Fraud Protection & Compliance
Identity & Authentication

Beyond biometrics:
identity proofing, authentication, and the customer experience

Q&A

Liz Lasher

Vice President, Fraud Product Marketing & Portfolio Strategy

As Vice President of Strategy for FICO's Fraud, Security, and Compliance Solutions, Liz helps to direct and cultivate communication about FICO's technologies, products, and competencies.

Twitter @lizfightsfraud

"With digital onboarding, banks can deliver a genuinely seamless and consistent customer experience, while dramatically improving the speed and efficiency of underlying complex operational processes."

Liz Lasher

Vice President, Fraud Product Marketing & Portfolio Strategy

FICO

As consumers continue to shift their banking activity to mobile devices, the industry is evolving as well. “Everything mobile” is driving digital transformation and, unfortunately, new fraud opportunities have come along for the ride. While consumers demand their banks protect them from fraud, enhanced protection must be delivered with a customer experience that is fast, easy, and consistent. In this Q&A, Liz Lasher explains how innovations in biometrics and behavioral authentication, combined with machine learning analytics, are creating trust in digital identities while streamlining complex onboarding, fraud, and compliance processes.

Q:
Why don’t biometric credentials provide adequate authentication? What more is required?

A:

Used alone, biometric data — such as your face, voice, retinal scan, or fingerprint — can be dangerously vulnerable to theft and reassignment. Biometrics are, after all, static attributes that cannot be changed. At the same time, they are a core component of effective authentication, which is composed of three elements: what you have, what you know, and what you are. When used in conjunction with additional attributes, biometrics add an extremely powerful layer of protection.

For example, biometrics are only one element of identity proofing — the digital process of onboarding customers without requiring face-to-face verification. It’s all about establishing trust in a digital identity and starts with what you have: you take a photo of your government-issued ID (a passport or license from anywhere in the world), and then take a selfie. Our solution, FICO® Falcon® Identity Proofing, then corroborates the information between those two inputs to verify your identity and establish your digital identity.

When you’re taking a photo of your ID, Falcon Identity Proofing analyzes elements of that ID to establish its legitimacy — elements such as its hologram, and an optical character read (OCR) of the text and machine-readable zones such as a QR code — while extracting a picture of you from the photo on the ID.

When you take a selfie, the software then executes sophisticated machine learning algorithms to detect liveness (i.e., the selfie is of a live person) and confirms that the ID has not been spoofed. The selfie also proves that you have possession of the ID card.

Q:
When are biometrics not a reliable authentication method? And why does that matter?

A:

For the three categories of authentication — what you have (possession), what you know (knowledge), and what you are (inherence) — the most common biometric used is the fingerprint. And while the fingerprint might seem to be an inherence factor, it turns out more than one person can register fingerprints on a phone, so, in this instance, they became a possession factor. Specifically, the fingerprint really doesn't capture who you are if you're dependent on the device and don't have independent biometrics; it becomes an element of what you have.

What you are can also be established by user behavior and device telemetry. FICO® Falcon® Authentication Suite includes behavioral authentication capabilities. These factors non-intrusively examine user patterns, such as keystroke analysis of the way you enter your password, geolocation, and other behaviors around your device, such as which browser you prefer. These patterns create a signature, something unique to you.

Back to biometrics, FICO's voice signature capabilities allow you to enroll in online and mobile banking by saying a short phrase, such as "Love my kids," three times while taking a selfie. By having the factor be specific to your banking app (rather than your device), you establish a mechanism to prove inherence. Voice biometrics provide a fast, easy way to create a more frictionless, seamless experience for the consumer. They can be used to log into the banking app and verify high-risk transactions involving large dollar amounts, wires, or other unusual characteristics.

Q:
How are FICO® Falcon® Identity Proofing and FICO® Falcon® Authentication Suite being used in the real world?

A:

FICO® Falcon® Identity Proofing is essential for a true, and truly seamless, digital onboarding experience. There are multiple functions at play here — establishing the customer's digital identity, assessing credit risk, and doing fraud and AML compliance checks such as KYC (Know Your Customer). With digital onboarding, banks can deliver a genuinely seamless and consistent customer experience, while dramatically improving the speed and efficiency of underlying complex operational processes. It's essential to create a positive customer experience for security checks. If not, users will abandon them and defeat the entire purpose of these new security protocols.

Falcon Identity Proofing is also used for electronic KYC (eKYC), a use case that is rapidly growing in Asia Pacific and in virtual banking, as well as at large, global banks. Digital authentication allows banks to build operational efficiencies during not just the initial KYC period, but on an ongoing basis, as well — critical capabilities in reducing money laundering and other financial crimes.

Get started today with risk-based, AI-driven identity proofing and authentication services, to deliver customer experiences that are consistent, seamless, and frictionless.

www.fico.com/identity

www.fico.com/authentication

Enrollment is typically the weakest link for fraud authentication capabilities. FICO offers both robust identification proofing and authentication capabilities to bridge the gap, and the FICO® Falcon® Authentication Suite functions as an integrated authentication hub. In this way, FICO offers a wide range of authentication factors that banks can mix and match. These include biometric capabilities, multifactor authentication such as mobile app push and QR code recognition, and behavioral authentication. With mandates, such as PSD2, regulators have set the technical standards and defined precisely how banks must link their technology platforms to outsiders. Falcon Authentication Suite helps ensure that banks meet Strong Customer Authentication obligations.

Together, FICO® Falcon® Identity Proofing and Falcon Authentication Suite provide a platform to establish and sustain trust in the digital identity, offering easy-to-use, integrated security across the customer lifecycle. Falcon Identity Proofing and Falcon Authentication Suite are strong complements to other FICO solutions that are used to manage risk and optimize customer interactions. For example, FICO clients using the FICO® Falcon® Fraud Manager solution will be particularly interested in understanding the account takeover and PSD2-compliant strong customer authentication capabilities that these new solutions provide; they are strong additions to the flexible, AI-empowered capabilities of FICO® Falcon® X.

FICO More Precise Decisions

4775EX 03/20 PDF

FOR MORE INFORMATION
www.fico.com
www.fico.com/blogs

NORTH AMERICA
+1 888 342 6336
info@fico.com

LATIN AMERICA & CARIBBEAN
+55 11 5189 8267
LAC_info@fico.com

EUROPE, MIDDLE EAST, & AFRICA
+44 (0) 207 940 8718
emeainfo@fico.com

ASIA PACIFIC
+65 6422 7700
infoasia@fico.com