EQUIFAX®

Discover Your Maximum Viable Person

Six Best Practices for Maximum Knowledge, Growth and Protection

Angela Jones applied for several accounts on your website yesterday. While new customers and accounts are exactly what your business is all about, there is a downside to doing business with Angela Jones… she may not really be who she says she is. The continued increase in fraud – the Aite Group reports new account fraud was up 200 percent in 2018 – requires the online application process to be reviewed by multiple business units within your organization. Each one with different questions. Each one trying to get to know the real Angela Jones. Is she a potential top-tier, long-term customer? Or a clever fraudster?

The line-of-business manager wants to know: Is Angela Jones an actual person and not a bot? Does she have a credit history?

The Chief Risk Officer asks: Why is she an authorized user on three different credit cards, none of which are owned by family members?

Security experts in your IT department are equally inquisitive: Why is that IP address in Romania? Is her identity verifiable? Is that iPhone 8 the device she'll be using to interact with us?

Marketing has a different point of view. They are eager to know: is our website easy to navigate? What can we do to keep her coming back? She owns an expensive home – can we interest her in our platinum account?

These questions are being asked about consumers every day – and the same questions are keeping you and your business associates up at night. Is this person real or phony? Low-risk or high-risk? The right mix of data, analytics and technologies, applied in ways that don't disrupt the consumer experience, can give you an answer.

EQUIFAX®

Fraud Continues to Rise

The cost of account takeover fraud tripled last year, reaching an estimated **$5.1 billion in the United States.**

Source: PracticalEcommerce, August 17, 2018

The rate of **contact center fraud has skyrocketed by 350 percent over the past four years.** In response, call centers increasingly rely on phone ownership factors and voice recognition for multi-factor authentication.

Source: PYMTS.com, November 21, 2018

Cell-phone account fraud is growing rapidly. **In 2018 the number of victims of fraudulent mobile-phone accounts surged 78 percent** from a year earlier.

Source: Consumer Reports, June 12, 2019

For better progress and protection, you need to know more.

As consumers gravitate to online and mobile channels for purchases and financial needs, companies seek to give them a smooth, convenient digital experience. But fraudsters, including global crime rings, are also using technology to find new ways to bilk billions of dollars from businesses, governments, and consumers.

Currently, incidents of new account, account takeover and synthetic ID fraud are expanding at an annual rate of 100% or more. Organizations face a dilemma: Improved fraud defenses can make it more difficult for valued customers to enjoy fast, convenient interactions with their lenders, retailers and service providers.

Clearly, to fight fraud effectively without disrupting the consumer's experience, organizations must change how they approach identity authentication and fraud prevention. Yet there is no silver bullet or magic solution. The key is gaining better knowledge of who you're doing business with. Advanced authentication strategies are essential for mitigating risks, especially when the risks are greater and growing due to the increasing number of transaction touchpoints, in-person and digital.

Moreover, advanced decision science and analytics will enhance your ability to have friction-free interactions with valued customers — even when the interactions occur across channels.

Source: Aite 2018 Analyst Report

Companies need to manage identity and fraud in a far more complex and dynamic manner than five years ago.

Compliance
Can I do business?

Identity Verification
Is this a real identity?

Authentication
Is this who they claim to be?

Fraud
Is this suspicious?

Throughout a consumer's interaction, companies seek to resolve multiple questions by leveraging vendors and their own capabilities.

Customer Lifecycle of Activity

- **Account Opening**
- **Account Access and Management**
- **Transaction and Payment**

1. How to manage given dynamic nature of fraud?
2. How to integrate and make decisions?
3. What data and scores to use?

Choosing the right identity authentication solution depends on where authentication is needed in the customer lifecycle. Multi-factor identification is a recognized best practice that uses at least two of these three methods of identity verification:

1. **What they know**
such as a password or the answer to a knowledge-based authentication question
2. **What they have**
such as mobile phone ownership or identity documents
3. **Who they are**
using biometric identifiers

Know your customers better. Find the Maximum Viable Person.

How can you raise the bar in your risk management and account decisioning operations? Seek out the Maximum Viable Person℠. When you know applicants and existing customers better, you can mitigate risks and focus on those who will help your business grow.

Equifax uses a rich set of data assets, technologies and expertise to help you identify each Maximum Viable Person. This full arsenal of capabilities drives our mission: to provide maximum knowledge that you can parlay into maximum growth for your business.

Equifax helps you evaluate every online applicants, going far beyond conventional credit reports and scorecards. Likewise, Equifax assets will be invaluable in authenticating those who are logging into existing accounts.

What are the benefits of always having A-plus knowledge and insights? Your organization will be poised for maximum growth, because you'll have less risk and more protection. You're more efficient, because you've minimized manual reviews. Your customers have better experiences, and that pays off with more loyalty, higher retention rates, and greater lifetime value.

Why you need the Maximum Viable Person.

You're searching for better ways to achieve growth by protecting your institution, delivering positive customer experiences, and continually innovating.

Meanwhile, you're facing major headwinds in fighting account takeover, new account fraud (including synthetic identity fraud), and card-not-present fraud. Attacks are rampant in every industry — and the fraudsters seem to be gaining ground. IT resources are scarce. And of course, you have budget constraints. Plus, you want to provide friction-free experiences for customers.

Failure to keep up with anti-fraud technology is not an option. After all, credit decisions are the heart-and-soul of your business. Bare-bones, fragmented, minimalist approaches to decisioning cannot deliver the growth and protection top management expects. Ditto for services that lure you with glittery new features, but address only a fraction of the comprehensive capabilities needed to know your customers better.

With the right technologies applied to the right sets of data, you'll have the means to spot a Maximum Viable Person in online and face-to-face interactions. You'll be able to harness relevant data and turn it into intelligence that evaluates each individual, revealing their potential — or their hidden risks. You'll be able to make critical decisions in real-time — without increasing the level of manual reviews or sacrificing customer satisfaction.

Cultivate the Maximum Viable Person in multiple channels.

Insights from digital interactions in online channels can be linked to face-to-face retail channels. A case in point is 700Credit LLC, a Michigan-based provider of screening and pre-qualification solutions for automobile dealers.

700Credit uses Equifax identity data and uniquely differentiated data sources to automatically prefill consumer applications for auto loans. The streamlined process, called QuickQualify Xpress, enables dealerships to improve closing ratios by dramatically reducing the data entry required. The short and simple pre-qualification step at a dealer's website has no impact on consumers' credit scores, so they are much more likely to complete the form and go to the dealership.

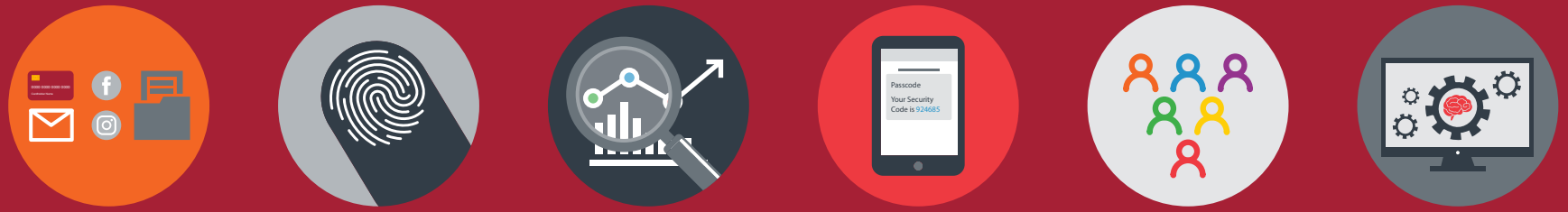
"QuickQualify Xpress is a natural evolution of our soft-pull technology," said Ken Hill, managing director of 700Credit. "Our QuickQualify platform was the first step in reducing the amount of data consumers need to provide before a soft-pull could be executed. QuickQualify Xpress further minimizes the data required for pre-qualification, enhancing their experience with the platform. 80% of consumers are shopping from a mobile device before they enter the dealership. This tool makes it even simpler for a consumer to start the pre-qualification process."

QuickQualify Xpress asks only for a ZIP code and last four digits of the consumer's SSN, before automatically populating the consumer's demographic information. In the mobile environment, QuickQualify Xpress helps mitigate risk by authenticating the user's identity before requesting further information.

"Generation Z has only known a digital world, and they are predicted to outnumber Millennials this year. This collaboration with 700Credit will help dealers stay current with today's buyers by simplifying digital interactions, providing instant identity results and minimizing the frustrations often associated with digital abandonment. Collectively, the convergence of data, analytics and technology can improve dealer outcomes across the digital interaction ecosystem."

Lena Bourgeois
Vice President, Enterprise Alliances
Equifax

Six best practices will lead you to the Maximum Viable Person.



1. Diversify data

Complement internal data with external data and analytics. The key is to know the person, not just their credit scores. The goal is to illuminate identities by getting 360-degree, multi-dimensional knowledge of applicants and customers.

Equifax does this through the diversity and depth of different types of data we own or manage. Unique data assets build holistic identity profiles that can signal anomalies in personal identifying information (PII) and behavioral characteristics.

Many businesses use identity verification just for their credit decisioning processes, possibly missing opportunities to go deeper into verification, authentication and fraud prevention signals. Equifax help can sharpen the picture by bringing in “signs of life” indicators, such as utility accounts, car registrations and court records. These will complement your internal data and enhance the basic information available externally from credit reports.

We go beyond basic identity verification techniques by associating PII with facts about email account history, social media accounts, or attributes of the device being used for online interactions, for example.

Data points generated by the consumer’s device during interactions are especially enlightening. We may detect a pattern typical of robots that visit websites, populating them with good PII and applying for credit. Or we may see that potential fraudsters are going directly to the application data page instead of following a consumer’s normal path while visiting a website.

2. Improve authentication processes

To spot a Maximum Viable Person, you'll need a robust combination of authentication techniques. Single-factor authentication is simply signing into a password-protected account. Multi-factor authentication processes apply second and even third checkpoints to authenticate a person more effectively.

Multi-factor authentication strategies are appropriate for all channels — and are vital for channels where consumers are interacting remotely.

Passive, unobtrusive measures include:

What device is being using? What phone attributes are detected?

Do the phone attributes and identity profile align with phone company records?

Is the IP address valid?

Active measures include:

Ask for two pieces of information on the phone number account.

Send out-of-band/two-factor messages through other channels (text or email) to confirm what you know about applicants.

Send push notifications from your mobile app. These are much more secure than one-time passcodes sent via SMS.

Employ biometric checks, such as voice recognition, facial recognition, or fingerprints.

You can use multi-factor authentication situationally (called context-based authentication). For example, in higher-risk scenarios, you might want to use stepped-up measures, such as verifying phone ownership or push notifications through a separate device, an email account, or your organization's mobile app.

Many experts have urged businesses to beef up their multi-factor authentication solutions. Weaknesses of legacy approaches transcend industries and all phases of a customer life cycle.

According to Javelin's 2019 Identity Fraud Study, it's not just financial institutions that need to improve their authentication processes. The report states:

"Fraudsters are finding easy targets outside financial services. Rewards programs, merchants, mobile network operators, and other online accounts all have value for fraudsters but frequently lack any authentication method more robust than passwords, security questions, or SMS one-time passwords."

Beyond Analytics: Machine Learning has Arrived

According to Aite Group, machine learning platforms are gaining traction in the fight against financial crime. Stanford defines machine learning as "the science of getting computers to act without being explicitly programmed."

In legacy authentication processes, static business rules are used to map the characteristics of an interaction to the appropriate decision. A rule that indicates fraudulent behavior will continue to do so until someone changes the rule.

Analytical tools focus on parsing data to detect suspicious patterns, and then applying established rules to determine actions and workflows. Machine learning embraces these concepts and takes them to a higher level. Machine learning is the power that enabled Equifax to make the Maximum Viable Person concept a working reality. With machine learning, you truly know your customers better.

3. Embrace analytics

Analytic tools can analyze behaviors and confirm identities using a variety of data sources and industry-specific inquiry patterns. By flagging suspect transactions earlier in the process, you can identify risks and avoid potential problems before they occur.

Advanced analytics will empower your organization to detect linkages and suspicious patterns. This not only reduces the time and money expended on manual reviews, but also will help protect your organization's reputation.

In new account situations, patterns such as shared Social Security Number and homeowner mismatches are some of the red flags that can indicate synthetic identities. Fraudsters often use the same address for many synthetic identities, and then change the address when they "bust out" with maximum charges up to account limits.

The credit card industry is the favorite target for synthetic fraud. Equifax data shows that other product types are also vulnerable to synthetic identity fraud. Here's a snapshot of what we're seeing for different product types:

PRODUCT TYPE	ACCOUNTS FLAGGED OVER 12 MONTHS AS POTENTIALLY SYNTHETIC	BAD BALANCE PER ACCOUNT
Automobile loans	210,000	$15,000
Credit Card Accounts	1,000,000	$1,830
Telecommunications and utility accounts	356,000	**Utilities:** $630 **Wireless:** $1,500
Unsecured personal loans	136,000	$2,000

Equifax collects data and uses a machine-learning platform to "connect the dots" from millions of interactions and dynamically adjust the business rules you use for decisioning. With the resulting intelligence, you can continually and seamlessly update the rules and policies your organization uses to detect anomalies and authenticate identities.

4. Orchestrate and optimize

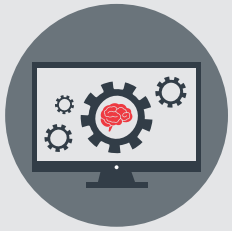
Many organizations experience high false-positive rates in their internal fraud prevention measures. The usual countermeasure — reaching out manually to question applicants— is an inefficient use of staff resources. In addition, it's prone to delays that can prompt consumers to move on to competitors.

Equifax can help you tailor your interactions — say, for a consumer opening a high-value account — by treating this applicant differently than those who are opening small accounts.

Orchestration is the mechanism for determining the types of experience you want the customer to perceive, balanced with the level of risk associated with that customer in a particular scenario.

A key tenet of orchestration is to authenticate a person's identity as passively as possible. Digital attributes and behavior pattern logic can run in the background to identify risks, and when triggered, these can orchestrate an appropriate, automated interaction with the consumer. For example, at most risk levels, the business might send a one-time passcode for the consumer to access his or her account, or use tools that verify the phone number isn't spoofed.

More obtrusive identity factors, such as knowledge-based authentication (KBA) questions, can be used as a last resort before triggering manual reviews. A note of caution on KBAs: Fraudsters are adept at finding answers to static KBA questions in social media, public records, or even on a driver's license. Then, if they can convince a contact center representative to change passwords, they can hijack the account.



What does machine learning bring to a risk management environment?

The key capabilities include:

Harnessing internal and external data

Using iterative analytics to detect fraud and optimize wallet share

Self-learning from data

Self-adapting to shifting patterns without relying on people to change the rules

In today's always-on, digitally connected world, these are precisely the capabilities needed to verify a person's true identity, crosschecked with a variety of outside data sources.

More obtrusive identity factors, such as knowledge-based authentication (KBA) questions, can be used as a last resort before triggering manual reviews. A note of caution on KBAs: Fraudsters are adept at finding answers to static KBA questions in social media, public records, or even on a driver's license. Then, if they can convince a contact center representative to change passwords, they can hijack the account.

Likewise, cybercrooks have a variety of ways to compromise traditional one-time passcodes sent via SMS to a customer's mobile phone. Consequently, in situations deemed to have a high level of risk, you'll want to go beyond conventional verification techniques. Analytic tools can apply rules dynamically to initiate more robust options, such as biometric techniques (voice recognition, facial recognition, or fingerprints), document verification, secure one-time codes and phone ownership and attributes.

You can also consider using dynamic, rather than static, KBAs. In a static scheme, customers pre-select the questions they will be asked and provide the answers. Perhaps the most over-worked KBA is, "What is your mother's maiden name?"

Dynamic KBAs, on the other hand, are not pre-selected by the user. Based on either memorable details from long ago or very recent events, dynamic KBAs are generated by data assets, such as car registration records or recent account charges. Two examples of dynamic KBAs: "What color was the Honda Accord you owned in Texas in 2005?" and "What is a clothing store you shopped at recently?"

Optimization analyzes how decisioning processes are working in relation to the risks involved. Of the various data sources available, you want to determine which ones give you the most value in particular scenarios.

Equifax uses a state-of-the-art machine-learning platform to enable quick reactions to data coming in and faster recognition of different types of attack. This means you can implement new checks and safeguards and put them into production the same day.

5. Monitor your customers

This best practice assesses whether the actions taken after a new account is opened– or an existing account is accessed – are legitimate and consistent with norms you expect in these situations.

Authentication focuses on “Who are you?” Post-authentication monitoring examines “Are you doing anything out of the ordinary?” and “Are you the same person we validated at account opening?”

Dynamic economic conditions, shifting trends and evolving regulations continually impact businesses — both positively and negatively — making it imperative to stay updated on the account activity of your userbase. One way to do this is to continually check your user base with passive multi-factor authentication strategies.

Monitoring is routinely done for credit card accounts — and can also extend to other account types as well as money transfers and bill payment. Post-authentication monitoring looks for anomalies in various metrics, such as dollar amount, location and frequency, and proactively issues early warnings of changes in risk level or signs of potential fraud so you can prevent losses. In addition, you’ll get early alerts of improving financial status, enabling you to quickly initiate actions that could drive more revenue.

A tremendous by-product of monitoring customers is improving the digital experience by learning from their choices and behaviors.

For example, if you offer choices on how users would like to authenticate themselves, you may uncover demographic differences in their authentication preferences. Are there age, income or geographic differences in customer preferences for email or text PINs? Do Millennials prefer facial recognition or fingerprint verification on their mobile device oppose rather than answering a KBA question?

How do customers react to alerts?

To avoid write-offs, it’s crucial to detect anomalies and take appropriate actions as early as possible and at the right points. Often this means contacting the consumer directly. Legitimate customers usually appreciate being asked if something is amiss. The inquiry gives the consumer confidence that the business is in control, has strong security measures in place, and is acting in the customer’s best interests.

IBM’s “Future of Identity” survey found that customers are increasingly willing to use technologies that enhance security. Eighty-seven percent of respondents would consider using different types of biometric authentication. The majority are unwilling to sacrifice security for convenience, especially in financial interactions.

What you learn can generate immediate benefits. You'll see ways to better balance your needs for fraud prevention with customer desires for safe and convenient online experiences. The goal is to guard against fraud effectively and unobtrusively, while bringing in stepped-up authentication measures only where there is a high potential for fraud.

You may find significant channel differences in the types of authentication that work best for your customer base. Mobile devices are becoming ubiquitous for making purchases, checking account balances, and applying for loans, but many businesses struggle with high abandonment rates in mobile transactions. Monitoring – and learning from – your mobile customers can deliver the seamless, secure experiences they expect.

6. Keep improving

When consumers interact with your business in any channel, they weigh their experiences with their pre-engagement expectations. If all goes smoothly, they reward you with their loyalty, which often translates into more transactions, more revenue, lower costs, and high long-term value to your business.

Rely on Equifax to help you continually improve the customer journey, reduce risk and drive business growth. Customers appreciate something as simple as automatically populating forms with known information about them. By minimizing data entry, you improve the customer experience for current clients — and cut abandonment rates for prospective ones.

You can turn newfound intelligence about a Maximum Viable Person into context-based offers of credit or services at the point of digital interaction.

Equifax customers can also use historical data on rules and optimization processes to do what-if analyses of changes. Analyses of previous performance will show how a set of changes would affect the outcomes going forward.

Apply the Maximum Viable Person concept to all customer-facing applications. By integrating various authentication processes that are currently fragmented, you're enhancing your organization's ability to offer a true omni-channel experience. In addition, applying stronger authentication methods across channels will help reduce the risk of fraudsters using the weakest channel as a "beachhead" for attacking other channels.

Keep looking for ways to elevate the customer experience. Intelligence gained from knowing your customers will streamline initiatives to create and sustain customer loyalty. The insights help you enhance how your business interacts with customers and delivers what they want.

Keep looking for ways to elevate the customer experience. Intelligence gained from knowing your customers will streamline initiatives to create and sustain customer loyalty. The insights help you enhance how your business interacts with customers and delivers what they want.

Summary

With this foundation of best practices, you'll routinely identify the Maximum Viable Person in all channels. Extensive data assets, advanced analytics, and a proven machine-learning platform positions Equifax to be your top resource for collecting, analyzing and enriching multi-source data.

You know your customers, and that puts you in full control. You're alerted to situations where we see identities being compromised. You can dynamically adjust your strategies to cultivate more business with a Maximum Viable Person, or open manual reviews of users suspected of fraudulent activity. You can accomplish more, cut losses, and perform more efficiently. That means you can focus more attention on cultivating the loyalty of every Maximum Viable Person you have identified in your user base.

EFX®

19-103234