Behavioral Biometrics

Improve Security and the Customer Experience
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader ROI &amp; Introduction</td>
<td>1</td>
</tr>
<tr>
<td>The challenges of authenticating mobile customers</td>
<td>2</td>
</tr>
<tr>
<td>The need for transparent customer authentication</td>
<td>3</td>
</tr>
<tr>
<td>The role of behavioral biometrics in authenticating online customers</td>
<td>5</td>
</tr>
<tr>
<td>The benefits of continuous authentication</td>
<td>6</td>
</tr>
<tr>
<td>The business benefits of behavioral biometrics</td>
<td>7</td>
</tr>
<tr>
<td>Less friction improves the user experience</td>
<td>8</td>
</tr>
<tr>
<td>Conclusion</td>
<td>9</td>
</tr>
</tbody>
</table>
Reader ROI

Before the Internet, customers who wanted to perform a bank transaction had only one option – a visit to their local branch for a face-to-face transaction. Now, in the “mobile age,” customers expect that their bank provide secure and easy access to the full suite of banking services via their mobile device. The availability of transparent, risk-based online authentication tools, such as behavioral biometrics, then, comes at a critical time.

Read this paper to learn:
- The critical challenges financial institutions face when authenticating an increasingly mobile customer base;
- How to establish a risk-based approach to online security;
- How behavioral biometrics helps financial institutions manage fraud risk, improve the user experience, increase customer loyalty, satisfy regulatory requirements, and deliver a frictionless, cross-channel user experience.

Introduction

To satisfy the demand for internet-enabled banking, financial institutions have evolved their online presence from merely providing access to account balances, to full-service banking. Unfortunately, as financial institutions increased the breadth of online services, they attracted even greater attention from cybercriminals. When banks and credit unions fail to deploy a robust online authentication process, fraud follows, and often on an organized scale.
To improve the online user’s experience, financial institutions have evolved their approach to customer authentication. Yet with each new layer of authentication, cyber criminals continue to uncover weak spots to exploit.

At the same time, institutions face ever-increasing customer expectations with respect to the convenience and security of online banking. One of the major factors driving the demand for online banking stems from the proliferation of devices equipped to access the Internet. Since many companies make their sites available to consumers via mobile devices, in turn, they expect their bank to do the same. However, despite their ubiquity, there are inherent challenges to securing mobile devices. A legitimate user can initiate access from anywhere, at any time, and expect instantaneous, unfettered access to conduct full-service banking. How can a bank determine if a login attempt from a foreign country, in the middle of the night, is in fact the actual account owner?

In addition to the challenges that result from portability, mobile devices require frequent patching to remove security weaknesses. Some devices are prone to the installation of malicious apps. To complicate matters further, consumers do not treat mobile devices in the same way that they do computers and install virus detection software. Such bad device hygiene increases the chances that a mobile phone or tablet becomes infected.
The need for transparent customer authentication

Regardless of the authentication method that a bank employs to vet mobile or desktop users, it cannot shift too much of the authentication burden to the customer. While the use of one-time passwords and multi-factor authentication can help secure the online channel, these approaches are labor-intensive and have the potential to alienate customers.

To meet their customers’ expectations, banks and credit unions need a transparent, yet highly effective approach to authentication that is risk-based, and able to supplement an existing suite of security protocols.

Behavioral biometrics, which gathers and analyzes numerous elements of a user’s behavior including their device finger pressure, and typing speed, among other factors and compares it to data in the user’s profile, meets the need for a higher degree of authentication without compromising the user experience. Financial institutions can use behavioral biometrics in combination with other means of authentication and as part of a layered approach to screening online users.

Matthias Valcke, Business Solutions Manager with VASCO Data Security stresses that while highly effective, behavioral biometrics is just one option to authenticate users. “We don’t necessarily believe in a single, all solving authentication solution, but more of a risk-based approach that’s dependent on the context that a user is accessing an application or performing a transaction,” Valcke says. “Behavioral is one component, but a bank...”
could also include push messages, biometric parameters, malware detection, geolocation, stuff like that as part of their authentication process."

When it comes to risk-based authentication, Shirley Inscoe with the Aite Group supports the use of behavioral biometrics. "Behavioral biometrics scores activity and enables financial institutions to take action when scores indicate suspicious activity. Institutions can define various low and high-risk use cases, adjusting required scores for the level of risk involved. For example, if a customer is moving funds out of the institution, a higher score can be required than if an account balance is being checked."
The role of behavioral biometrics in authenticating online customers

Traditional authentication methods offer varying degrees of effectiveness. Yet they often shift a great deal of the security burden to the customer. While customers should play a role in securing their accounts, asking them to recall convoluted passwords, or the answers to personal questions they have long forgotten, is a quick way to alienate them.

Behavioral biometrics rely upon the user’s data input, movement within a site or app, and the user’s interaction with a device, including finger pressure, and swipe patterns, etc. as a means of authentication. Behind the scenes, behavioral biometrics analyzes the user’s interactions with the device in comparison to a previously developed user profile. Call this the “similarity score.” The greater the similarity score, the less the bank has to worry about the user’s identity and intent. Conversely, a lack of similarity between a user’s behaviors in comparison to their profile justifies the application of additional layers of authentication. In essence, the user’s actions or behavior facilitates a risk-based approach as it proscribes authentication commensurate with risk.

Incoe sees behavioral biometrics providing financial institutions with an effective new tool to improve their approach to customer authentication and combat the constant stream of account takeover attempts. She also sees the convenience of behavioral biometrics as a major selling point. “Customers expect their accounts to be protected, but are not willing to be inconvenienced to enhance security. Methods such as behavioral biometrics enable FIs to authenticate their customers in a transparent manner with no negative impact to the consumer. This also improves the customer experience, which is a goal of many financial institutions in addition to preventing fraud.”
The benefits of continuous authentication

Increasingly, financial institutions recognize that effective authentication is more than just a one-time event. Behavioral biometrics support contextual authentication by monitoring a user’s activity during a session. Monitoring, and where appropriate authenticating the user during a session can help weed out sophisticated cybercriminals with the ability to overcome a bank’s initial login security measures, or insert themselves during a session. “One of the strengths of behavioral biometrics is that it runs continuously; if a session is taken over by a fraudster, it will be detected,” explains Inscoe. “This is superior to a solution that only authenticates a consumer one time at the beginning of a session.”

“Behavioral biometrics scores activity and enables financial institutions to take action when scores indicate suspicious activity.”

Shirley Inscoe, Senior Analyst with Aite Group

Figure 1: Usage of Mobile Banking and Mobile Payments by Mobile Phone type

The business benefits of behavioral biometrics

Given that behavioral biometrics relies on a user’s natural actions, it minimizes the time it takes to authenticate a user, and therefore increases the time the user can spend accessing the bank’s online services. Less friction within the online channel increases the likelihood that customers will use additional services as they become available. In addition to encouraging the use of the online platform, behavioral biometrics also provides a secure platform to release new services that require robust authentication such as those involving the transfer of funds.

Valcke believes that behavioral biometrics has sufficient flexibility to make the authentication process efficient and almost entirely transparent. “Let’s say the user is traveling and he’s logging in from a suspicious location. If you can analyze how is he typing, how is he entering data on the phone, you can determine it’s the real user, just in another location. In that case, we will not ask that user for additional authentication,” Valcke says. To illustrate the point further, Valcke notes that if a user is in their normal location, using their regular phone, yet typing differently as if he was driving for example, behavioral biometrics has sufficient context to allow the user to conduct normal banking activities.

Figure 2: Mobile banking usage by millennials

US Smartphone Market Share By Age and Operating System

<table>
<thead>
<tr>
<th>Age</th>
<th>Android OS</th>
<th>Apple iOS</th>
<th>Windows Phone</th>
<th>Blackberry</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-24</td>
<td>98%</td>
<td>97%</td>
<td>96%</td>
<td>1%</td>
</tr>
<tr>
<td>25-34</td>
<td>98%</td>
<td>97%</td>
<td>96%</td>
<td>1%</td>
</tr>
<tr>
<td>35-44</td>
<td>96%</td>
<td>97%</td>
<td>96%</td>
<td>1%</td>
</tr>
<tr>
<td>45-54</td>
<td>89%</td>
<td>97%</td>
<td>96%</td>
<td>1%</td>
</tr>
<tr>
<td>55-64</td>
<td>80%</td>
<td>97%</td>
<td>96%</td>
<td>1%</td>
</tr>
<tr>
<td>65+</td>
<td>68%</td>
<td>97%</td>
<td>96%</td>
<td>1%</td>
</tr>
</tbody>
</table>

Less friction improves the user experience

Shirley Inscoe sees the use of passive biometrics as particularly appealing given how little the customer sees of it in action and removes the need to ask them to enroll in additional authentication methods. “By using behavioral biometrics, financial institutions can avoid having to ask customers to enroll in a new authentication method; many security methods are effective, but have low acceptance/enrollment rates by consumers.” She believes that the lack of friction associated with behavioral biometrics is a major selling point. “Using a transparent authentication method allows the financial institution to protect the activity on accounts without negatively impacting the customers or inconveniencing them.”

Yet, for all its benefits, behavioral biometrics is just one layer of an effective fraud program. “FIs that have a good understanding of fraud mitigation realize there are no silver bullets; no one solution will provide adequate protection against all fraud threats,” says Inscoe. “Biometrics and all other forms of authentication are fallible, and have some level of false positives and false negatives. Layering various types of solutions will enable financial institutions to authenticate customers successfully,” Inscoe adds.

Layering various types of solutions will enable financial institutions to authenticate customers successfully.

Shirley Inscoe, Senior Analyst with Aite Group
Behavioral biometrics delivers a multi-channel solution, with particular benefits for smartphone and tablet users. Up until now, banking institutions normally submitted mobile users to traditional authentication methods, which often proved ineffective. Since behavioral biometrics takes place without a users’ knowledge, the user experience improves. In fact, there are numerous benefits for the customer when financial institutions employ a transparent contextual authentication process. Since the user’s activity is the means to authenticate, the security burden associated with authentication disappears. In addition to authenticating users transparently, the potential for fraud drops significantly. Banking institutions also ensure regulatory compliance having vetted the user.

Aite’s Inscoe believes that behavioral biometrics has staying power. “Cybercriminals have been able to defeat every safeguard that financial institutions have implemented over the years, so anything is possible. However, behavioral biometrics will be more difficult to overcome because each individual has a behavioral profile, which is constantly compared to activity being performed during a session. As long as the analysis is taking place, and the financial institution is acting upon the results promptly, the fraudsters should be thwarted.”

Conclusion

Also download the ‘Increasing Business with Mobile Banking’ security ebook: www.vasco.com/MobileBanking
About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets.

Learn more about VASCO at www.vasco.com or visit blog.vasco.com

About iSMG

iSMG is the largest media company solely focused on Information Security, Risk Management, Fraud, Compliance and other related topics. The firm’s footprint and the subscriber-base extends from the North American markets to Europe, Asia and Australia.

Learn more about iSMG at www.ismg.io