Calculating the Real ROI of Implementing a Biometric Authentication Solution

With identity theft, data breaches, and financial fraud on the rise, the financial services industry needs a secure biometric solution that can't be easily compromised. Although biometric technology currently uses non-duplicative data to authenticate users, financial firms have been slow to adopt.

Security Risks

Traditional authentication methods rely on PINs and passwords, both of which are vulnerable to exploitation. In fact, **Verizon's 2016 Annual Data Breach Incident Report** found that 63% of confirmed data breaches involved the use of weak, default, or stolen passwords.

Unlike standard business and operating expenses, data breach costs are often unknown and overlooked by companies. Yet, every day firms face the risk of sizable financial losses due to theft, fraud, legal settlements, and regulatory fines. According to Juniper Research, data breach losses are expected to reach US $2.1 trillion globally by 2019, with **an average cost per incident to exceed US $150 million by 2020**.

Average cost per incident to exceed US $150 million by 2020

Operational Costs

Many industries have begun forcing their customers to create longer, more complex passwords, which are easily forgotten and inconvenient. Even with easy-to-use password reset systems, companies still experience a significant number of direct help-desk requests. In fact, surveys reveal that 30% of help-desk resources are devoted to access and authentication issues. With an **average cost per password reset call of $22 to $25**, according to Gartner and Forrester Research, respectively, annual help-desk costs for a company can be staggering.

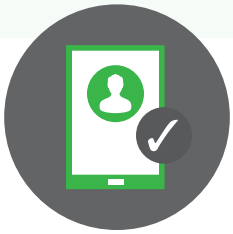
Biometric technology minimizes the need for passwords and the significant costs to support them. Additionally, with an **estimated 600 million biometric-equipped mobile devices in use** (about 28% of smartphones in use globally, according to Acuity Market Intelligence) the hardware to support biometrics is already in the hands of many customers.

An estimated 600 million biometric-equipped mobile devices currently in use globally

Level of Security: Lower → Higher

User authentication methods	Launch cost per user (1 time)	Licensing cost per user (year)	Maintenance cost per user (year)	Total per user (year 1)
Password	< $0.50	Not Appplicable - large banks build this function in-house	$0.003	$0.5
Certificate	$0.20-0.60		$0.003	$0.2-0.6
Token	$0.014 (software) $10-50 (hardware)	$5-10	$20	$35-80
USB/Smart Card	$0.014 (software) $30-60 (hardware)	$5-15	$20	$55-95
Biometrics	**$0.014 (software)**	**$5-6**	**$0.003**	**$5-6**

* Data compiled by Samsung SDS 2017



Customer Impact

When it comes to meeting customer expectations, the bar continues to rise for the financial services industry. Today's customers demand more personalized service, greater convenience, and improved experiences across all channels. Failure to meet these expectations has significant financial repercussions for companies.

Investments in advanced technologies, such as biometrics, to improve the customer experience and strengthen data security help companies attract new customers, as well as improve customer retention rates. According to Bain & Company, a **5% increase in customer retention can increase a company's profitability by 75%**.

A 5% increase in customer retention can increase a company's profitability by 75%

ABOUT SAMSUNG SDS AMERICA, INC.

Samsung SDS America (SDSA) is the U.S. subsidiary of Samsung SDS, a global IT solutions company. SDSA provides purpose-built technology solutions in the areas of enterprise mobility, security, advanced analytics, mobile sales productivity, and training. We enable our customers in the public sector, finance, retail, and other industries to achieve greater freedom, more operational efficiency, and smarter decision making as the driving force for their competitive advantage. SDSA is headquartered in Ridgefield Park, NJ, with offices in Herndon, VA, and San Jose, CA. To learn more about Samsung SDS Biometric Solutions visit www.samsungsdsa.com or email us at bd.sdsa@samsung.com.

ABOUT BIOCATCH™

BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions to protect users and data. Banks and other enterprises use BioCatch to significantly reduce online fraud and protect against a variety of cyber threats, without compromising the user experience. With an unparalleled patent portfolio and deployments at major banks around the world that cover tens of millions of users to date, BioCatch has established itself as the industry leader. The company was founded in 2011 by experts in neural science research, machine learning and cyber security and is currently deployed in leading banks and e-Commerce websites across North America, Latin America, and Europe. For more information, please visit www.biocatch.com.

SAMSUNG SDS AMERICA SAMSUNG BIOCATCH Less Friction. Less Fraud.