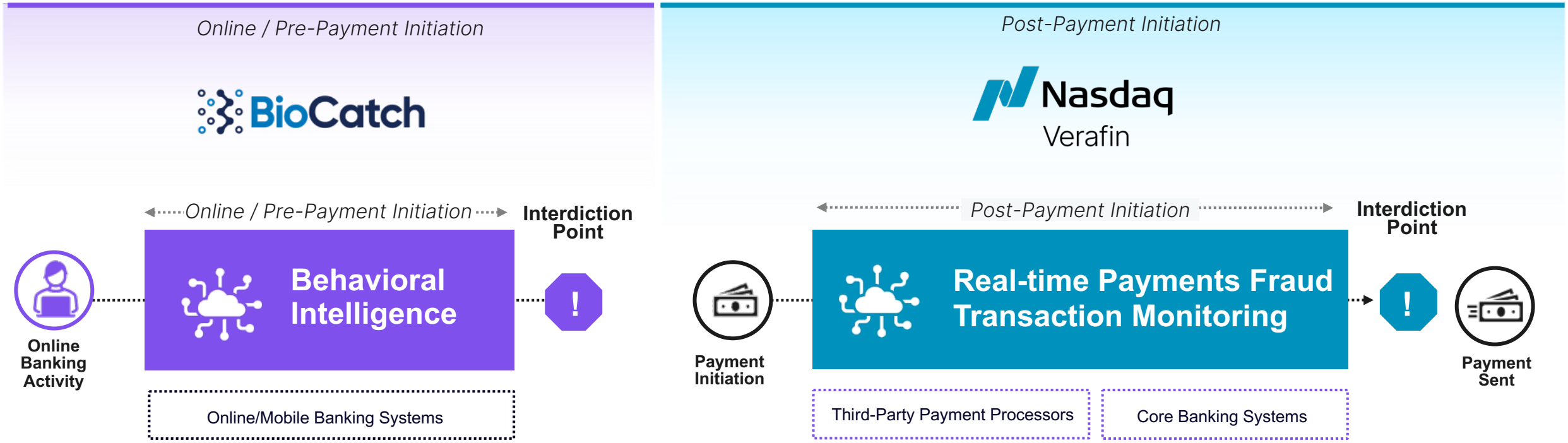
in **impersonation fraud** cases
(2022-2024)



50% increase

in **online account takeover** cases
(2022-2024)

Maximizing Fraud Prevention Across Transactions

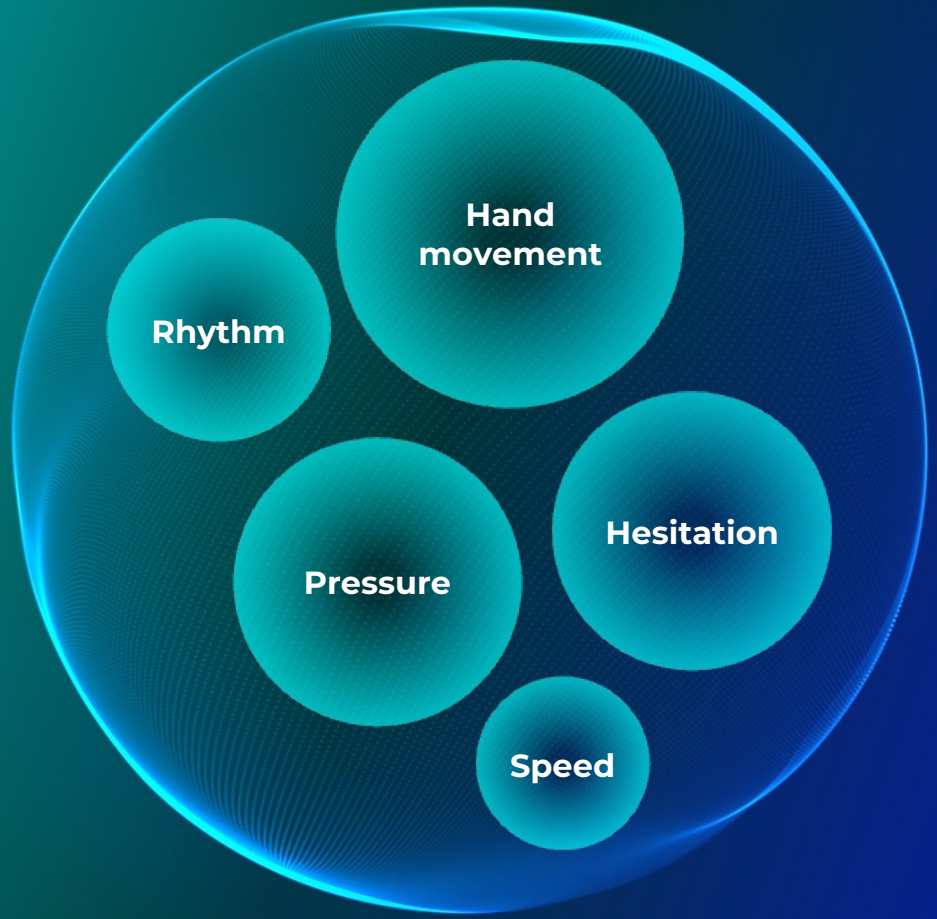


The Power of Behavioral Intelligence

Every interaction tells a story.

How we type, swipe and scroll creates a behavioral signature.

BioCatch analyses thousands of signals in real time.



Turning behavior into protection.

Under duress

Vulnerable

Distracted

Elderly

Continuous protection throughout the entire customer journey.



Account Opening



Account Takeover



Social Engineering Scams



Money Mules

Why Choose BioCatch?

Positive business outcomes for >200 customers globally

Reduced Fraud Losses

Improved Customer Experience

Reduced Operational Overhead

https://www.biocatch.com/resources

Account Takeover Solution

What are behavioral insights and how does it work?

BioCatch

A Comprehensive Profile for Every User

BioCatch monitors user behavior and builds a profile of what is normal for the user and risk rate activities. BioCatch requires about 60 days of production activity to establish a meaningful profile. We also require you to mark fraud in the system during our onboarding process and ongoing

User Profile (>2,000 attributes)

Behavioral Intelligence

Behavioral Attributes

- Holding
- Press size
- Scrolling
- Swiping
- Hand-eye coordination

Cognitive Attributes

- Interaction preferences
- Field-specific input habits

Behavior Analysis

- Devices
- Locations
- Transactional habits
- In-app actions and activities

In-session

Monitor **real-time interactions** between users and devices

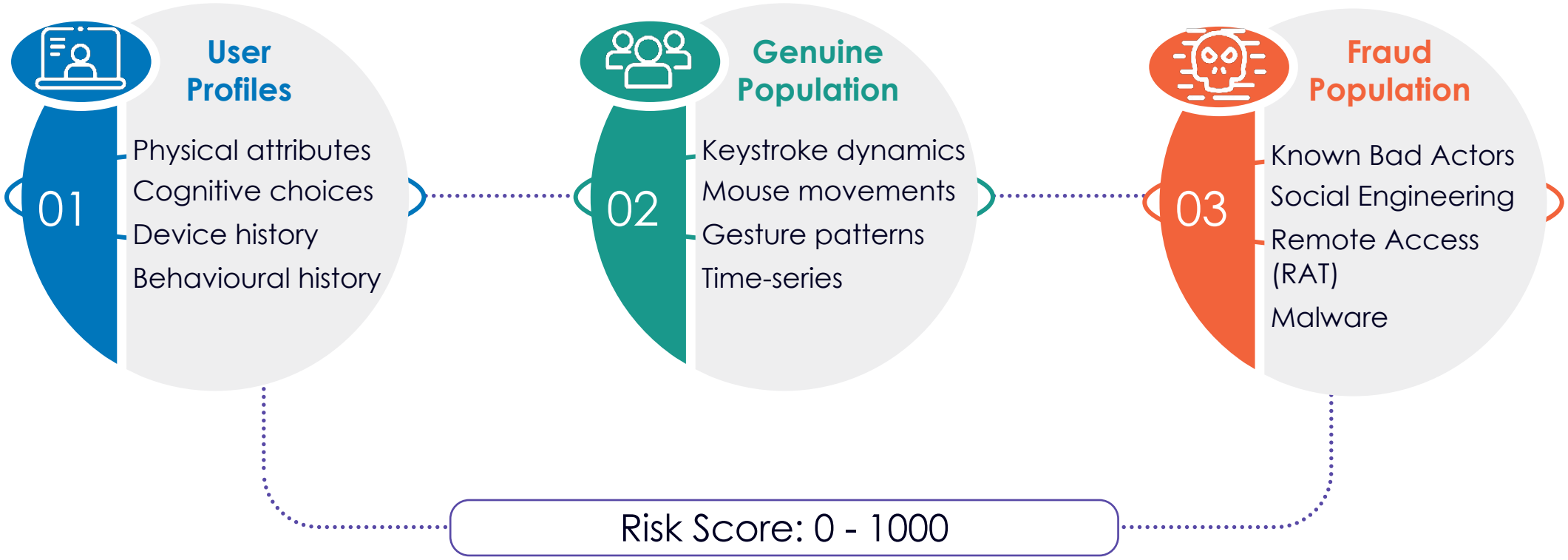
Analyze live user behavior to provide **continuous protection** during the entire post login online session

Service is **invisible** and **frictionless** to the user and offered across both web and mobile (Hybrid only)

Profiles are unique and anonymous

Real-Time Session Risk Scoring

Our risk engine dynamically compares the data obtained from the current session with the profiles and calculates a highly accurate risk score.



The BioCatch Approach

Continuous Protection

+

Actionable Intelligence

+

Frictionless Experience

Collect Data

- Web & Hybrid Mobile

Mouse Activity

Keyboard Activity

Screen Behavior

Mobile Use

Analyze

Behavioral Attributes

- Typing
- Scrolling
- Mouse clicks
- Holding
- Hand-eye coordination

Cognitive Attributes

- Interaction preference
- Field-specific input habits

Take Action

- Real-time decisioning

BioCatch Insights: Score

Session Strategy

- Approve
- Step-up Authentication
- Decline Block/Lock

What does BioCatch return?

Sample Risk Engine insights from 100+ attributes across use cases

General

- Customer ID
- Session ID
- Device ID

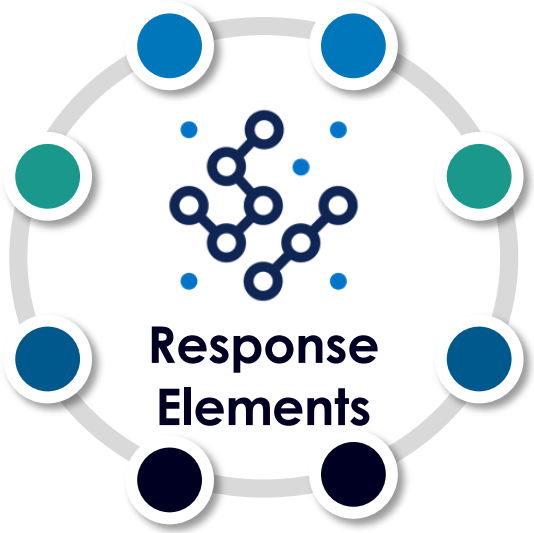
Score + Attributes

Geolocation

- IP City, Country
- Latitude / Longitude

Threat Indicators

- BOT / Hybrid BOT
- RAT / Recent RAT
- Emulation
- Guided Voice Scam



Misc. Data Points

- Behavioral
- Location
- Device
- User History

Risk Factors

- Change Dominant Hand
- Typing Pattern Anomaly
- Special Keys
- Fast Traveler
- Data Import
- Mouse Anomaly

Genuine Factors

- Autofill
- Fluid Typing
- Consistent Device
- Consistent Wi-Fi
- No Delay to Data Entry

Case Studies

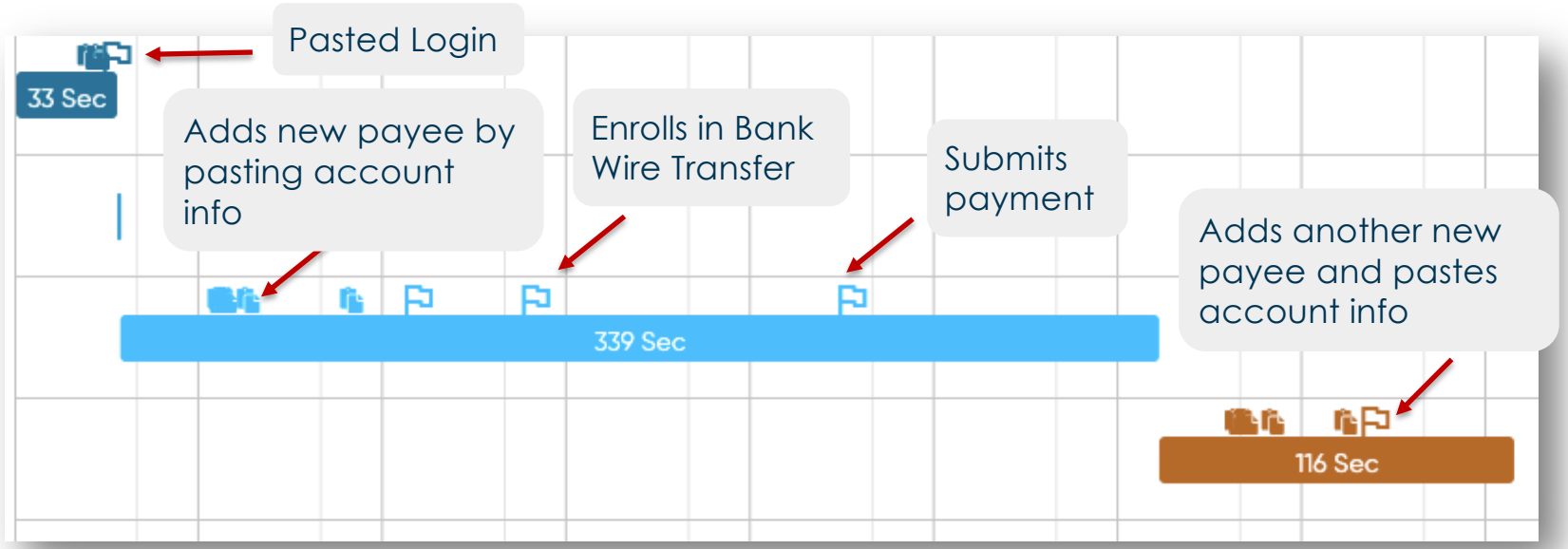
Preventing Account Takeover at a Mid-Market Customer

BioCatch

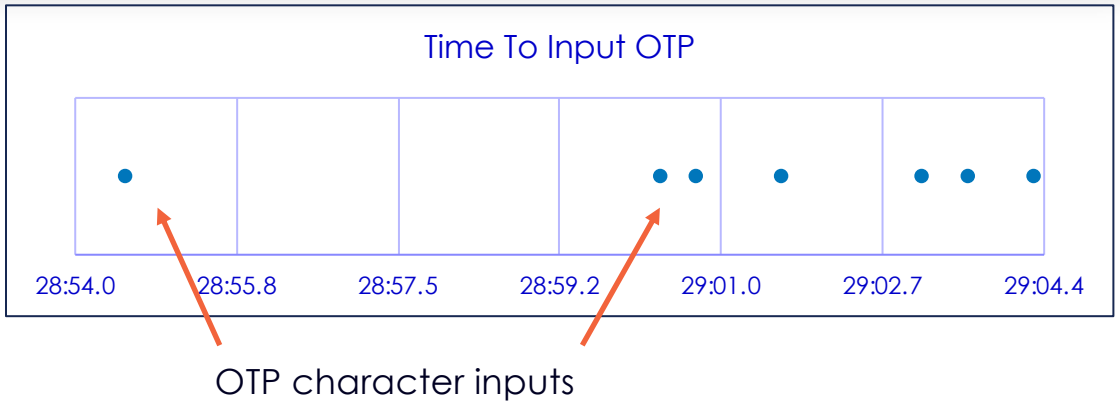
OTP Vishing Example

Social Engineered Access

- Password was reset in prior session – scored high by BioCatch
- Login credentials are pasted and the fraudster enrolls in Bank Wire Transfer
- New payees are added and paid a high sum

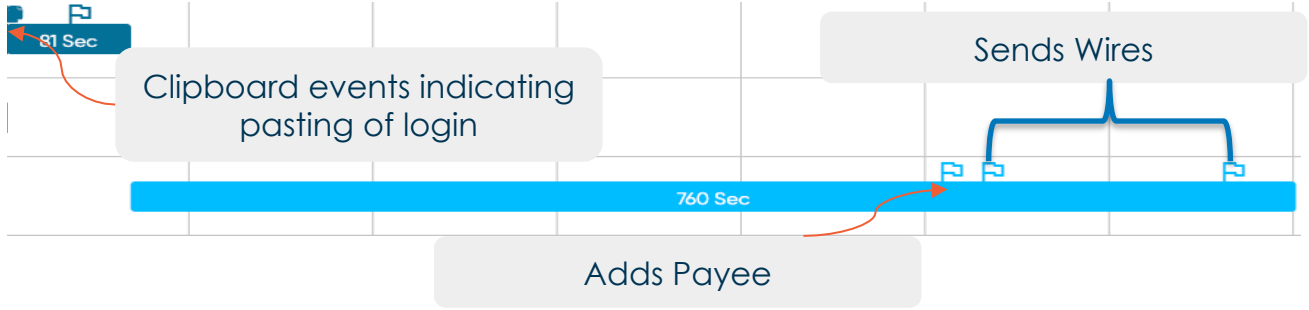


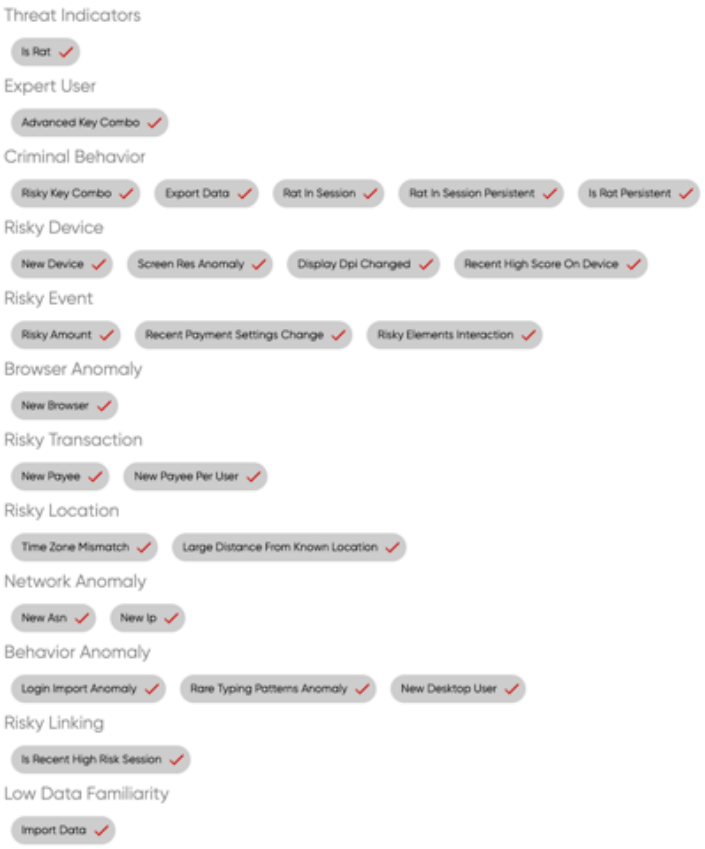
- User is required to enter OTP to make wire transfer
- User's typing cadence when inputting OTP is much longer than average population
- Single OTP character input followed by long pause and remaining characters typed in 3's indicating info is dictated

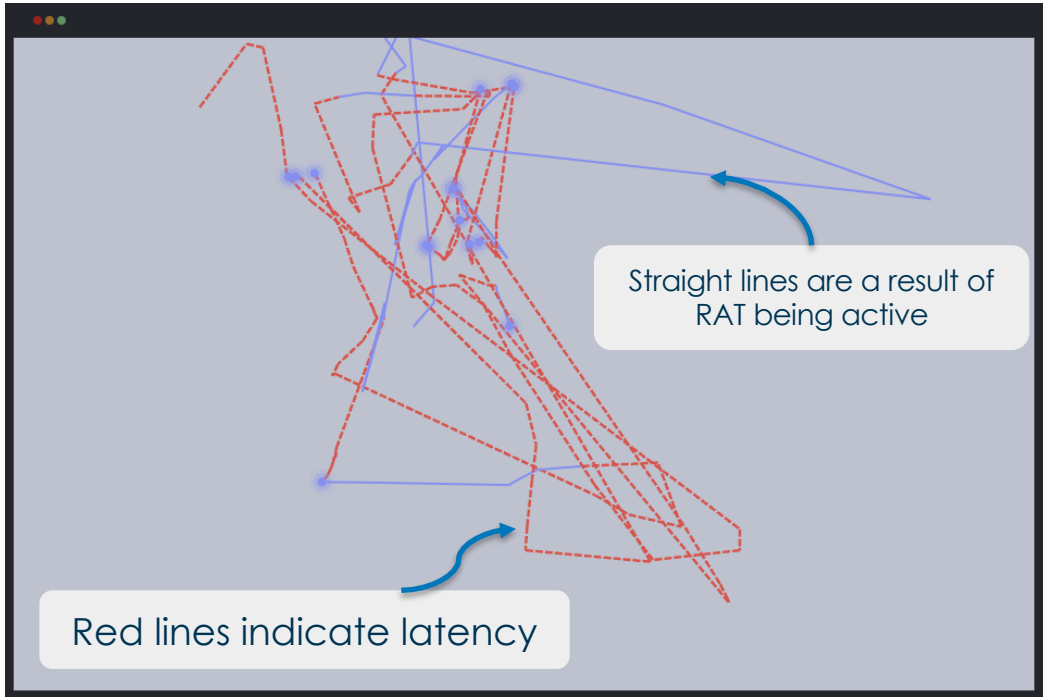


Remote Access Tool Detection

- Login
- Wire







Highlights

- User pastes password details
- session scores 1000 on ATO model
- User sends 2 wire payments after adding a payee. One for $6K and another for $5.5K to the same payee
- Session has a RAT active throughout the full duration
- User has 75 days of history with BioCatch but the device, IP, ASN, and IP City are new to their profile

Fraudulent Wire Transfer

Comparing genuine & risky sessions

Distinct behavior changes detected in the fraud session compared with previous genuine payment sessions:

1. Change from mostly numpad to keypad only
2. Higher rate of Left-Shift and introduction of Left-Ctrl use
3. Genuine user uses mouse wheel to scroll
4. Touch detected for the first time

GENUINE

Keyboard Typing	Session Value	User History %	User History Value
Keypad	8	100%	12
Numpad	31	84%	40
RightShift	0	0%	0
RightCTRL	0	0%	0
RightALT	0	0%	0
LeftShift	4	99%	8
LeftCTRL	0	1%	0.01

Navigation	Session Value	User History %	User History Value
Tab	0	0%	0
Wheel	21	91%	45
Touch	0	0%	0

FRAUD

Keyboard Typing	Session Value	User History %	User History Value
Keypad	78	100%	13
Numpad	0	83%	39
RightShift	0	0%	0
RightCTRL	0	0%	0
RightALT	0	0%	0
LeftShift	26	98%	8
LeftCTRL	1	2%	0.02

Navigation	Session Value	User History %	User History Value
Tab	0	0%	0
Wheel	0	90%	43
Touch	69	2%	0.63

Baxter Credit Union

One of our many successful outcomes

95%

Reduction in Zelle fraud

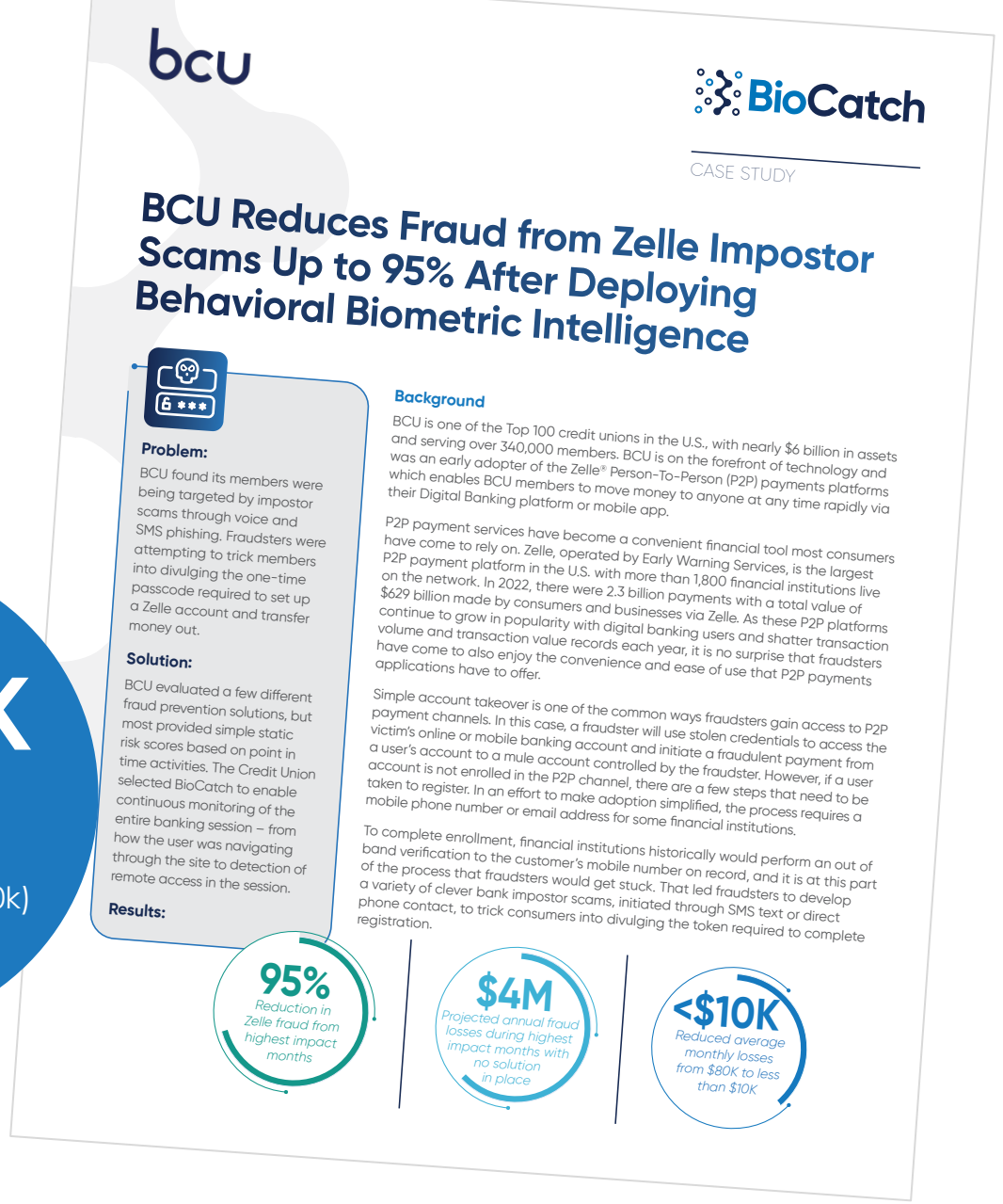
$4M

Projected annual fraud losses with no solution in place

<$10K

Reduced average monthly losses ($80k to less than $10k)

Head to www.biocatch.com/resources for more info



bcu

BioCatch

CASE STUDY

BCU Reduces Fraud from Zelle Impostor Scams Up to 95% After Deploying Behavioral Biometric Intelligence

Problem:

BCU found its members were being targeted by impostor scams through voice and SMS phishing. Fraudsters were attempting to trick members into divulging the one-time passcode required to set up a Zelle account and transfer money out.

Solution:

BCU evaluated a few different fraud prevention solutions, but most provided simple static risk scores based on point in time activities. The Credit Union selected BioCatch to enable continuous monitoring of the entire banking session – from how the user was navigating through the site to detection of remote access in the session.

Results:

Background

BCU is one of the Top 100 credit unions in the U.S., with nearly $6 billion in assets and serving over 340,000 members. BCU is on the forefront of technology and was an early adopter of the Zelle® Person-To-Person (P2P) payments platforms which enables BCU members to move money to anyone at any time rapidly via their Digital Banking platform or mobile app.

P2P payment services have become a convenient financial tool most consumers have come to rely on. Zelle, operated by Early Warning Services, is the largest P2P payment platform in the U.S. with more than 1,800 financial institutions live on the network. In 2022, there were 2.3 billion payments with a total value of $629 billion made by consumers and businesses via Zelle. As these P2P platforms continue to grow in popularity with digital banking users and shatter transaction volume and transaction value records each year, it is no surprise that fraudsters have come to also enjoy the convenience and ease of use that P2P payments applications have to offer.

Simple account takeover is one of the common ways fraudsters gain access to P2P payment channels. In this case, a fraudster will use stolen credentials to access the victim's online or mobile banking account and initiate a fraudulent payment from a user's account to a mule account controlled by the fraudster. However, if a user account is not enrolled in the P2P channel, there are a few steps that need to be taken to register. In an effort to make adoption simplified, the process requires a mobile phone number or email address for some financial institutions.

To complete enrollment, financial institutions historically would perform an out of band verification to the customer's mobile number on record, and it is at this part of the process that fraudsters would get stuck. That led fraudsters to develop a variety of clever bank impostor scams, initiated through SMS text or direct phone contact, to trick consumers into divulging the token required to complete registration.

95% Reduction in Zelle fraud from highest impact months

$4M Projected annual fraud losses during highest impact months with no solution in place

<$10K Reduced average monthly losses from $80K to less than $10K

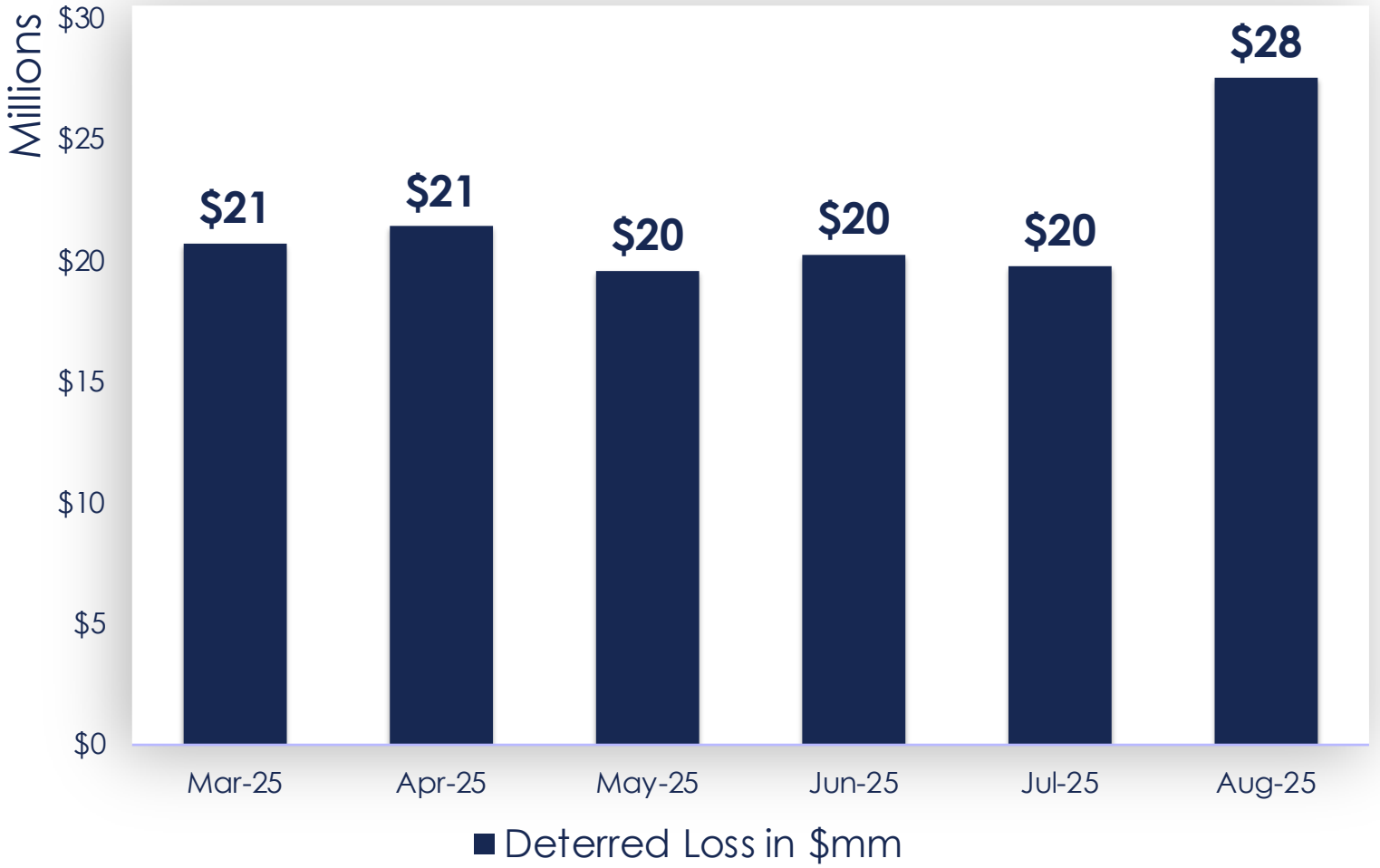
The Value of Blocking Transactions in Real-Time

Our impact in the U.S. midmarket over the past 6 months.

$128M

in aggregate blocked and alerted fraud

Based on customer reported fraud across our U.S. midmarket base over the last 6 months.



Our Integration

Nasdaq Verafin's consortium insights and transaction monitoring already offer leading protection for initiated payments.



Nasdaq Verafin's Consortium by the Numbers

More than
2600
customer partners

More than
$10T
in collective assets

More than
725M
counterparties

More than
1B
transactions a week

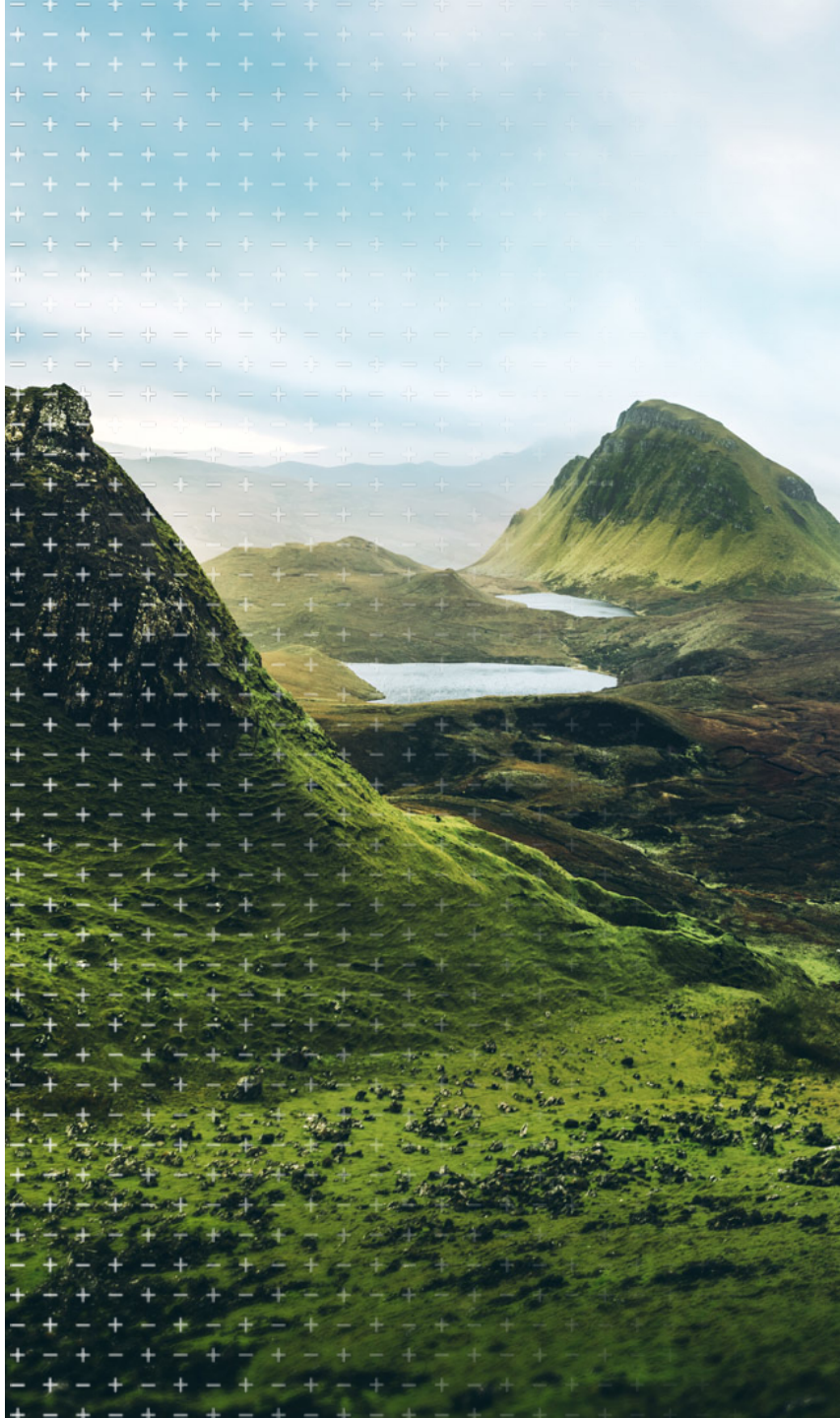
Power our consortium analytics today



Cross-institutional analysis in the Nasdaq Verafin Cloud determines payee history.



Risk scoring counterparties based on relationships across the Cloud.



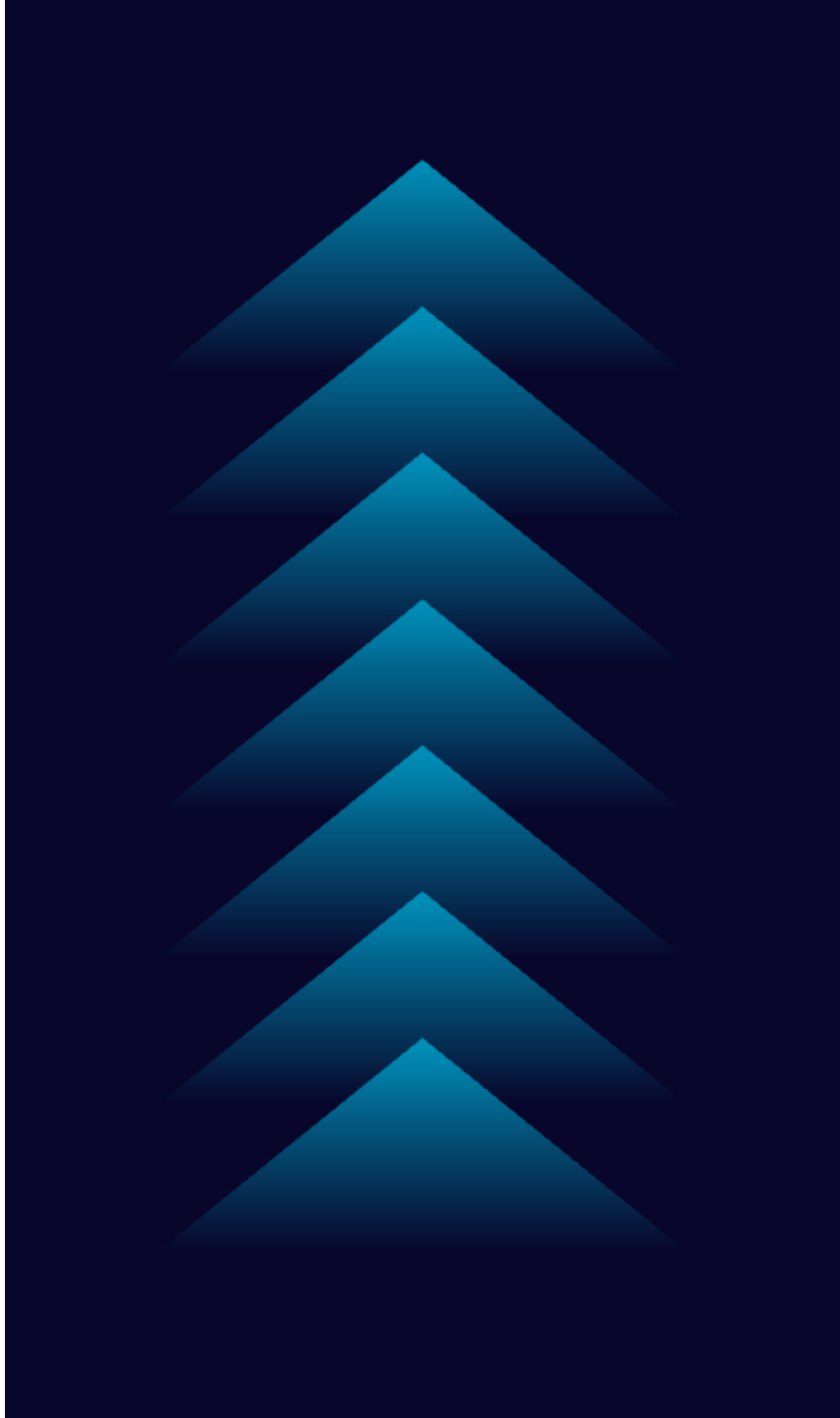
Explaining away established or low-risk interactions to reduce false positives.



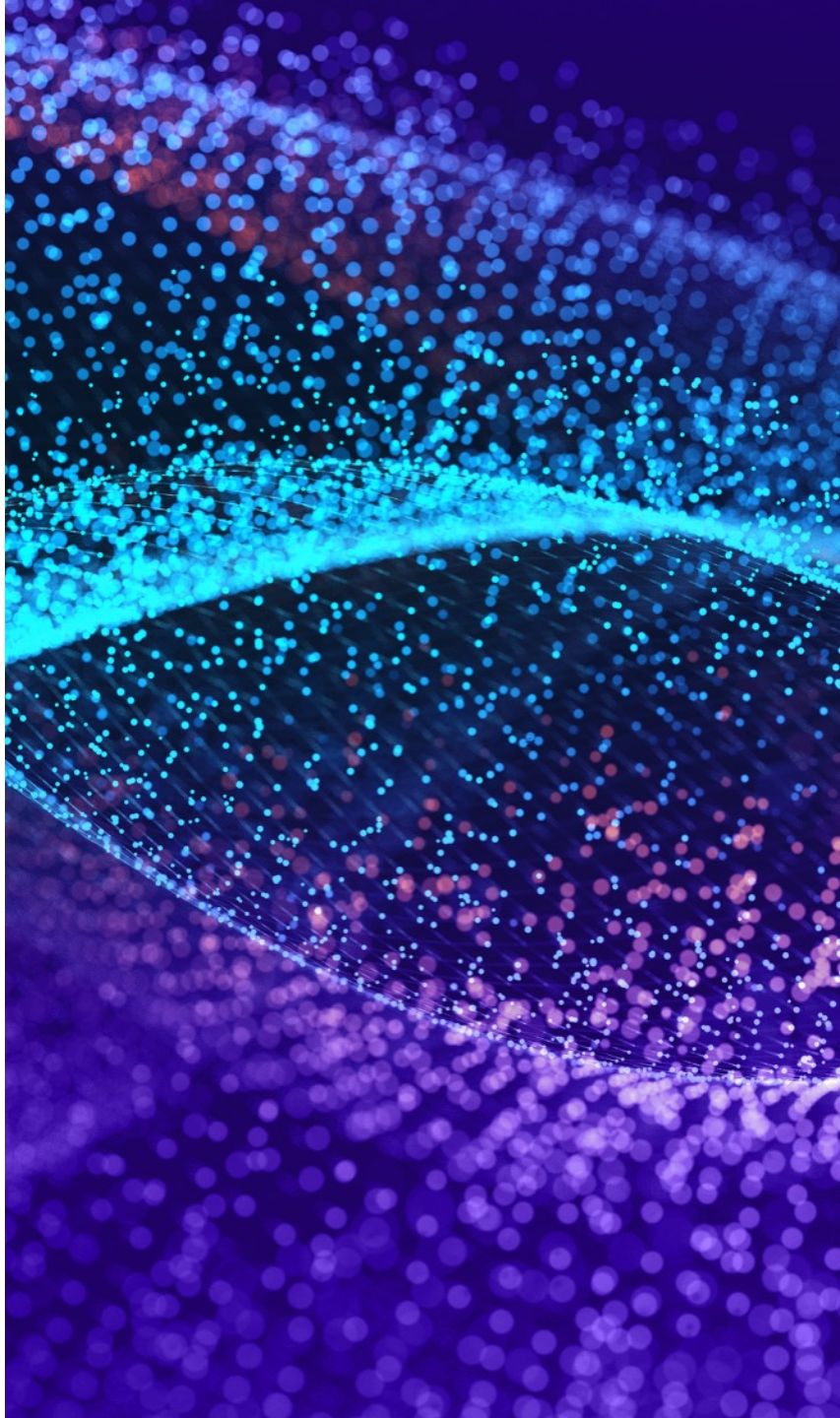
If the receiver is new
to your customer or
new to your institution,
but has a trusted history
in the Nasdaq Verafin Cloud,
the risk is reduced.



If the receiver is new to the Nasdaq Verafin Cloud you are alerted to a higher-risk transfer.



Combining this approach with BioCatch provides a complete picture of payment risk from pre- to post-initiation.



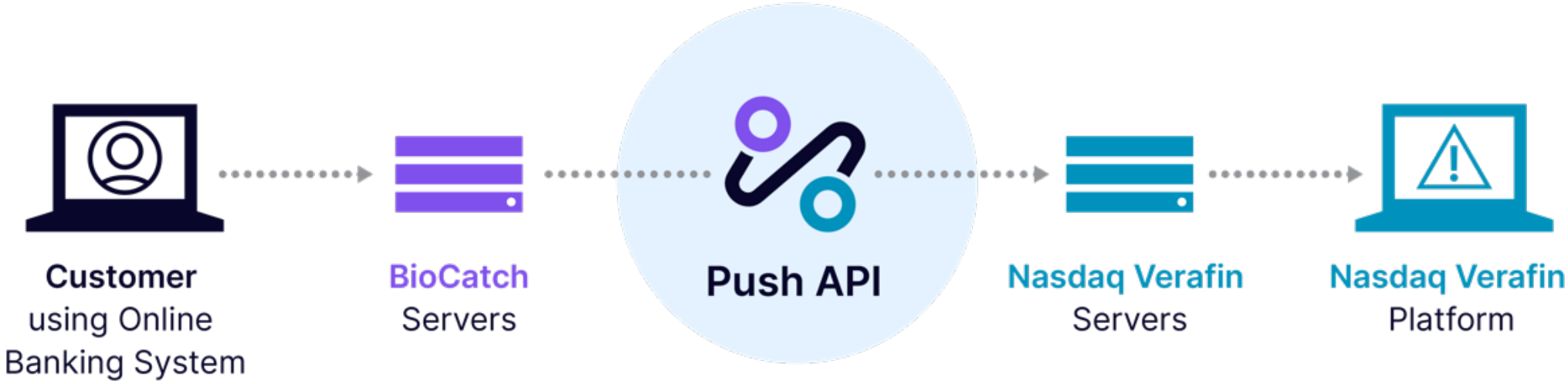
Benefits of our Integration

- Enhanced fraud detection and prevention, even for sophisticated typologies.
- Improved efficiency, better investigations, and reduced manual effort.
- Fewer false positive alerts and reduced friction for legitimate payments.

Investigate with Nasdaq Verafin's powerful Link Charts and Visual Storytelling tools.



The BioCatch – Nasdaq Verafin Implementation



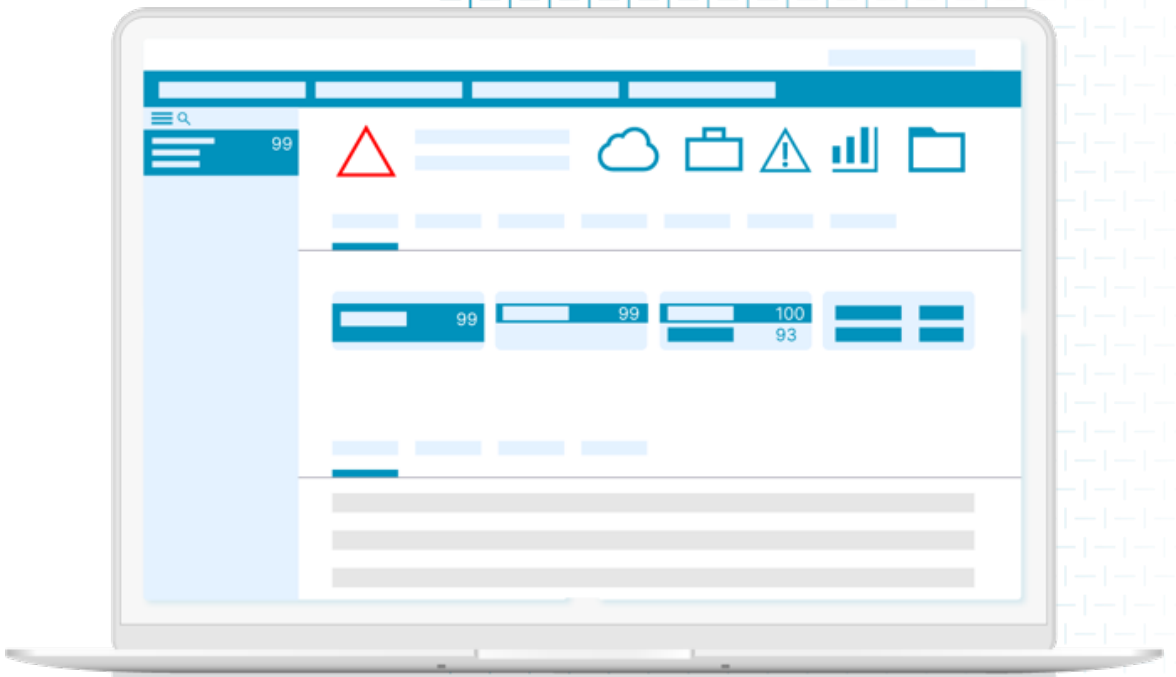
Fast & Effective

Direct Data Flow: Customer behavioral data from BioCatch is securely delivered into the Nasdaq Verafin platform for real-time fraud prevention.

Easy-to-Install API Connection: The BioCatch connector can be switched on instantly using a secure subdomain setup — no code changes required.

Entity Match: Nasdaq Verafin matches the User ID from BioCatch to a Nasdaq Verafin entity, alerting on that entity within the platform.

Product Demonstration



Nasdaq Verafin

+

BioCatch
Stay Safe.

Fraud detection platform and consortium data network.

Industry-leading behavioral intelligence capabilities.



Register your Interest

Harness integrated BioCatch insights in Nasdaq Verafin

verafin.com/nasdaq-verafin-biocatch-partnership

Nasdaq Verafin

BioCatch Stay Safe.