WHITE PAPER

FRICTION-RIGHT FRAUD DETECTION

De-risking Frictionless Digital Banking Experiences

GuardianAnalytics.com

White Paper: FRICTION-RIGHT FRAUD DETECTION

The Rise of Digital Risk

Financial institutions and fintechs are competing for customers in a mobile-first, frictionless payments era.

With new payments-enabling technologies, mobile, and other new channels, including human contactless voice-driven banking and wearable devices, customers and businesses have shifted towards a friction-less payment experience.

Yet key challenges remain. Digital Banking is still ripe with fraud. Javelin Research Group has observed that Mobile Phone Account Takeover (ATO) cases have increased from 380,000 in 2017 to 670,000 in 2018 and New Account Fraud (NAF) losses where fraudsters open new accounts under victims' names has increased from $3.0 billion in 2017 to $3.4 billion in 2018 with common targets such as mortgages, student loans, car loans, credit cards.

Massive data breaches feeding a never-ending supply of stolen data on the dark web, combined with financial crimes sophistication and increasing identity and payments digitalization are building a perfect environment for exponential growth of synthetic identity fraud.

To regain trust and stay compliant in a digital world, there is a need to balance customer experience with risk of financial crimes.

In this whitepaper, Guardian Analytics, the leader in machine learning and behavioral analytics for financial crimes detection, is proposing a path towards Friction-Right Digital Banking that will bring financial institutions back to the center of Digital Trust, which is required to securely perform any digital banking activities.

This white paper is intended for CIO, CISO, Chief Risk Officer, Chief Compliance Officer, Fraud Manager & BSA Officer

Massive data breaches feeding a never-ending supply of stolen data on the dark web, combined with financial crimes sophistication and increasing identity and payments digitalization are building a perfect environment for exponential growth of synthetic identity fraud.

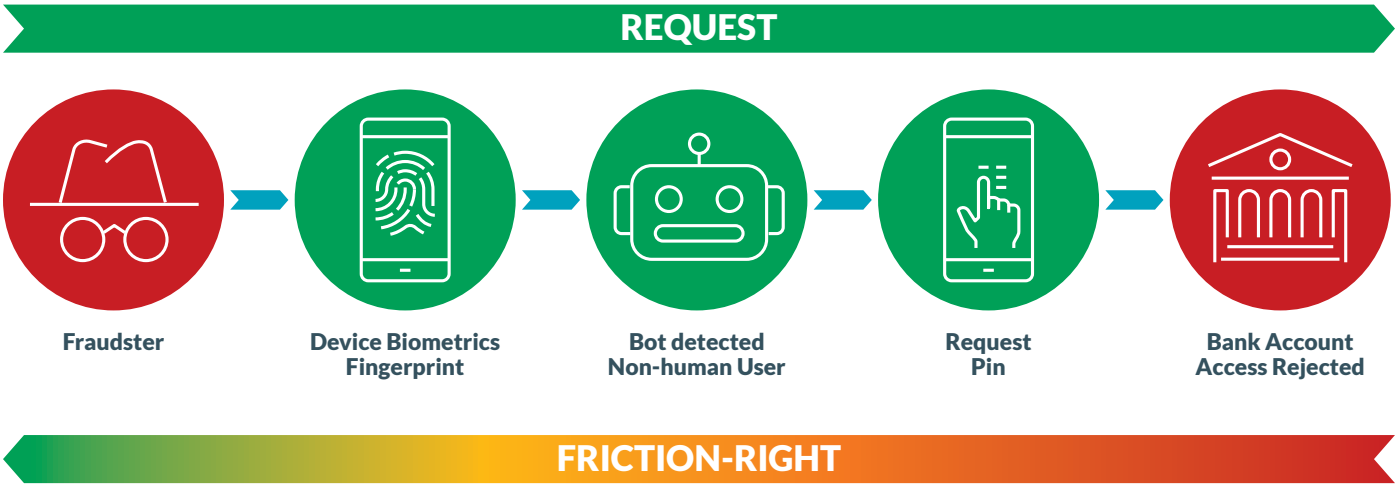
What is Friction-Right Fraud Detection?

The main design principle of Friction-Right Fraud Detection is to identify customers with behavioral biometrics, as opposed to static identity verification, self-learn customers' digital (online/mobile) and omni-channel payments activities, and enable the right-friction with multi-factor authentication. A simple way to visualize this concept is a closed loop starting with:

1. Learning "Something You Are" and Detect Anomalous Biometrics Digital Identity
2. Learning "Something You Do Online and Mobile" and Detect Fraudulent Digital Behavior
3. Learning "Something You Do with Payments" and Detect Fraudulent Payments Behavior

Analyzing across these three types of risks and enabling the right-friction with multi-factor authentication is the key to Friction-Right Fraud Detection.

For example:



You may have the right picture, device fingerprint, the right PIN, but if your biometrics behaviors or payments behavior are off, your account access request will still be rejected.

Why It Matters

Financial institutions and fintechs competing for friction-less digital transactions and a user-friendly onboarding experience need significant investment in infrastructure and expertise in regulations compliance.

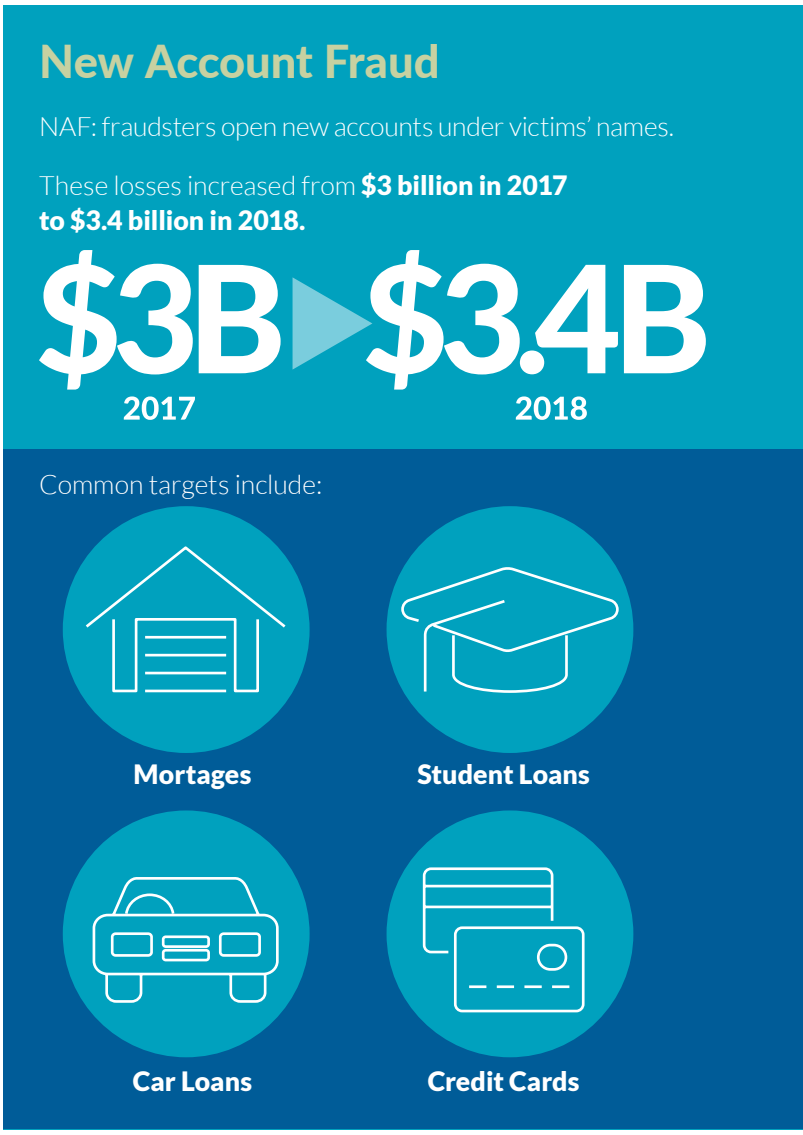
The Quest for Frictionless Digital Experience

Customers are more and more used to frictionless mobile payments with non-bank players such as Uber and the Amazon shopping cart, hence financial institutions and fintechs are shifting more and more towards a frictionless experience for opening new accounts. According to Financial Brand, this must be done urgently. Startups and fintechs are challenging incumbent financial institutions by finding opportunities to remove friction across all touchpoints in the customer journey. Opportunities to innovate abound — from the digitization of back-end process to point-of-sale service offerings and task automation, even the reinvention of "money" itself.

As customers are more accustomed to frictionless digital transactions, financial institutions and fintechs are also shifting towards a much more user-friendly onboarding experience.

As Synthetic Identity Fraud Surges...

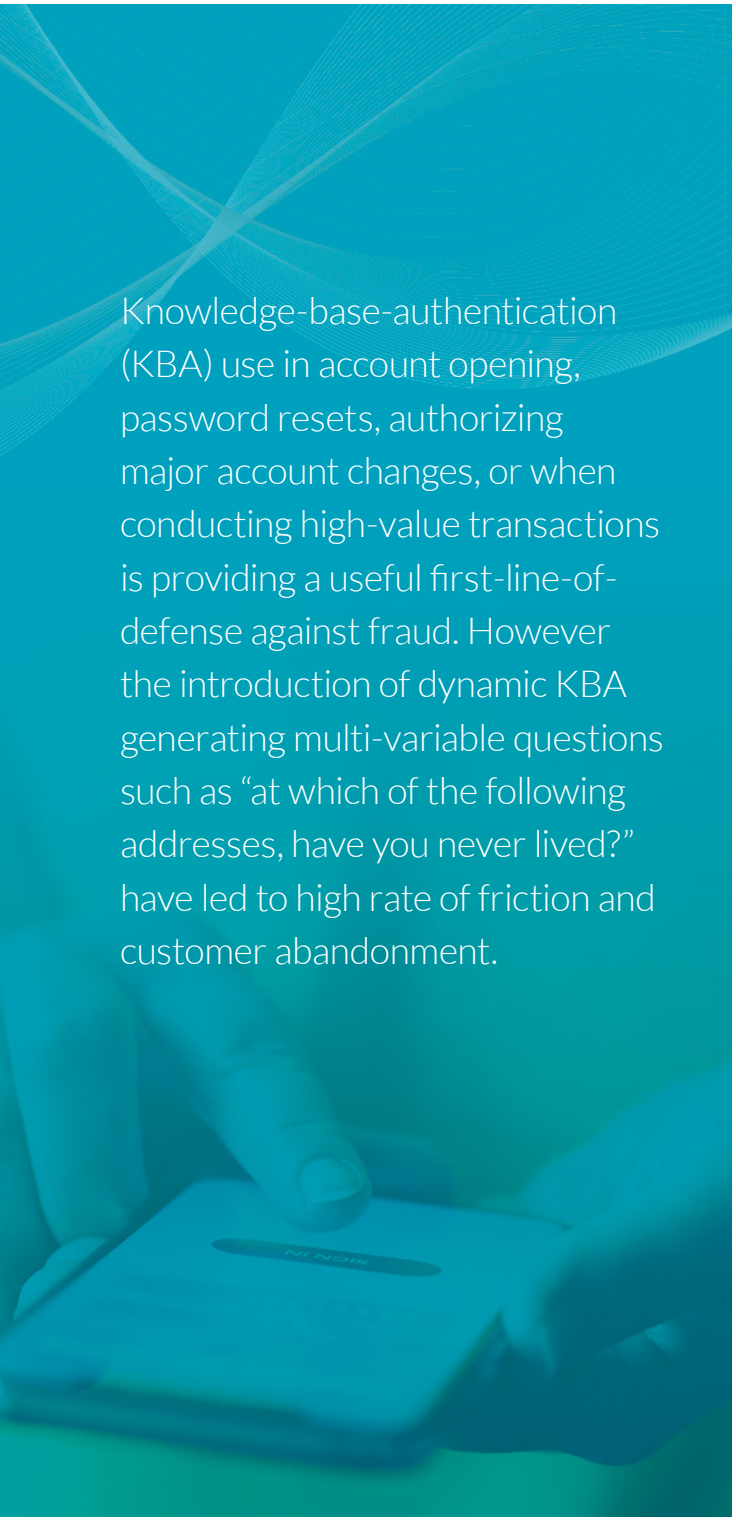
Synthetic identity fraud occurs when cybercriminals use either a combination of real and fake identity information – such as child's Social Security number, along with a false name, address and date of birth – or entirely false information to create a new "individual".



Millions of real Social Security numbers exist on the dark web for about $1 each. With a consumer's Social Security number (SSN), cybercrooks can file fraudulent tax return in their name to claim a refund, or use it to open bank accounts and credit cards. In the case of credit cards, a fraudster can run up a sizable debt, making no payments, while the consumer's credit takes the hit.

Conventional customer identity proofing is based on static information, even biometrics can be defeated. Static identity verification based on static personally identifiable information (PII) such as picture, name, address, date of birth or government identifier is being easily defeated by fraudsters.

As a result, fraud risk on account opening is surging. According to Javelin Research Group, New Account Fraud losses rose from $3.0 billion in 2017 to $3.4 billion in 2018.



Requires Rethinking Identity Verification

Requiring more document verification and introducing dynamic knowledge-based-authentication will increase the rate of friction and ultimately cause more customer abandonment.

Recent changes in KYC regulatory guidance, however, calls for even more static information collection and verification at different stages of the customer lifecycle:

- At onboarding, identity check is required for new account opening.
- During ongoing activities monitoring, any substantial account information changes will also require new account holder identity verification to avoid account takeover.
- Finally, anomalous and/or suspicious transactions will trigger a flag that may require additional account holder identity verification.

Knowledge-base-authentication (KBA) use in account opening, password resets, authorizing major account changes, or when conducting high-value transactions is providing a useful first-line-of-defense against fraud. However the introduction of dynamic KBA generating multi-variable questions such as “at which of the following addresses, have you never lived?” have led to high rate of friction and customer abandonment.

The Need for Liveness Risk Detection and Preventative Fraud Detection

Irrevocable real-time peer-to-peer (P2P) or account-to-account (A2A) payments are the main target of synthetic fraud, because when the “transaction is gone, it is gone”.

Synthetic identities profile themselves differently than traditional fraud because they access accounts using actual identity elements such as Social Security number, name, and date of birth, and swap new contact information (such as phone and address). As such, their behavioral digital identity can mirror the real user. With customers increasingly adopting real-time peer-to-peer (P2P) payments such as Zelle, RTP or soon FedNow, detecting fraud when the transaction has already occurred is too late. In the real-time payments’ era, post-transaction fraud means loss-recovery every single time.

The need to leverage liveness signals to detect non-human behavior versus real human behavior before the transaction is being even performed is a key capability for financial institutions and fintechs.

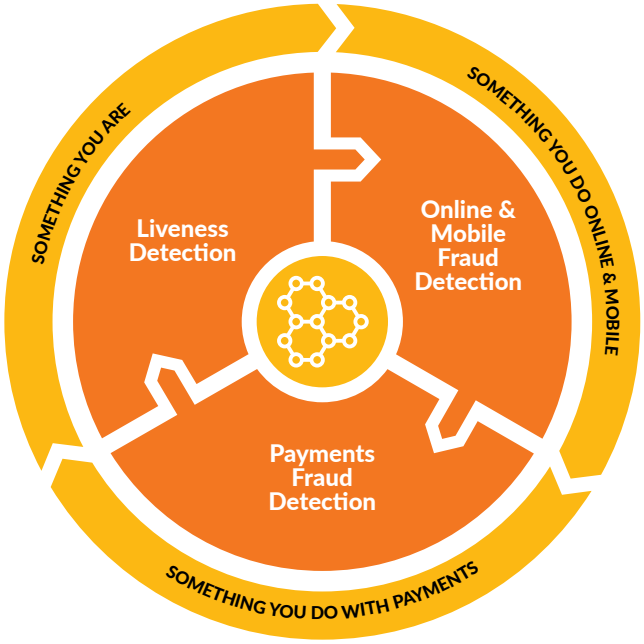
Why Guardian Analytics?

A Holistic Friction-Right Omni-Channel Fraud Detection

At the core of Guardian Analytics Friction-Right Fraud Detection Platform is our powerful, patented, unsupervised machine learning and behavioral analytics fraud detection risk engine. It self-learns fraud schemes performed over hundreds of financial institutions and detects fraudulent activities across multiple channels such as online, mobile, wire, ACH, check, P2P, Zelle.

Something You Are and Something You Do

A biometric such as a fingerprint, iris, voice pattern



A login into your mobile banking app from a specific location

A request for a wire transfer, an ACH transfer, a P2P payment...

To fight synthetic identity fraud, Guardian Analytics is integrating best-of-breed biometric technologies to detect liveness and score appropriately non real-user activities such as malware and bot.

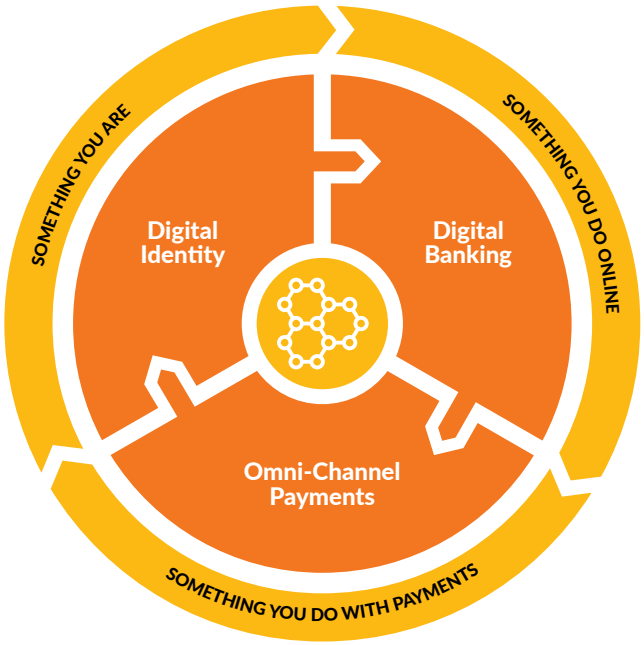
Together, these technologies help optimize the necessary balance between a smooth customer experience and protection from fraud.

Closed Loop Digital Identity, Banking and Omni-Channel Fraud Detection

The integration of the biometrics behavioral analytics with online, mobile banking and omni-channel behavioral analytics enables the closed loop fraud detection between digital identity, digital banking and omni-channel payments.

Digital Identity Behavior
Learn and detect human vs. non-human signals, fraud behavior risk, self-learn from person's history data familiarity. Enables friction-right with 3rd party MFA.

BIOCATCH



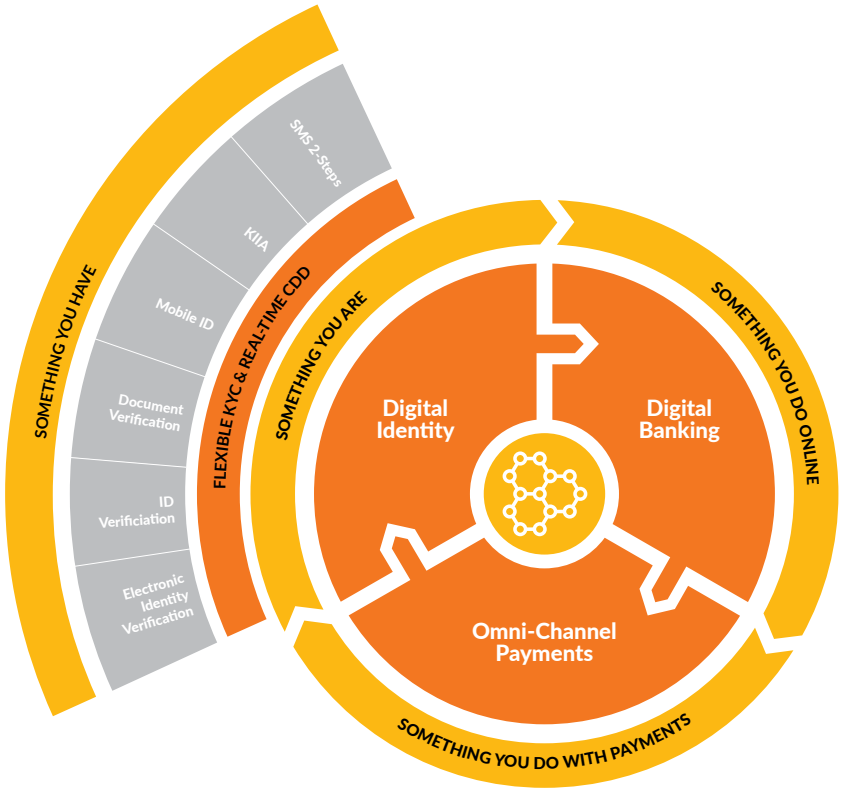
Digital Banking Behavior
Learn and detect your online and mobile authentication patterns including your user account management activities.

Omni-channel Payments Behavior
Learn and detect your payments transactions patterns, baseline frequency, recipients, transactions velocity, detect fraud risk, enables payments interdiction/intervention.

Digital Identity Integration with KYC & CDD

According to Aite Group, new account fraud rates in the online channel are "eight times that of accounts opened in the branch." Aite also projects that digital and mobile demand deposit account (DDA) applications will represent 45 percent of total account opening volume in 2020. One of the reasons New Account Fraud (NAF) increased from 2017 to 2018 is that many banks are not screening for out-of-pattern behaviors and not having enough fine-grained customer risk rating scenarios considering the new gig economy and the attraction of crypto currencies. Without combining static identity attributes and liveness identity detection, fraudsters have the advantage. Because they have access to compromised data, their application can look completely legitimate to traditional ID verification systems.

By integrating flexible KYC and Real-time CDD with digital identity, digital banking and omni-channel fraud detection, you can complement the account opening process with digital identity verification.



Something you have

Something you are

Something you do

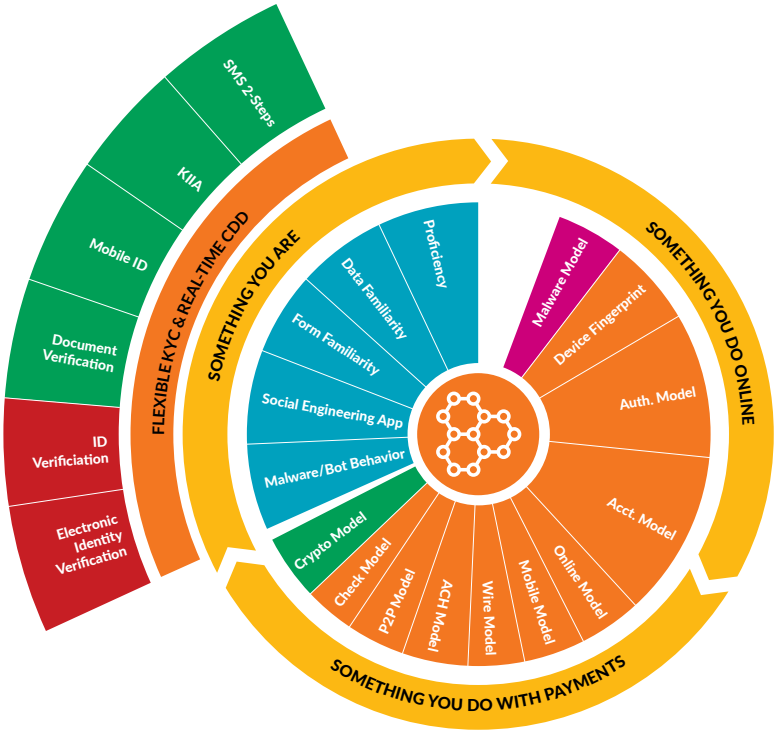
By integrating device biometrics (e.g. 3D facial liveness verification) with device fingerprint (e.g. OS, IP velocity, service provider change, phone type change) and other identity-related data points, it will increase the ongoing customer risk assessment accuracy and raises the cost to breach for the fraudster.

"Best-of-Breed" Machine Learning and Behavioral Analytics Hub

Enterprise financial crimes detection has changed significantly. Previously, single supplier solutions will static rule-based engines requiring multi-million-dollar consulting fees for deployment and tuning were the norm.

Increasingly, this 'one size fits all" approach cannot scale with the volume of data financial institutions have to cope with across digital and non-digital channels. Furthermore, this costly approach is being defeated by sophisticated fraud.

Guardian Analytics leverages expertise in machine learning and behavioral analytics, strong innovation in cloud data storage, elastic compute, and advanced visualization to bring a modular approach to enterprise financial crimes management.

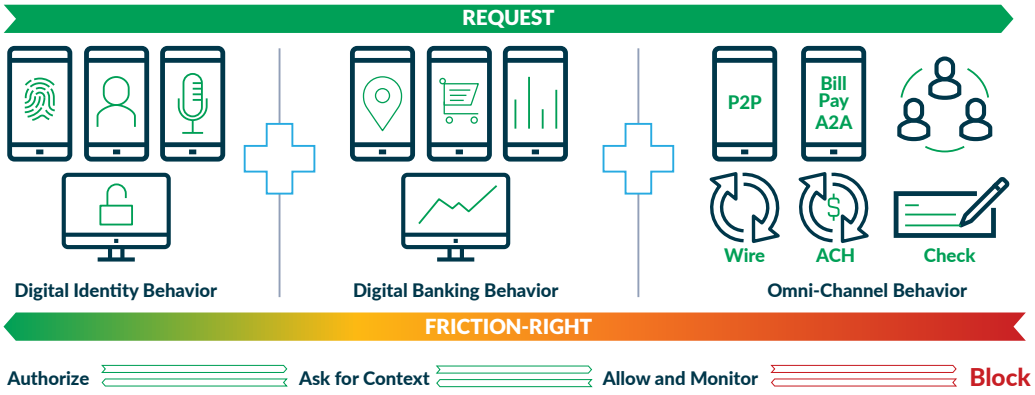


The key advantages of this approach are:

- **Accuracy:** Best of breed technologies are faster and better at detecting new fraud schemes.
- **Reliability:** Detecting fraud uses multiple "spokes" of technologies. If a single "spoke" does not perform, the hub can still function with the other "spokes".

How it Works

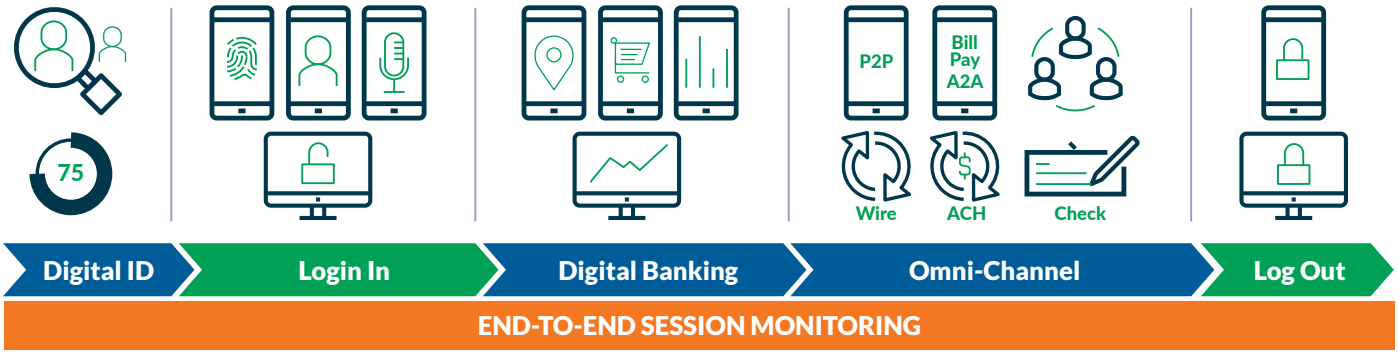
Digital Friction-Right Payments as-a-Service



End-to-End Session Monitoring Cross Channels

From digital identity verification, to login, online and mobile activities, and omni-channel payments behavior, Guardian Analytics machine learning and behavioral analytics is analyzing all events for risks of financial crimes and producing risk scores that can be used for multi-factor authentication decisioning.

From onboarding with a flexible KYC form and Configurable Customer Risk Scoring, to Online & Mobile Login/Logout Behavior, and Payments Transactions Behaviors, Guardian Analytics is analyzing all the events in real-time to detect risk of fraud.



As financial institutions and fintechs compete for new customers in a today's increasingly frictionless payments market, it's important to understand and have the right tools and technologies to balance consumers' expectations of frictionless transactions with the need to protect both consumers' and organizations from increasingly sophisticated fraud schemes and other financial crimes.

Guardian Analytics offers the right combination of machine learning and behavioral analytics to create Friction-Right Digital Banking, which enables financial institutions optimize this balance and enable secure yet customer-friendly digital banking.

ABOUT GUARDIAN ANALYTICS

Guardian Analytics is the pioneer and leading provider of behavioral analytics and machine learning solutions for preventing banking and enterprise portal fraud. Hundreds of financial institutions have standardized on Guardian Analytics' innovative solutions to mitigate fraud risk and rely on the company to stop the sophisticated criminal attacks targeting retail and commercial banking clients. With Guardian Analytics, financial institutions build trust, increase competitiveness, improve their customer experience and scale operations. Guardian Analytics is privately held and based in Mountain View, CA. For more information, please visit www.guardianananalytics.com. Guardian Analytics is a registered trademark of Guardian Analytics, Inc.

650.383.9200 2465 Latham Street, Mountain View, CA 94040

Guardian Analytics®

GuardianAnalytics.com