An InAuth White Paper

The Importance of Knowing Your Device in a Digital World

Deliver Real-time, Frictionless Digital Experiences While Mitigating Fraud

InAuth

Digital Intelligence Experts

FOLLOW THE **MONEY**

Although he denied ever saying it, infamous bank robber Willie Sutton is best remembered today for giving one memorable reply to a question. When asked why he robbed banks, he answered, “Because that’s where the money is.”

This simple explanation outlines an easily understood dynamic – where money goes, criminals are soon to follow. And with the number of data records stolen, lost, or exposed worldwide hitting 2.6 billion in 2017[1], there is a multitude of personally-identifiable data (PII) available for fraudsters to use to commit fraud in the anonymous, online world. According to PwC’s Global Economic Crime and Fraud Survey 2018, 49% of respondents said their companies had suffered fraud, up from 36% in 2016 – a rise driven by rising global awareness of fraud, a more robust response rate, and greater clarity around what ‘fraud’ actually means.

The increasing sums of money, number of users, volume of transactions, and speed at which it operates make the digital channel an attractive target for fraudsters who use a variety of techniques to commit fraud, which can be broken into the following categories:

NEW ACCOUNT OPENING & APPLICATION FRAUD, where fraudsters open an account with a true or fake identity

Fraudsters are increasingly moving their business online. The 2018 Identity Fraud Study by Javelin Strategy & Research revealed that the number of identity fraud victims increased by 8% (rising to 16.7 million U.S. consumers) in 2017, with the amount stolen totaling $16.8 billion. Fraudsters commit identity fraud by using compromised PII to open accounts using stolen identities, particularly in digital channels where they can remain anonymous. With some companies pushing to open accounts faster to generate more revenue and gain market share, there is less time for manual review to prevent fraud.

PAYMENTS FRAUD, where fraudsters use compromised card or account credentials to make purchases

Payment fraud can be described as:

- Fraudulent or unauthorized transactions
- Lost or stolen merchandise
- False requests for a refund, return or bounced checks

Ecommerce businesses rely on electronic transactions to charge customers for products and services. The increased volume of electronic transactions has also resulted in an increase in fraudulent activities.

ACCOUNT TAKEOVER FRAUD, where fraudsters obtain access to a legitimate user’s account

Customers are associated with accounts that store personal information, financial information, and purchase history. Fraudsters often hack into these accounts through phishing schemes as well as by hacking into databases to steal usernames, passwords, credit card numbers, and other personal information.

[1] Gemalto, Breach Level Index, April 2018

FOLLOW THE **MONEY**

Many industries are undergoing necessary digital transformations, attempting to provide real-time decisions and enhanced digital experiences. Security needs to be a priority when such innovation takes place or fraudsters will quickly adapt and find any potential points of exposure. Whether a financial institution, retailer, insurance provider, lender, travel and transportation business, or any other business, it's key to understand the trustworthiness of the person interacting within your digital channels.

Security ecosystems must include advanced digital intelligence in order to identify trustworthy and risky devices and deliver the best customer experience throughout various points of the user's digital journey including:

- Account Changes
- Payment Transactions
- Money Movement
- Card Provisioning to mWallets
- Bookings
- Payouts
- Loyalty Redemption
- Gift Card Purchases

This white paper will examine "Know Your Device" (KYD) as a method to not only protect against fraud, but also enhance your customer's digital channel experiences and compete in a crowded marketplace.

KYD: A Necessary Protection Against Fraud

To counter the predicted fraud increase in digital channels, businesses will need to enhance their security capabilities by employing multiple layers of authentication and requiring users to provide additional information, above user name and password, to prove they are legitimate. Key to this strategy is KYD security – utilizing the digital intelligence elements provided by the devices consumers use to transact with in order to assess risk.

This insight provides businesses the confidence necessary to allow good consumers to transact with the least amount of security steps necessary, helping to provide a more frictionless experience. At the same time, those devices with high-risk indicators, a fraud history, or a negative reputation among other businesses can be challenged or denied altogether to protect the organization and its customers.

Next-generation digital intelligence technology is available for businesses to use trusted device identifiers that help to recognize returning customers. Trusted device identifiers utilize the attributes of the device to create a unique ID that doesn't suffer change if a device is factory reset or the operating system changes. This makes them a reliable second factor of authentication for a login or transaction scenario.

Typically, once a fraudster has used a device to commit fraud, they may try to make it appear as a new device to avoid negative lists or velocity checks. However, when a device is associated with a trusted device ID, that ID can be used to uniquely and consistently recognize the device along with an associated transaction history. Repeated use of a device by a fraudster will then be easier to recognize and block in future fraudulent attempts.

Digital intelligence technology can also be used to detect and analyze unusual device behaviors that can be leading fraud indicators including

- non-typical location
- geolocation inconsistencies
- unusual access times
- velocity across many accounts
- non-human activity and evidence of bots
- cloaked root and hidden jailbroken devices
- mobile apps that have been tampered with
- devices with malware or crimeware installed
- evidence of spoofing tools, emulators, or proxies
- device attributes that have changed significantly from what is normally expected
- negative device and associated identity reputation

Optimize The Digital Experience

The widespread adoption of digital channels continues to lower transaction costs to a fraction of their original price and has made higher volume transactions possible, all very attractive to business operations. However, the technology has also lowered the human interaction involved, as well as the time allotted for proper evaluation of requests. There is also a balancing act that businesses are trying to strike between adding more layers of security to protect their company from fraudulent activity without creating a cumbersome user experience that causes abandoned transactions.

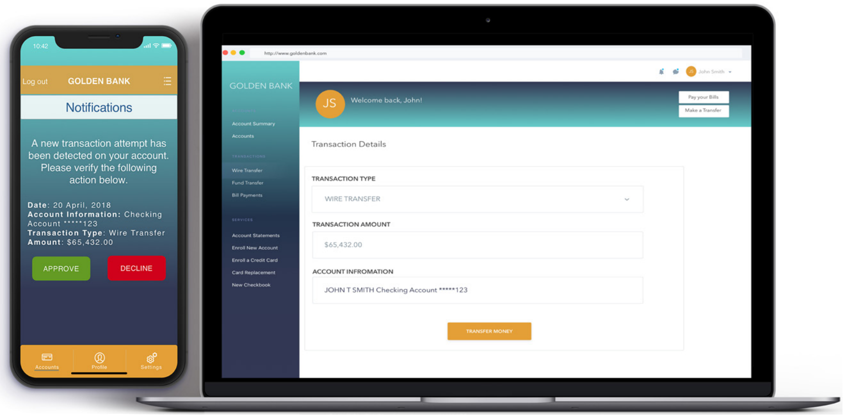
Ensuring digital security and offering a frictionless user experience no longer have to be mutually exclusive. By using next-generation digital intelligence technology, it allows the two forces to work together for mutual gain. When a device's trustworthiness can be established, the transaction can be both more secure and smoother for the user.

ENSURING
DIGITAL SECURITY
A FRICTIONLESS
USER EXPERIENCE

No longer have to be mutually exclusive

Imagine a scenario in which a business could identify that a user is logging in from their home Wi-Fi address on a clean device, and all device attributes are similar to the last login attempt. This could support a simplified login scenario or complement authentication methods, such as touch ID, and even some pre-authentication visibility into information such as account balances or prior order history.

The mobile device can also be leveraged as a trusted security token to shore up security gaps inherent in a browser session. For example, if additional authentication is required such as when verifying a high-value purchase on an ecommerce site or confirming an insurance claim payout in online session, knowing that a mobile device is trusted allows insurers to send contextual and transaction-specific messages to the user via its mobile app through a secure connection. Compared to the current method of delivering a one-time passcode through out-of-band email or SMS, which creates far more exposure and vulnerabilities, an "in-app" delivered, contextual, and transaction-specific message provides superior security for the organization, an improved experience for the customer, and a reduced transaction abandonment rate.



A new transaction attempt has been detected on your account. Please verify the following action below.

Date: 20 April, 2018
Account Information: Checking Account *****123
Transaction Type: Wire Transfer
Amount: $65,432.00

Transaction Details

TRANSACTION TYPE
WIRE TRANSFER

TRANSACTION AMOUNT
$65,432.00

ACCOUNT INFROMATION
JOHN T SMITH Checking Account *****123

A step-up authentication can also be provided as a biometric. Knowing and trusting the device will further secure the transaction by leveraging it as a secure token, ensuring the identity of the customer is known.

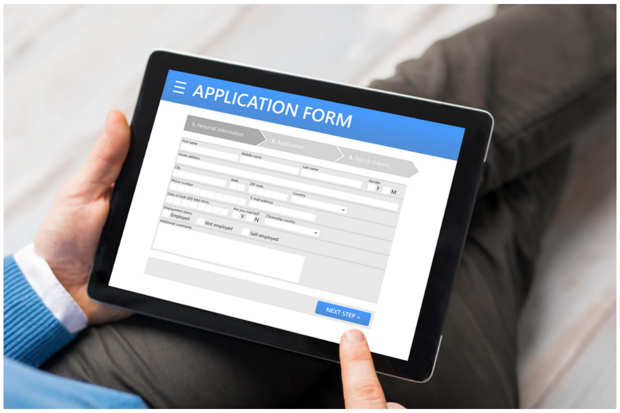
Expanding Your **Digital Vision**

When KYD capabilities are used to augment existing fraud and security policies, it provides the foundation for businesses to offer truly innovative features that take full advantage of the inherent benefits digital has to offer.

INCREASED MOBILE FUNCTIONALITY

Mobile Account Opening – With nearly 1 in 3 checking account applicants turning first to smartphones, mobile origination is a huge problem for the banking industry that is long overdue for a makeover. A combination of poor user experience, confusing fraud screening processes, and an inability in most cases to save and resume applications continue to force applicants offline, or to competitors. Within two years, more than half of all new bank account applications will involve mobile devices.[2] Therefore, organizations need to immediately prepare to service consumers that want to open an account using the mobile channel, or they will lose these potential customers to their competitors.

Cardless ATM - Imagine for a moment, instead of inserting a card into an ATM, it was possible to just wave a phone in front of it and the requested amount of money was dispensed. This is not a futuristic fantasy but is actually something that already exists. Spain has offered cardless ATMs since 2011, and the technology is currently available in the US for customers of Bank of America, Wells Fargo, JP Morgan, and Fifth Third Bank to name a few. These types of cash transactions, where money is instantaneously dispensed via mobile, can be made far more secure with a powerful authentication model and eliminate the cost and inconvenience of replacing lost or stolen cards.



INCREASED SELF SERVICE AND FASTER APPROVALS

Consumers are expecting real-time decisions and self-service on loan and credit applications, online transaction approvals, and insurance decisions such as faster claim payouts and new policy creation. All major industries are undergoing a digital transformation, and those companies that are failing to embrace digital are being disrupted and losing to their competitors. For example, the expectation for the insurance sector is to become more digitized with consumers expecting more self-service options and faster results. According to Ernst and Young, 80% of consumers are willing to use digital and remote channel options for their insurance needs.[3]

[2] Javelin, Overhauling The Mobile Account Opening Experience, March 2018

[3] EY, Global insurance trends analysis 2016, May 2017

Expanding Your Digital Vision

BIOMETRIC AUTHENTICATION

Today, many industry professionals are calling for the elimination of passwords entirely as they are a weak security tool. Likewise, emails and SMS are also insecure due to malware, interception, and manipulation of contact information by fraudsters. Call centers are both costly and highly vulnerable to social engineering. Today's top global security experts are raising alarms about each of these antiquated forms of authentication, which is why the incorporation of biometrics into the digital security equation is gaining widespread acceptance and adoption.

Biometrics represents a viable answer to these challenges, and fingerprint technology leads the charge as the biometric of choice among consumers due to ease of use, convenience, and familiarity as just another feature on their smart phones. By 2021, the number of mobile devices with biometric authentication capabilities will reach 600 million[4]. Customers will demand this functionality, and organizations must be ready. But for fingerprint biometrics to be truly secure, it must be combined with right device authentication solution in order to provide multi-factor authentication (MFA) that delivers maximum trust not only in the user, but also in the device itself.

REAL-TIME PAYMENTS

Stronger authentication models also enable faster payments, eliminating the processing lag and executing the transaction in real time. Currently many of the anti-fraud tools and processes used by businesses are either performed manually or geared around having a built-in time delay. These slower payment processes give institutions more time to detect and prevent possible fraud. In an always-on world, however, customers won't be satisfied with delays. Strong device authentication and risk assessment is necessary to provide immediate review of a user's device so faster payments can be enabled for these trusted users.

TARGETED MARKETING

In addition to fraud prevention, device authentication can enable geo-fencing services which are based on the device's (and thus the person's) location to drive targeted, proximity-based marketing programs. Using this approach, commerce providers can detect when a consumer is in proximity to one of their physical locations and then send the owner of the device a compelling marketing message or call to action in real-time.

[4] Juniper Research, Mobile Biometrics: Consumer Markets, Opportunities & Forecasts 2016-2014

An InAuth Whitepaper: The Importance of Knowing Your Device in a Digital World

Expanding Your Digital Vision

SUMMARY

Digital transformation is opening up a world of opportunity for individuals and businesses alike around the globe. However, organizations will not be able to fully realize the benefits and enormous potential that this emerging technology represents until they deploy next-generation digital intelligence solutions to properly secure their digital channels.

Confident authentication of the devices transacting within organizations' digital channels and utilizing digital intelligence to assess risk is a solid step toward fulfilling security objectives, empowering businesses to innovate, compete, and thrive in a digital world.

To learn how InAuth's solutions can help your business innovate, compete, and thrive in today's always-on digital world, contact us today.

ABOUT INAUTH

InAuth is a leading digital intelligence company deployed in many of the largest businesses around the globe. InAuth analyzes devices and associated identities to ensure trust with those interacting with your digital channels. InAuth's digital intelligence platform helps businesses verify identity, assess and mitigate risk in real time, optimize the customer experience, improve operating processes, and reduce cost. With safer digital transactions, banks, payment networks, merchants, insurance providers, and other organizations are better positioned to capture new revenue opportunities and compete more effectively in an always on world. Learn more at www.inauth.com.

AMERICAS

Headquarters
376 Boylston Street
Suite 501
Boston, MA 02116
855.801.0774

West Coast Office
227 Broadway
Suite 200
Santa Monica, CA 90401

Latin America Office
Eje 5 Norte 990
Building C, 1st Floor
Santa Barbara
Mexico City 02230
+52 (55) 52097037

UK & EMEA

Belgrave House
76 Buckingham Palace Rd
London, SW 1W 9AX
United Kingdom

ASIA PACIFIC

Australia
Level 9, 12 Shelley Street
Sydney, NSW
Australia 2000
+61 2 9152 2851

Level 14, 360 Collins Street
Melbourne, VIC
Australia 3000
+61 3 8374 7184

Singapore
Level 15, Marina Bay
Financial Centre
Tower 2
Singapore 018983
+65 6317 6414

InAuth