

# Digital Identity Verification: A Competitive Advantage for Banks & Credit Unions

Sara Seguin,  
Principal Advisor, Fraud & Identity Risk,  
Alloy

THE FINANCIAL BRAND

FORUM

# Sara Seguin

Principal Advisor, Fraud & Identity Risk  
[sara@alloy.com](mailto:sara@alloy.com)

- Sara Seguin is the Principal Advisor on Fraud and Identity Risk at Alloy and brings 17 years of experience in the field to the company.
- Prior to joining Alloy, Sara was the Head of Enterprise Fraud Strategy for KeyBank.
- Deep experience within various fraud risk domains which include deposit, payments, online activity, card, risk, and identity.



FINANCIAL BRAND

**FORUM**

# What We'll Cover

- Why fraud hinders growth
- Striking a balance between user experience and identity verification
- Centering identity in your digital verification process throughout the customer lifecycle
- Using digital identity verification to grow your business



There were more than 1M reports of identity theft in the U.S. in 2023. As a result, Americans lost a record \$10B to fraud—up from \$1.6B in 2013\*.

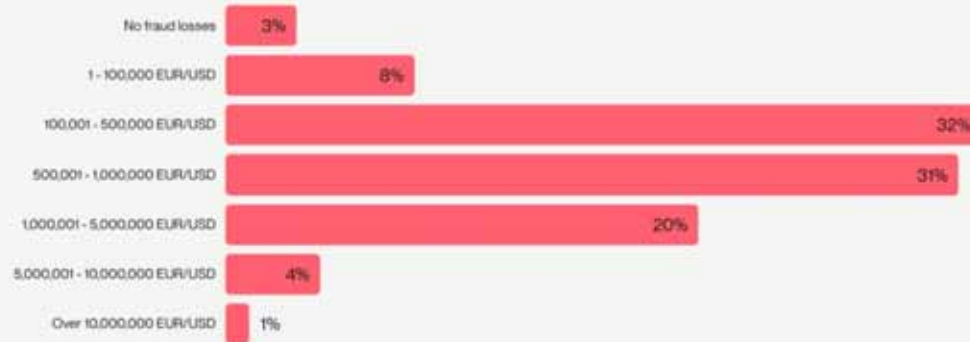
\*Source: Federal Trade Commission

THE FINANCIAL BRAND

FORUM

# Why fraud hinders growth

How much do you think your organization may have incurred in direct fraud losses over the last 12 months?



\*Combined US and UK data

Source: Alloy 2024 State of Fraud Benchmark Report



- According to Alloy's State of Fraud Report, 25% of financial institutions lost over \$1M to fraud in 2023
- Because it is difficult to identify fraudsters after they have already stolen money, most funds are not recovered: 68% of financial institutions recovered less than half of their losses in 2023

# The rise of digital banking has led to a tradeoff between fraud prevention policies and top-notch digital experiences

FIGURE 3

## Respondents used mobile and online channels most frequently

■ Never ■ Less than once a month ■ 2-5 times per month  
■ 6-9 times per month ■ 10 or more times per month



Note: Percentages may not total 100% due to rounding.  
Source: Deloitte Center for Financial Services analysis.

Deloitte Insights | [deloitte.com/insights](https://deloitte.com/insights)

- According to a study from Deloitte, 84 percent of consumers use online banking to access their primary bank
- 72 percent use mobile apps to access their primary bank

# Financial institutions must balance a variety of identity challenges

**Customer Friction**  
Lengthy manual review & unnecessary MFA



**Unscalable**  
Legacy systems struggling to keep up



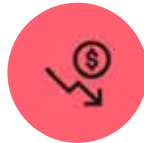
**High Fraud Rates**  
Sophisticated fraud attacks



**Resource Constraints**  
Building & maintaining legacy systems



**Lost Revenue**  
Declining good customers



**Penalties & Fines**  
Ineffective compliance controls



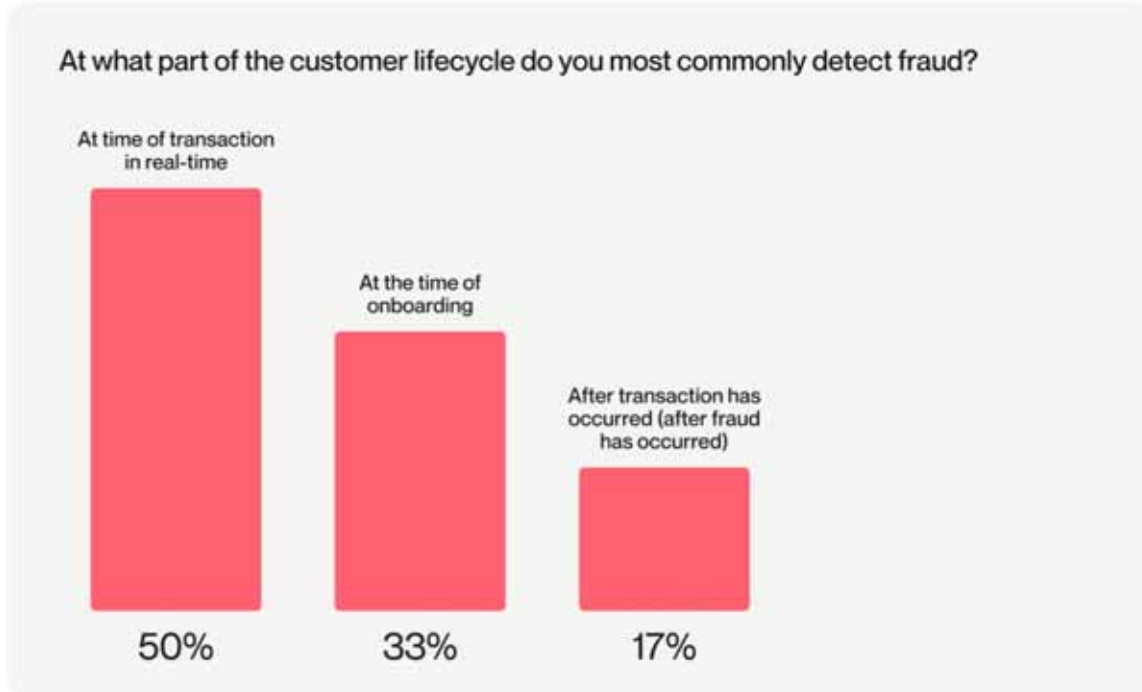
“If you were only worried about risk, you wouldn’t be giving anyone a card. So the question becomes, what return do we get for the additional risk?”

**Jacob Wallenberg**  
Risk Operations at Ramp



Centering *identity* in your verification process is the key to balancing fraud prevention, user experience, and growth.

# Financial institutions need to adopt a holistic approach to fraud prevention



\*Source: Alloy 2024 State of Fraud Benchmark Report

- Detecting fraud at the time of the transaction is the last opportunity to prevent monetary losses
- Moving from a proactive approach to analyze identity in advance of the transaction will not only prevent fraud, but also better predict who will commit fraud in the future

# How to prevent fraud in real-time

Once an anomaly or risk is identified, what do you do about it?

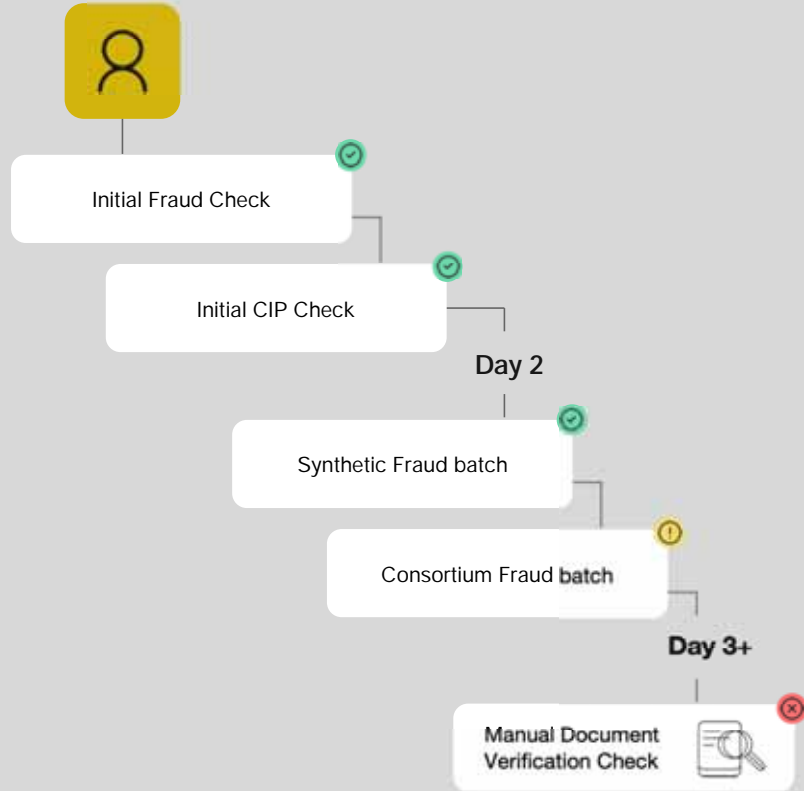


\*Source: Alloy 2024 State of Fraud Benchmark Report

- Strengthen controls at onboarding by layering solutions
- Use step-up verification methods on riskier applicants before onboarding them
  - Phone verification
  - Selfie ID verification
  - Document verification
  - Multi-factor authentication

Linear →

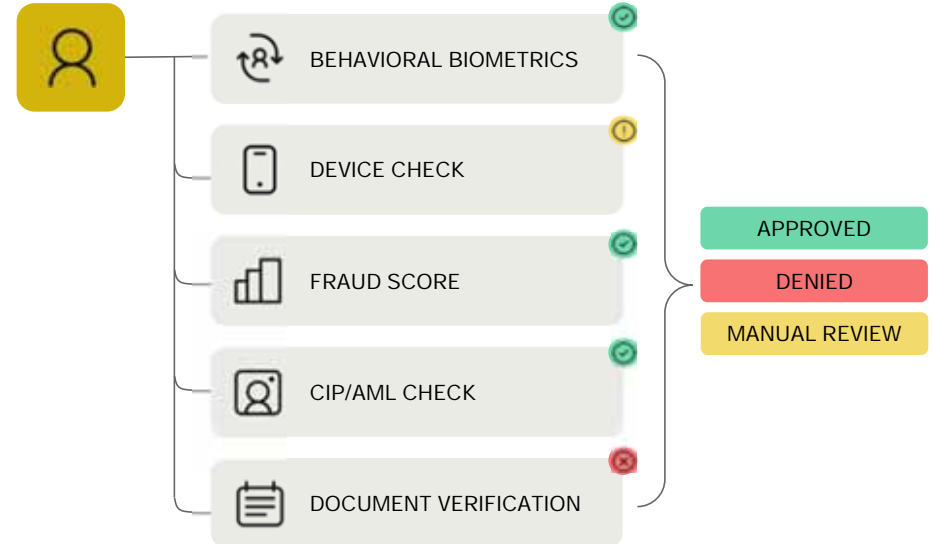
Linear & sequential evaluation amplifies errors, customer friction & increases manual processes.

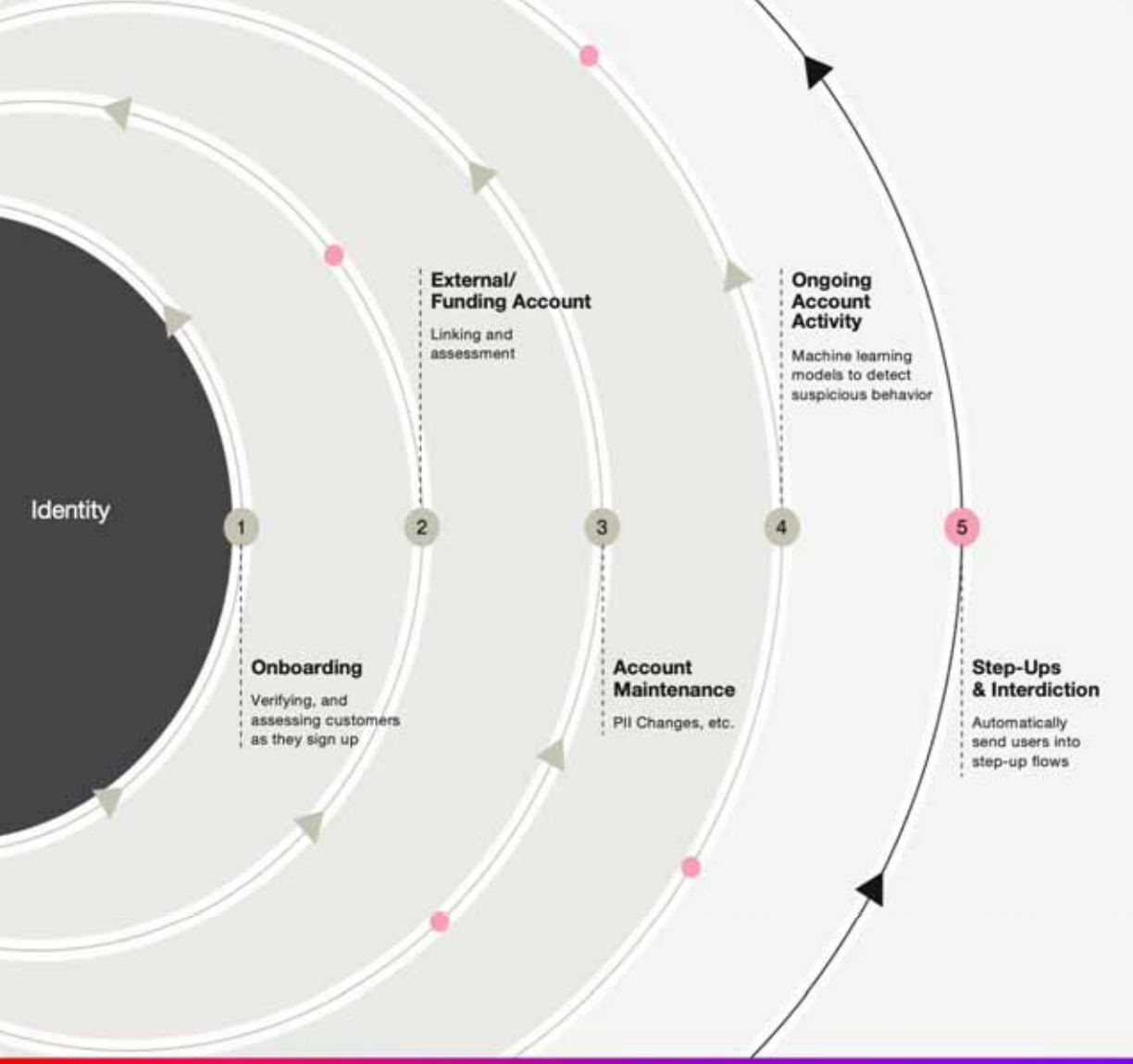


## What strong controls look like

Holistic →

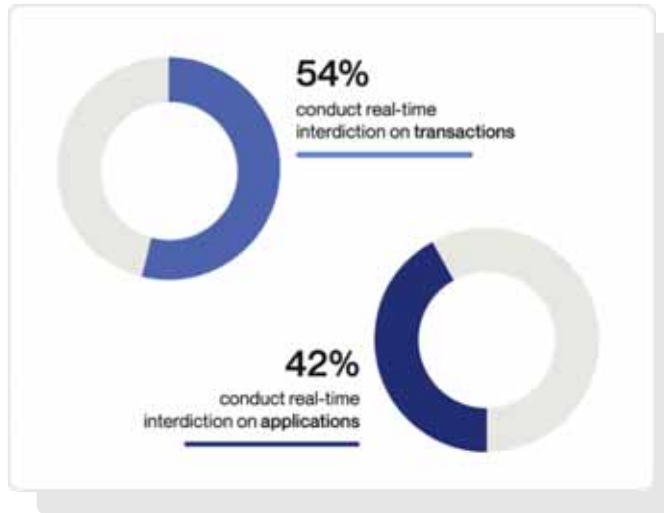
Select from a library of data vendors to screen your applications in real time.





**At the same time, financial institutions should continuously monitor customers throughout their lifecycle to prevent fraud down the line.**

# Use real-time interdiction to catch fraud threats post onboarding without increasing abandonment from good customers



RECENT TRANSACTIONS

Filter by [Clear Filters](#)

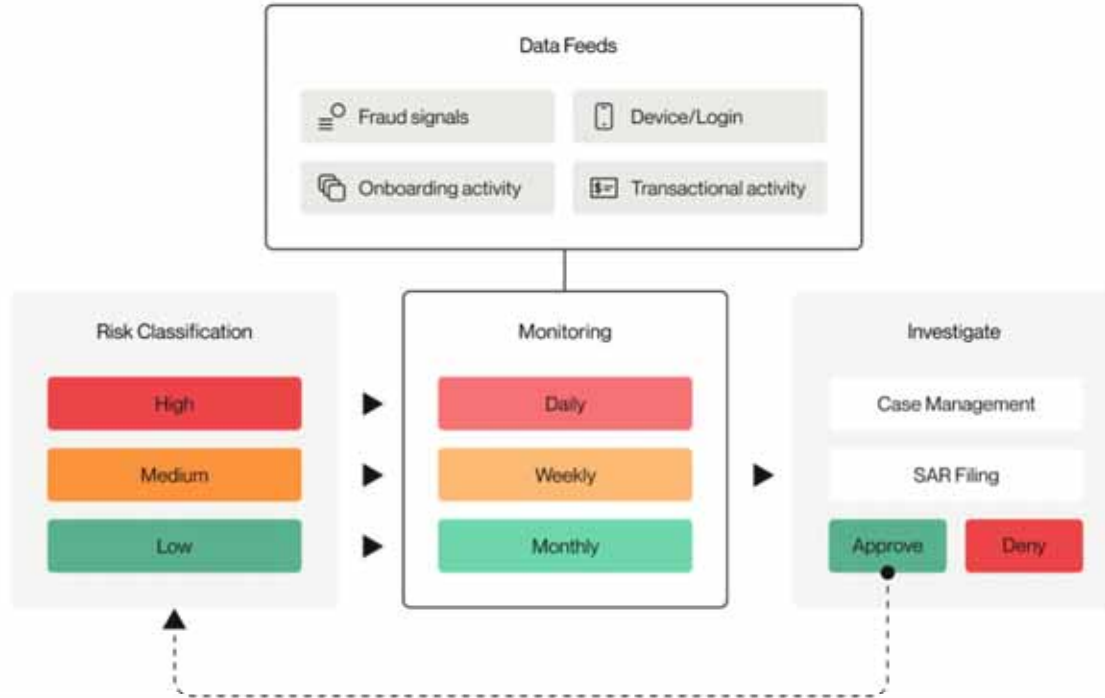
Date Range: All Time | Flow: All

Date	Amount	Status	Alerts	Transaction Type	Transaction Description	Currency Code
02/01/2020	-\$2,500.00	Approved	Alert	Mastercard Settlement	APPLE.COM/BILL 866-712-7753 CA	USD
02/01/2020	-\$500.00	Approved	Alert	Interlink Settlement	PETCO 1532 FRANKFORT KYUS	USD
02/01/2020	-\$9000.00	Declined	Alert	Mastercard Settlement	Amazon Digi*1W2WH4392 amzn.com/bill WA	USD
02/01/2020	-\$10.00	Approved		Mastercard Settlement	Amazon Digi*1W2WH4392 amzn.com/bill WA	USD
02/01/2020	-\$3.00	Approved		Mastercard Settlement	Amazon Digi*1W2WH4392 amzn.com/bill WA	USD

\*Source: Alloy 2024 State of Fraud Benchmark Report

Identify and contain fraud threats in real time by automatically rejecting or holding ACH and wire transactions upon identification of suspicious activity

# Automate digital identity verification with perpetual KYC



- Evaluate customers on an ongoing basis by assessing account activity, PII changes, and other triggers
- Take automatic action off the back of high-risk activity – instead of just sending these cases through for manual review, trigger a KYC refresh or route to step-up verification when necessary

Digital identity verification can help you grow your business.



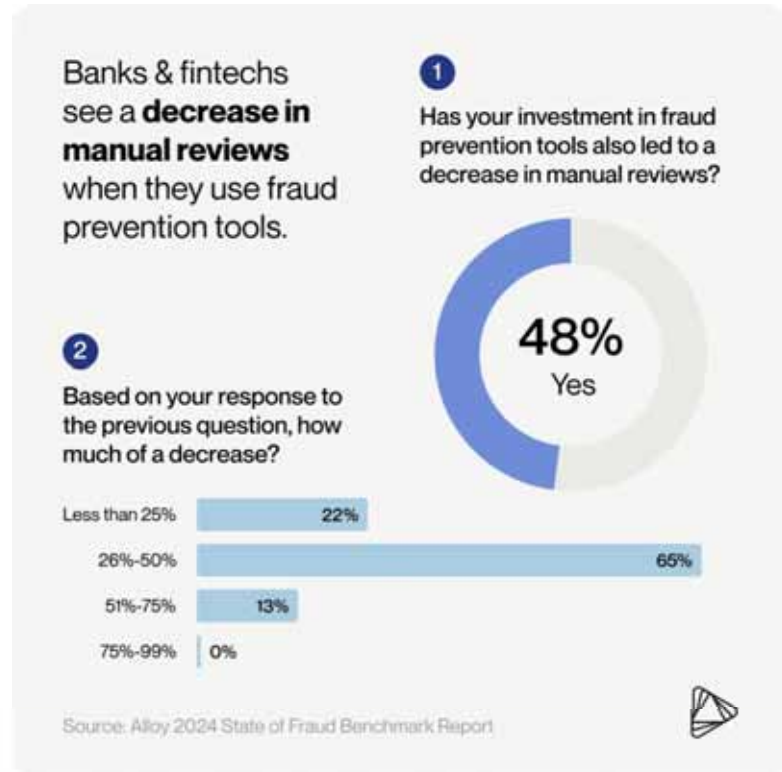
Retail banks that regularly practice customer experience optimization grow 3.2x faster than competitors that don't\*

\*Source: Forrester

THE FINANCIAL BRAND

FORUM

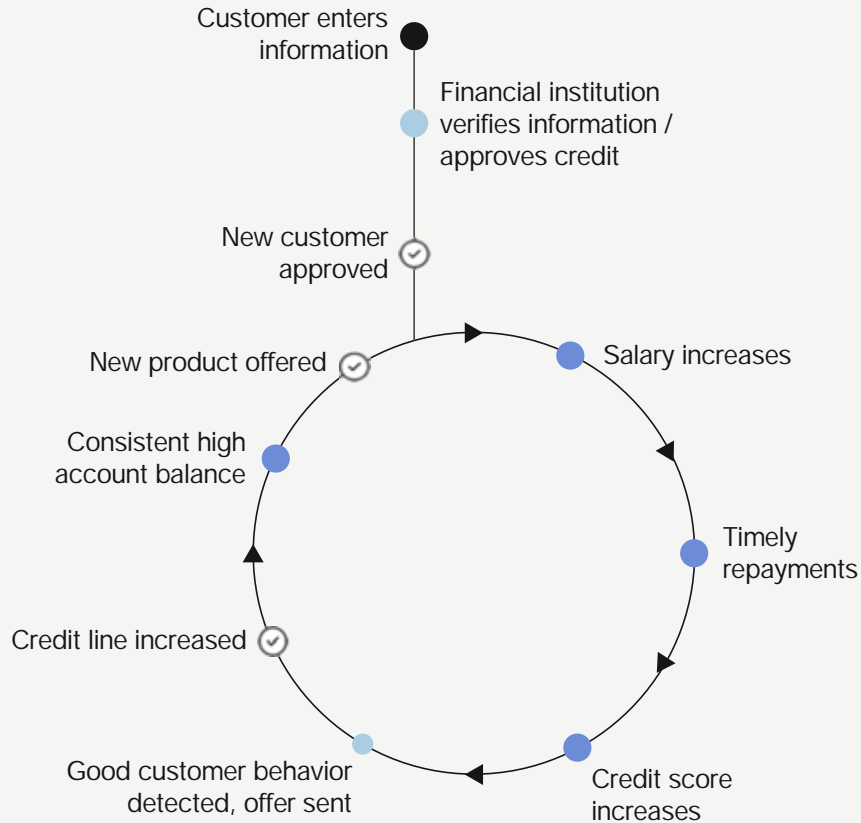
# Real-time digital identity verification helps reduce manual reviews



- Avoid “Day-2” review processes
- If you instead monitor risk signals in real-time, you have the opportunity to select the appropriate risk threshold on which accounts should be immediately approved or declined
- With this flexibility, you can:
  - reduce false positives
  - provide clients the opportunity to self-resolve
  - maintain a higher level of risk and oversight
  - reduce fraud team’s workload

# Digital identity verification creates new cross-selling and upselling opportunities

- Real-time, ongoing monitoring can help you increase the lifetime value of customers and identify new opportunities for growth
- Extend new product offers to customers practicing good habits



## Case study:

Live Oak Bank reduced  
investigation time by 30%\*

\*Source: Data sourced internally by Live Oak as of March 2024

FINANCIAL BRAND

**FORUM**

# The Challenge

- In 2021, Live Oak was using an in-house legacy onboarding platform for deposit customers, and between the time it took to review each application and the quality of data they were able to access, their existing process simply wasn't cutting it anymore.
- The team needed a solution that could automate some of the manual processes for their day-to-day operations so they could focus on expanding their product offerings and attract new customers.

'Historically, we've shied away from targeting small balance lending simply because we didn't have a platform with the ability to scale — it takes a lot of time and effort to underwrite and feel confident about a credit decision.'

**Tristan Manley**

SVP, Small Business Banking Product Leader

# The Outcome

- Live Oak enlisted Alloy to bring onboarding, transaction monitoring, and credit underwriting into one centralized platform.
- By using a wide array of data to put identity at the center of their onboarding process, Live Oak turned digital identity verification into a growth vector for their business.

27%

decrease in fraud YoY

8%

decrease in manual review rate

30%

reduction in investigation time

FINANCIAL BRAND

FORUM

## Case study:

Jovia Financial Credit Union decreased  
daily fraud volume by 35%

# The Challenge

- Jovia Financial Credit Union is an 85-year-old Long Island based financial institution serving 200,000+ members with more than \$4.5B in assets. The organization expanded nationwide in 2022.
- Within 10 months of Jovia's expansion, the number of daily applications, fraud, and account closure rates rose drastically.
- Unable to separate risky applications from genuine ones in real-time, there were times Jovia was forced to turn off their online application form and stop instant booking of accounts in order to manually review 100% of applications. This cumbersome process created a significant backlog and restricted new customers from onboarding during a critical period of growth.



# The Outcome

Jovia used Alloy to implement real-time fraud mitigation that leveraged best-in-class risk checks and expertise so they could return to servicing their customers.

**35%** Decrease in fraudulent applications

**0%** Negative impact on approval rates

“We had been running deposit performance checks on applicants. After implementing Alloy, we were able to save the cost of these checks for fraudulent individuals.”

**Evan Get**  
Business Systems Analyst at Jovia

# ACTION ITEM #1

Layering strong controls at onboarding is key to identifying fraudsters before they can steal money.

## ACTION ITEM #2

Use step-up verification on riskier customers to request more information, while sending good customers to approval.

# ACTION ITEM #3

Conduct real-time passive and active monitoring to ensure customers continue to make safe transactions.



# Questions?

#fbforum

THE FINANCIAL BRAND

**FORUM**

# Thank you!

**Sara Seguin**

 sara@alloy.com

 @usealloy

THE FINANCIAL BRAND

**FORUM**