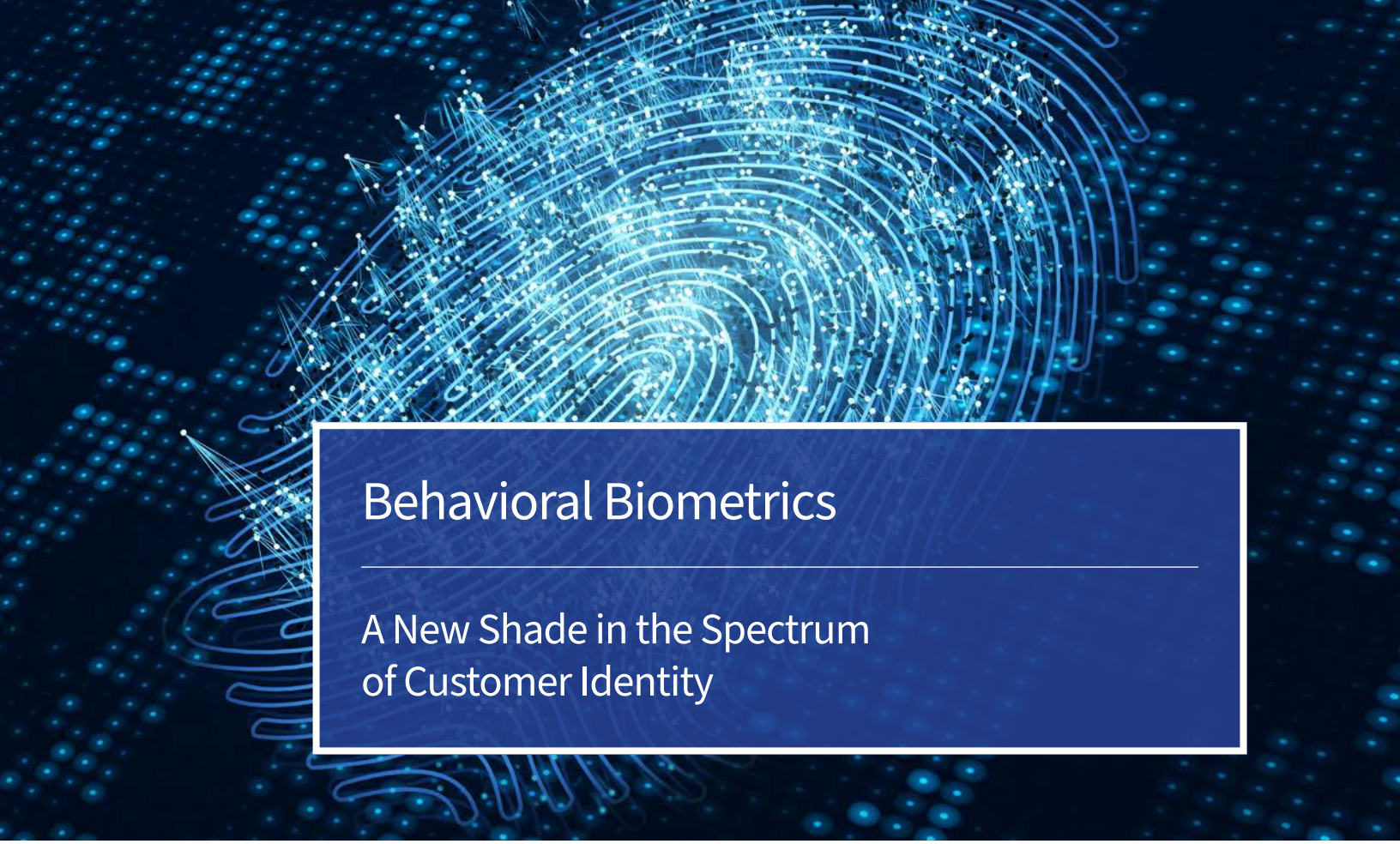

Behavioral Biometrics

A New Shade in the Spectrum of Customer Identity

Logging in to online banking on my laptop, I always pause on the higher numbered digits of my password. I spell the word out in my head: the first two digits are intuitive, the seventh and eighth require a little more effort.

Perhaps this is a unique quirk that few others share, but what if a fraudster was inputting this data instead of me? Looking down at their typed list of stolen credentials, or perhaps a grid of passwords on a different computer screen, it's likely that a fraudster would enter it completely differently. They wouldn't be recalling a familiar word as I do, rather they might be counting the letters, checking and re-checking that they are entering the correct digit.

Behavioral Biometrics is the term used to describe the way an online user interacts with a desktop, mobile or laptop device via their keyboard, mouse and/or touchscreen. It's about intransient features that are unique to you. Even if static pieces of information are breached, the way that information is used and inputted into websites, application forms and login screens is hard to replicate.

This only seeks to adds further credibility to the logic that layering of different tranches of information relating to a user's identity can build a water-tight system of protection. It also gives us new scope to question what, if anything, is "fraud-proof". Not only that, how can we continually seek to improve digital experiences for all users, regardless of age, location or digital maturity.

LexisNexis®
RISK SOLUTIONS

When layered with digital identity intelligence Behavioral Biometrics can create a new shade in the spectrum of identity; helping businesses to differentiate between trust and risk, fraudster and legitimate customer, human and bot.

We have collectively felt the impact for many years of stolen identities: passwords, credit card details, email addresses that are used in widespread attacks on individual consumers. Step forward digital identity intelligence: the armor that reliably defends against identity theft, device spoofing, impersonation, obfuscation and coercion by layering the fundamental pillars of a person's online identity. This can help organizations better understand whether a particular transaction is coming from a trusted user, or a potential threat.

However, there is always room for improvement. Supposing some of that digital identity intelligence is missing or immature, perhaps new digital users have a less complete digital identity, underbanked populations lack the history of online transacting that gives a holistic picture. A particularly tech-loving consumer may upgrade devices often and prefer the anonymity of a VPN connection, making his digital identity more ghostlike and harder to verify.

While digital identity intelligence can be reliably bolstered with layers of authentication such as physical biometrics tokens – iris scans or fingerprint verification – or one-time passcodes (OTPs) and push notifications, these tools can add a layer of friction to verification and authentication processes that might be inappropriate or lack cost efficiency for a particular transaction.

Neither are they immune to hacking, impersonation or spoofing. Consider for example, the case of researchers from NYU who developed fake fingerprints capable of deceiving fingerprint scanners. Or the all too common practice, by fraudsters, of intercepting OTPs via a well-timed SIM swap to fraudulently register for a new mobile banking app and then taking over good customer accounts.

When layered with digital identity intelligence Behavioral Biometrics can create a new shade in the spectrum of identity; helping businesses to differentiate between trust and risk, fraudster and legitimate customer, human and bot.

A newer and potentially more radical approach to utilizing behavioral biometrics is as part of an authentication workflow, that is to say building profiles or behavioral "fingerprints" of good trusted customers and using those as part of an authentication strategy to validate point-in-time transactions. This is particularly pertinent in the context of evolving regulations that are increasingly mandating secure authentication strategies to better protect high-risk transactions such as logins and payments.

The question arises — how unique is each person's interaction with their group of devices?

What type of tapper are you? When you type out your email address and proposed password when creating an account with a new merchant for example, do you type forcefully, with purpose, or almost silently, so as not to disturb your fellow colleagues or family members?

Does the movement of a mouse feel more familiar to you, or do you prefer your touchpad sensor? Do you tend to click through fields on a web page, or do you prefer to use the tab to navigate the input of data? Perhaps the way you move your mouse always curves to the left or right because you are left-handed not right.

Do you type text on your mobile with your thumbs and fingers or just fingers? One hand or two? What angle do you hold your phone? I remember being astounded watching a close friend deftly composing a message with her mobile flat on a table using just her forefingers. How unusual, I thought.

It's traits such as these, as well as a vast array of other attributes that can be gleaned from mouse, keyboard, touchscreen and sensor data, that can start to build up your own "unique" behavioral profile. Over time, it may well be possible to combine this fingerprint with other strong authentication tokens to create reliable, and passive, authentication workflows.

LexisNexis® Behavioral Biometrics

LexisNexis® Behavioral Biometrics was built in order to add an additional layer of defense for fraud and risk decisioning by combining the way a user interacts with their device, with existing digital identity intelligence, delivered via the ThreatMetrix® product.


RECOGNIZE BEHAVIOR


DETECT BOTS


IDENTIFY CLUSTERS


BUILD TRUST

It can help to reliably differentiate fraudulent from trusted behavior, separate human and non-human traffic, identify clusters of fraudulent behavioral fingerprints, and build trust over time with good returning users.


WHITE-BOX SOLUTION


PRIVACY-BY-DESIGN


LOW FRICTION


FULLY INTEGRATED

LexisNexis® Behavioral Biometrics has been designed as a white-box solution, is privacy-by-design, inherently low friction and fully integrated with existing technology.

LexisNexis® RISK SOLUTIONS

For more information, please call +44 (0) 203 2392 601 or visit risk.lexisnexis.com/FIM-EN

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.