CONTENTS

Consumer Choice and Convenience................................................................. 3
  Consumers demand choice – let’s give it to them........................................ 3
  Convenience does not have to equal poor security ..................................... 4
Reducing Fraud ................................................................................................. 5
Mobile First ........................................................................................................ 6
Meeting Latest Regulation ............................................................................... 7
Summary ........................................................................................................... 8
RSA Adaptive Authentication and Biometrics ................................................. 9
Eyeprint ID ......................................................................................................... 9
About Goode Intelligence.................................................................................. 10
A drive for seamless user experience and rising levels of fraud are changing how organizations design and deploy today’s authentication solutions.

This white paper from cyber security research and consulting company Goode Intelligence (GI) has identified consumer choice and convenience, demonstrable fraud reduction, meeting a ‘mobile-first’ strategy and regulation compliance as being key considerations that organizations should use when selecting an authentication partner.
CONSUMER CHOICE AND CONVENIENCE

Consumers demand choice – let’s give it to them

We are living in a world where consumer choice in technology has never been so powerful. The ‘bring your own’ movement where employees are able to use their own smart mobile devices for enterprise applications has liberated many people from the restrictions of using a device purely for corporate use. This bottom-up approach for technology adoption that is easy-to-use is having a profound effect on how consumers view the authentication experience.

Ease-of-use has been a prime reason for the success of mobile-based biometric authentication systems. The arrival of mobile biometrics with Apple’s Touch ID fingerprint authentication, first introduced on the iPhone 5s during 2013, has allowed consumers to benefit from convenient one-touch authentication. Consumers have turned to Touch ID in increasing numbers leading to 89 percent of iPhone users that have Touch ID capability using the fingerprint biometric authentication service.

68 percent of consumers want to use biometrics as a method of payment authentication

The ability to quickly and seamlessly unlock a valuable device or approve a financial payment with a glance of an eye has introduced consumers to a new method of consumer authentication.

Equipped with the latest mobile technology consumers are also demanding choice in the biometric tools that they use. Integrated fingerprint may not always be appropriate for certain use cases and applications so the availability of additional biometric technologies provides consumers with alternatives. Almost 80 percent of US consumers want the opportunity to use more biometric choices for mobile banking and payments.

1 https://techpinions.com/apples-penchant-for-consumer-security/45122
3 The Retail Banking Biometrics Confidence Report, May 2017 by EyeVerify
Key Considerations for Selecting a Consumer Authentication Vendor

Convenience does not have to equal poor security

There is a school of thought in security that says the more difficult the task to perform a security function the better the security. For authentication, by getting people to perform complex tasks, such as remembering your favourite brand of ice cream when you were seven or entering in a minimum 20-character password that MUST have at least one special character, a capital letter, a number and the combination of the CTRL-ALT-PrtScn buttons held down for exactly 3.5 seconds, equals stronger security.

Thankfully with the arrival of smarter authentication technologies including adaptive authentication and biometrics, security can lose its reputation as being the ‘as many hoops as you must jump through’ system.

The combination of something you have (a mobile device), something you are (your biometric identifier) and something you do (data analytics/risk-based authentication) allows consumers to identify themselves online and to approve transactions with as little inconvenience as is possible.

Convenience is also being able to use an authentication mechanism across a range of business channels. In this mobile-first age we can forget that many consumers use a variety of channels to manage their bank accounts or to access healthcare services. Identity has to be verified across physical, telephony and web channels in addition to the ever-dominant mobile. By offering consolidated and integrated authentication solutions across multiple channels consumers benefit from similar user experiences. Service providers also benefit by avoiding authentication and identity silos where a single authentication technology is chosen for a single product or application.

The need to harmonize user authentication methods across a range of delivery channels benefits consumers and service providers
REDUCING FRAUD

A modern consumer authentication solution must be able to demonstrate that it can help in the fight against fraud. This is not only confined to the authentication process itself, you must have the threat and intelligence capability to identify the latest threats that result in fraud. This capability can come from either a full service authentication and fraud vendor, such as RSA, or from an ecosystem of solutions.

Identity theft is a major cause of financial, business and healthcare fraud. It can be caused by a number of security incidents that are often combined. Common security incidents include data breach of a central identity database, identity stealing malware, phishing and man-in-the-middle (MiTM) attacks. The number of account credentials that have been compromised is huge; according to the ‘have I been pwned’ website\(^4\) a total of 3.75 billion account credentials have been breached.

- **Data breach of identity database**
- **Malware including key-loggers**
- **Phishing attacks**  
  (costing $10.8bn in 2016)\(^5\)
- **Man in The Middle (MiTM) attacks**

Once a person’s identity has been ‘stolen’ or duplicated by fraudsters then a number of fraud events often occur. These include the theft of money from a bank account, impersonating a valid account holder to purchase products and services, and even using stolen healthcare information to seek medical services.

Fraud levels are on the rise around the world with mobile becoming the number one cybercrime target; both as an originator, with 60 percent of overall fraud now originating from a mobile device\(^6\), and a target. An organization may choose a convenient authentication solution but if it can be bypassed or spoofed then it fails to meet a critical requirement of being secure and being able to demonstrate fraud reduction. The ability for an authentication solution to demonstrate that it reduces fraud levels is a must have consideration for organizations when choosing a suitable vendor.

---

\(^4\) [https://haveibeenpwned.com/](https://haveibeenpwned.com/)
MOBILE FIRST

A consumer authentication solution must be able to meet a ‘mobile first’ strategy to ensure that the most popular technology end-point is supported and to ensure that there is a common user experience whatever the device a consumer is accessing a digital service from.

What is a Mobile First Strategy?

Mobile first is an approach to responsive design: design for smaller screens first, then add more features and content for bigger and bigger screens – Mobile / tablet / desktop

Consumer authentication must also have a ‘mobile first’ strategy. This means an authentication vendor must meet the demands of millions of global consumers using their smart mobile devices as the primary computer by designing authentication solutions that puts mobile first.

There are two main scenarios for authentication on mobile:

1. **Using the mobile as the prime authenticator** for non-mobile digital services and authorizing digital transactions; accessing web services and supporting omnichannel service delivery. For instance; a bank customer is attempting to make a payment to a new beneficiary using a web-based banking service. The bank’s risk-based authentication service flags this transaction as being above a pre-defined risk rating and sends a message to the customer’s mobile banking app that requests them to provide ‘step-up’ authorization using mobile biometric technology – EyeVerify’s Eyeprint ID for example. The customer authorizes the payment by verifying their Eyeprint and the payment is made.

2. **Using mobile-based authentication services** to secure mobile applications and services. This is usually provided by the vendor in an authentication SDK that can be integrated into a service provider’s mobile app. The SDK should support a number of authentication technologies to allow consumer choice and to also match the right authenticator to the risk rating of the particular authentication scenario or transaction request. This can include combining more than one mobile biometric technology to offer ‘multi-modal’ biometric authentication. For instance, a healthcare customer can access (open) the mobile healthcare app using built-in biometric technology, usually a fingerprint. To access sensitive medical records the healthcare provider may request a biometric technology that can provide greater assurance of identity, an Eyeprint as example.
MEETING LATEST REGULATION

Industry and federal regulation is changing at a rapid pace to support new methods of business and service delivery. The rise of mobile commerce is a key driver for this regulatory change that also aims to protect consumers against changing threat scenarios.

A key consideration for selecting a consumer authentication vendor is its ability to address the requirements of current regulations and also to provide advice on the impact of forthcoming regulation. A key question to ask your technology partner is “Does your current authentication partner have the ability to provide you with insight into the impact on your authentication services from regulation that is coming and also to influence regulators in creating regulation that meets your business strategy?”

Table 1 provides a summary of important regulation and industry guidelines that have a significant impact on authentication.

Table 1: Regulation and Industry Guidelines - A Major Impact on Authentication

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Region</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU Payment Services 2 (PSD2)</td>
<td>European Union</td>
<td>Strong Customer Authentication (SCA) guidelines that include multi-factor authentication technologies including biometrics linked to risk-based authentication</td>
</tr>
<tr>
<td>EU General Data Protection Regulation</td>
<td>European Union</td>
<td>Methods to verify consumer identity linked to demonstrable security controls</td>
</tr>
<tr>
<td>New York State Department of Financial Services (DFS)</td>
<td>New York State, USA.</td>
<td>The DFS requires organizations to use multi-factor authentication (MFA) or risk-based authentication (RBA) to protect against unauthorized access to non-public information systems</td>
</tr>
<tr>
<td>“Cybersecurity Requirements for Financial Services Companies”⁷</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FFIEC “Authentication in an Internet Banking Environment”⁸</td>
<td>USA</td>
<td>Strong consumer multi-factor authentication &amp; fraud detection techniques</td>
</tr>
</tbody>
</table>

Organizations must comply with regulations that mandate security controls and authentication mechanisms. Failure to do so will result in heavy financial penalties; for instance failure to comply with EU GDPR regulation could lead to financial penalties that are 4% of global turnover or €20 million (US$22 million).

SUMMARY

This white paper from Goode Intelligence identifies five key considerations that must be met when organizations are selecting a consumer authentication vendor:

1. Consumer choice
2. Convenience
3. Fraud reduction
4. Mobile first
5. Meeting latest regulations

These five considerations are powerful criteria for organizations when assessing authentication solutions and vendors.

Consumers must be given a choice of convenient, easy to use authentication services. The availability of a wide range of device-based authentication technologies including multiple biometric solutions supports this requirement. Convenience and consumer choice can also be combined in a well-designed consumer authentication solution. The combination of risk based authentication (RBA) and mobile biometric authentication services (MBAS) can meet this criteria. Risk based authentication can meet a good percentage of normal authentication scenarios and mobile biometrics can be applied to authentication scenarios that require further ‘proof’ of true identity; a combination of frictionless and friction-light authentication.

Service providers are increasingly pressured to support legacy service channels including physical (bank branch and retail store) and telephony at the same time as evolving their offering to work across a wide range of new technology, first web, now mobile and moving swiftly into the Internet of Things (IoT). When choosing an agile technology partner that can support multiple delivery channels, omnichannel support, an organization must ensure that they choose an authentication solution that can operate across a wide range of these channels. The mobile first strategy can allow organizations to design and deploy effective authentication services that meet this consideration.

Fraud is rising in all sectors. A consumer authentication vendor must be able to demonstrate fraud reduction as a result of deploying the chosen authentication solution – measurable and tangible fraud reduction benefits.

Around the world, regulatory powers are adapting existing regulation or introducing new ones to ensure that consumers are protected when using the latest digital services. A trusted technology partner must be able to demonstrate:

a. It can help organizations address the latest federal and industry regulations; and
b. It actively participates in influencing regulatory bodies to ensure that convenience and ease of use are not sacrificed at the expense of over rigid security requirements.

Getting the balance between security and convenience is an essential ingredient in supporting flexible digital service delivery.
RSA Adaptive Authentication is a risk-based authentication and fraud detection platform that provides advanced protection across both Web and mobile users. The Adaptive Authentication Mobile Module leverages RSA’s proven Risk Engine which includes a mobile-optimized risk model that analyzes a variety of risk indicators, including mobile device identifiers, location and behavioral profiles, to identify fraudulent or suspicious activity. Adaptive Authentication can be used to secure multiple types of mobile channels including mobile browsers, WAP browsers and mobile apps.

Adaptive Authentication offers integration through a web services call and a Software Development Kit (SDK) that allows developers to embed strong authentication directly into their mobile applications for banking, e-commerce, and enterprise access. The Adaptive Authentication Mobile SDK also supports biometrics for step-up authentication including fingerprint and EyeVerify’s Eyeprint ID. Supported platforms include Apple iOS, Android OS.

For more information, please visit www.rsa.com/fraudprevention.

EYEPRINT ID

Eyeprint ID from EyeVerify is one example of a biometric authentication solution that can support the changing requirements for consumer authentication. This mobile biometric, which uses the front-facing cameras on smartphones to authenticate the user via their visible veins and other eye-based micro features. Over 50 financial institutions are already using Eyeprint ID to authenticate their customers, and it is now built into the step-up authentication functionality within RSA’s Adaptive Authentication mobile SDK.

Visit eyeverify.com to learn more.
Key Considerations for Selecting a Consumer Authentication Vendor

ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consulting services for the cyber security industry.

For more information on this or any other research please visit www.goodeintelligence.com. This document is the copyright of Goode Intelligence and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Goode Intelligence.