WHITE PAPER

Balancing Fraud Detection and the Customer Experience

Why it can be more important to identify the good customers than the fraudulent ones

sas
THE POWER TO KNOW.

Contents

The coveted convenience of digital transactions

Computing devices, even impossibly small ones you wear on your wrist or stash in your pocket, open up a world of possibilities.

Buy a plane ticket or summon an Uber car. Monitor your home or business. Apply for a loan, view account balances or pay bills. Attend business meetings from home or away. Listen to your voice mail. Send an email. Use your smartphone to pay for your cappuccino. Order groceries, clothes, a car or your next quarter's inventory without ever leaving the sofa.

It's hard to imagine any facet of our personal and professional lives that hasn't been redefined by the convenience of digital. It's no wonder consumers and businesses have been embracing digital and mobile ways in fast-growing numbers.

The banking industry has certainly seen it, with rapid growth in online and mobile banking for such activities as account opening, monitoring account balances, transferring funds or applying for loans. According to Juniper Research, by 2021, half of all adults worldwide will use a smartphone, tablet, PC or smart watch to access financial services – up 53 percent from 2017.[1]

Digital channels are a must-have in the industry as customers flock to the businesses that can offer that speed and convenience.

But there's a dark side.

The relative anonymity of digital channels opens up new doors for fraud. Financial institutions need to be able to verify a user's identity, but they can't compromise the speed and ease of the transaction for good customers. There's always the need to balance high security – which can mean higher friction and latency – with the need to provide a positive customer experience.

In the minds of customers, it's all very simple. Just stop every fraudulent attempt and approve every good one – because they want access to their money as quickly as possible, preferably immediately.

> Banks must find the delicate balance between letting transactions process unencumbered (so customers aren't frustrated by delayed access to their money) and doing the right level of diligence to detect and prevent fraud.

[1] Bhas, Nitin, "*Retail Banking: Digital Transformation & Disruptor Opportunities 2017-2021*," Juniper Research, February 2017

The risks are escalating

In 2018, online and mobile fraud drained an estimated $1.45 trillion from financial institutions, payment processors and other businesses, according to the payment systems company Vocalink, which also estimates that 47 percent of firms were victims of financial crime.[2]

Fraud is a thriving trade, for several reasons:

- **More account openings are taking place through digital devices and the internet**, which provide the access and anonymity fraudsters require. According to Javelin Strategy and Research, about 80 percent of adult bank customers in the US use online and mobile banking frequently.[3] That's a big target audience – and a vulnerable one. Account takeovers on mobile channels rose 107 percent from the first half of 2018 to the second half.[4]

  With remote transactions, the lender or creditor can't verify applicants in person through photo IDs such as drivers' licenses, passports and other paperwork. And a single fraudster can generate many spurious credit applications, which would be difficult or impossible with traditional in-person applications.

  Furthermore, the pressure to render real-time decisions on loan or service applications (or lose the business to a lender who will) cuts short the time available to do thorough due diligence.

- **It's easy to harvest all manner of personal identity credentials.** Data breaches spill a flood of information, much of it then easily obtained from the dark web. Cybercriminals steal, trade, augment and sell identity data not just to make money but also to build a more complete and convincing picture of stolen user identities. Credit bureaus now hold files created by fraudsters that are sophisticated enough to pass identity verification checks.

- **People unwittingly broadcast nuggets of their identity.** For a wellspring of factoids commonly called for in verification questions – your first car, where you met your spouse, the name of your pet, your elementary school – identity thieves need look no further than Facebook. Oops. In September 2018, Facebook reported a security breach that affected nearly 50 million accounts, potentially giving attackers access to view account information and use accounts as their own.

- **Automation scales fraud to new levels.** Automated bots have accelerated the speed and volume of fraudulent activity. According to ThreatMetrix, which provides digital identity technology to the financial services industry, a record 3 billion bot attacks were detected in just the second half of 2018.[5] Automated attacks can compromise more accounts and steal more data in less time, which leads to more exposure for more channels, services and companies.

In short, businesses are being forced to operate in a zero-trust landscape, but your customers have to feel trusted. It's a very fine line.

[2] *Vocalink On The Grim Facts Behind Financial Crime's $1.4T Toll*, PYMTS.com, October 2, 2018, https://www.pymnts.com/news/security-and-risk/2018/vocalink-financial-payments-crime-corporate-fraud/

[3] Javelin Strategy and Research, *Overcoming the Top 10 Challenges to Omnichannel Fraud Management*, November 2018

[4] ThreatMetrix, *2H 2018 Cybercrime Report*, December 2018, https://www.threatmetrix.com/info/h2-2018-cybercrime-report/, accessed March 19, 2019

[5] ThreatMetrix, *2H 2018 Cybercrime Report*, December 2018, https://www.threatmetrix.com/info/h2-2018-cybercrime-report/

Balancing security and convenience

"Efforts to stop these nefarious activities have sometimes led to overly aggressive policies and additional identity proofing requirements," says Mike Yeardley, Senior Director for Fraud and Identity at ThreatMetrix. "Customers get frustrated when they've got to jump through hoops to log in or complete a transaction, even as cybercriminals continue to find inventive new ways to bypass these same controls."

Consumers have very short patience for authentication and verification processes. They don't want laborious, multilevel logins. They don't want to answer multiple authentication questions or quizzes to prove they're not robots. In fact, they'll defect after a surprisingly short period of inconvenience.

"Bank executives are really struggling with this," says Shirley Inscoe, a Senior Analyst covering fraud, data security and consumer compliance issues for Aite Group. The authentication measures they're using have some gaps, or are just not as effective as they need to be. At the same time, you've got to balance that customer experience. I'm a consumer too, and I hate really invasive authentication measures. Most consumers do. They really need to reexamine their tools and strategies enterprisewide."

Smarter authentication, not more authentication

From the wide range of identity and fraud detection tools available, you would think the most powerful ones would be the most cumbersome to the user. Not so. Some of the most effective authentication tools are invisible to the user, while some of the more intrusive ones are losing their power.

Take knowledge-based authentication (KBA), for example. The customer is stalled by having to recall the answer to a security question, and thanks to major data breaches and a strong black market for the data, there's no fortitude in static KBA anymore. Conversely, there are analytics-driven techniques that provide high security value without inconveniencing the customer at all.

Here are some examples of approaches already proven in the financial services industry:

Connect the demographic dots

Do an applicant's details match historical records from credit bureaus and other sources? Is a Social Security number or account number associated with multiple birth dates? Does a 30-year-old have a transaction history that spans 40 years? Given the demographic data on the credit application, would the credit holder be likely to purchase from the type of merchants where the account is being used?

Connect the communications dots

The use of digital channels creates new information about a customer's digital identity – device fingerprint, IP address, geolocation and more. This data that can be folded into the analysis along with personal and credit bureau information to create a richer view of the customer (or the illusion).

Have we seen this device before? If so, was it associated with the same customer, account and provided information? Is a user who logged in from one location minutes ago now logging in from a different location using another device?

Does the interaction show any of the hallmark traits of unsafe activity such as location cloaking, spoofing, malware, bot attacks, session hijacking or phishing?

Assess past experience

What is the creditor's past experience with applications that included the same data element, such as the same device ID, address or SSN? Were any declined? Have any of the details of the identity been linked to fraud elsewhere? Negative information may prompt further due diligence to understand the relationships between accounts and applicants.

Find 'proof of life'

Many fraudulent identities, particularly synthetic identities, do not have records we would associate with a real person, such as driver's license, voter registration or property ownership. Lack of well-rounded life details can be a strong red flag to an identity that warrants a closer look.

Analyze the network

Network analysis plays a big role in understanding the connections (or lack of connections) among applicants, devices, open accounts and application data. For instance, does an account have authorized users who are not family members? Are payments from the same source (bank, account or device) being used to pay otherwise unrelated accounts? Visualizations of these links can be very useful both in assessing applications and conducting investigations.

Look for anomalies

Are credit lines fully used soon after account opening, or repeatedly maxed out and paid in full without carrying a balance? Has there been a spike in transaction frequency or amount? Is a payment coming by check when prior payments were made online?

Recognize faces

Several companies offer products that validate a user by facial recognition. The user takes a smartphone selfie and a photo of an identity document, such as passport or driver's license. The system compares the two. "It's very effective," says Inscoe. "I recently talked to two bankers whose banks are doing this not just for applications, but in their branch networks to eliminate account takeover."

With the breached data freely available on the dark web, traditional static authenticators and identity proofing methods are nearly useless. Usernames and passwords can be easily compromised using automated bot attacks. Two-factor authentication is useful but hardly foolproof.

The evolving risk environment calls for smart authentication based on a comprehensive view of the customer across the entire life cycle and all digital touchpoints.

Use behavioral biometrics to identify bots

Some pioneering banks are using analytics to determine if an online applicant or account holder is a human or a bot.

A first line of defense uses keystroke analytics. Does this online activity seem human-like? There's a certain cadence a person would make in completing an online application. Some sections of the form, such as basic demographic information, would be filled out fairly quickly. You know your address, date of birth and SSN right off the top of your head. But when you get to unfamiliar sections of the form, you may have to stop, read and understand the request – maybe look up the needed information. The cadence changes. Analytics can detect if the pattern of keystrokes has the natural flow of a human or the staccato rhythm of a bot.

Toward a comprehensive digital identity

A driver's license, Social Security number, face and fingerprint validate your identity in the physical world. Verification questions based on your life – childhood pet, where you met your spouse, birth month of your oldest sibling, etc. – augment that real-world, physical identity.

It's time to modernize the concept of identity for the digital world. We each have a potential digital identity based on our online credentials and activity – an amalgam of online behaviors, social profiles, device information, location, browser patterns, search history and more.

What device is being used, and where? Is it a trusted device and application? What kind of connection is being made? Using what email address? What is the transaction volume? How much time is spent on a given web page?

Over multiple transactions, this information builds a unique picture of that particular user – normal behavior, online personas and destinations, and more. It's an intricate online footprint that users create as they transact online. Digital businesses that can capture the nuances of this digital identity don't need to know the user's name to know who it is. This provides a unique and fresh opportunity to rethink the concept of identity and how to authenticate users online.

"This approach goes beyond device intelligence, beyond static identity data, beyond usernames and passwords," says Yeardley. "It takes us to a place of truly understanding the complex, networked interrelationships between every piece of information we know about an individual transaction – building this into a genuine global digital identity over time."

With this capability, businesses can build trust among good returning customers, authenticating them in real time and without friction. And if a customer's identity were to be compromised by a data breach or other infiltration, the system would detect anomalies in real time.

At the heart of every online transaction lies a gold mine of useful information. There are hundreds of dynamic data elements associated with a legitimate user and the device being used, none of which can be stolen or manipulated.

Instead of focusing on trying to ferret out the bad guys, the concept of digital identities shifts the focus to understanding the devices, behaviors and patterns of good users. When this process is informed by global-scale intelligence, anomalies instantly become evident.

Five pillars of effective digital fraud detection

The technology platform for accurate, real-time fraud detection without compromising the customer experience includes four key attributes:

A decision hub

As the rise in fraud incidents and losses makes clear, traditional silo and product-centric authorization systems are not enough. What is needed is a central decision hub that:

- Brings transaction monitoring and device monitoring together for analysis.
- Assesses activity at multiple levels.
- Combines multiple analytical approaches.
- Provides a unified view of an account/entity across the entire relationship.

You get the greatest precision when the decision hub is fed by crowdsourced data to create a deep and rich pool of insight. For example, the ThreatMetrix Digital Identity Network collates intelligence from approximately 35 billion global transactions a year, such as logins, payments and new account applications. This consortium data provides a wealth of real-time, cross-industry intelligence to accurately:

- Create digital identities for legitimate customers and transactions.
- Ensure true digital identities can't be faked or duplicated.
- Detect high-risk or fraudulent behavior in real time.

Data and digital identity intelligence

This is the depth of data from the myriad connections among devices, locations and anonymized personal information. This rich data resource about digital identities and their context serves as the foundation for analysis.

Analysis of nonmonetary events

In-session behavior can reveal a lot about a user. Most online/mobile users have regular patterns of engaging with merchants and financial portals. They use similar navigation patterns and a small number of devices. Departures from habit could signal unauthorized access. A strong authorization system can capture user behavior patterns from multiple sources and evaluate it every time a customer interacts or a payment transaction is scored.

When you can analyze behavior on an individual rather than a business level, you reduce false positives for frequent travelers or anybody who operates a little out of the range of normal or average behavior.

Hybrid analytics

When you layer multiple analytics methods, you can more accurately distinguish between legitimate users and fraudsters. For example, anomaly detection and predictive analytics can uncover new forms of risk by examining what's happening right now, not just comparing it to the past. Social network analytics can establish links that point to collusion or discrepancies that represent potential red flags. And self-learning techniques take fraud detection to the next level.

Machine learning

Unlike rules-based systems, which are fairly easy for fraudsters to test and circumvent, machine learning adapts to changing behaviors in a population through automated model building. With every iteration, the algorithms get smarter and deliver more accurate results. It's easy to see the value of machine learning to keep pace with the emerging risks of new payment channels.

Consider a consortium

When confirming an authentic identity by triangulating the data, obviously the more data you have, the more accurate the determination. Cast a wide net both within and outside the industry.

When you share information in a consortium environment, you can understand the normal combination of device, locations and other account markers that are associated with a real person. You can see the profile of that identity that has been seen by all these other organizations.

"The big 'aha' moment for a lot of organizations, especially on the financial institution side, is that they can benefit from the experience across the globe of all of these other, unrelated industries in informing their decisions," says Chris LeBaron, a Senior Director at ThreatMetrix. It's about gaining a holistic view of that person across as many intelligence points as possible – locally and globally.

"And when you tie that with the ability to share negative indicators across a trusted, targeted peer consortium network, you really start to drive decisions that are based on insight, intelligence and shared experiences."

Closing thoughts

The stakes for truly understanding an online user's digital identity have never been higher. Businesses need to verify true identity – digital and otherwise – authenticate accurately and identify high-risk behavior in real time.

At the same time, digital users expect a speedy and frictionless online experience. You can't alienate honest customers by making it cumbersome to perform an honest transaction.

With a multifaceted approach powered by analytics in a central decision hub – augmented by consortium data – you can manage the risk while meeting customer expectations for ease, convenience and trust. By bringing together and truly understanding multiple elements of every transaction, you can build a more holistic, complete picture of a user's digital identity. And with the computing power available today, you have the option to score all activity through the decision engine in real time.

Learn more

sas.com/fraud
www.threatmetrix.com

Financial institutions are always seeking that optimal balance between reducing the false positives that can damage customer relationships and the false negatives that can lead to financial loss for the institution. That requires analytics, the ability to detect anomalies that represent potential red flags – at the speed of now, in an ever-changing fraud environment.

To contact your local SAS office, please visit: sas.com/offices