

December 2012



**AUTHENTICATION & IDENTITY
MANAGEMENT SOLUTIONS**
*Technology Analysis**

Jason Malo
Research Director, Retail Banking and Cards

Vendor Assessment and Quantitative Insight Teams

** For full copies please contact Matt Angier at CEB TowerGroup*

RETAIL BANKING & CARDS PRACTICE

Executive Director

Aaron Kissel

Practice Manager

Joanne Pollitt

Research Director

Jason Malo

VENDOR ASSESSMENT TEAM

Managing Director

Jaime Roca

Project Manager

Magda Rolfes

Research Analyst

Helen McCann

QUANTITATIVE INSIGHT TEAM

Project Manager

Carolina Valencia

Research Analyst

Ben Fieselmann

COPIES AND COPYRIGHT

As always, members are welcome to an unlimited number of copies of the materials contained within this handout. Furthermore, members may copy any graphic herein for their own internal purpose. The Corporate Executive Board Company requests only that members retain the copyright mark on all pages produced. Please contact your Member Support Center at +1-866-913-6450 for any help we may provide.

The pages herein are the property of The Corporate Executive Board Company. Beyond the membership, no copyrighted materials of The Corporate Executive Board may be reproduced without prior approval.

LEGAL CAVEAT

CEB TowerGroup has worked to ensure the accuracy of the information it provides to its members. This report relies upon data obtained from many sources, however, and CEB TowerGroup cannot guarantee the accuracy of the information or its analysis in all cases. Furthermore, CEB TowerGroup is not engaged in rendering legal, accounting, or other professional services. Its reports should not be construed as professional advice on any particular set of facts or circumstances. Members requiring such services are advised to consult an appropriate professional. Neither The Corporate Executive Board Company nor its programs are responsible for any claims or losses that may arise from a) any errors or omissions in their reports, whether caused by CEB TowerGroup or its sources, or b) reliance upon any recommendation made by CEB TowerGroup.

TECHNOLOGY ANALYSIS SCOPE & METHODOLOGY

In response to feedback from our membership, CEB TowerGroup developed this technology analysis product to identify key components of a technology investment decision and effectively compare vendor technology products. The basis of our process comes from the knowledge that investment decisions revolve around the benefit to the end-user and enterprise of a technology rather than the feature set alone.

This technology analysis is tailored to reflect the needs of the end-user to diagnose the technology attributes particular to a firm, and to effectively identify vendor products that align with the firm's needs. To that end, CEB TowerGroup conducted a series of interviews and surveys with financial services executives, industry experts, and vendors regarding authentication and identity management technology. The results of this research formed the basis of our anatomy and informed the proprietary five point rating system on which we scored individual products.

CURRENT MARKET & FUTURE INVESTMENT

Rapid new channel growth forces financial institutions to effectively manage fraudulent activity across all channels. The preferred banking method changed drastically from 2010 to 2011: customers became almost two times as likely to favor internet banking. Meanwhile, branches and ATMs decreased by 5% and 7% respectively as preferred forms of banking. This does not mean, however, that those same customers will not use other channels because when referring to problem resolution, only 21% of customers preferred online or mobile person-to-person interaction. Consistency in security practices and a holistic view of fraud in all channels is essential since customer information and transactions can be performed at multiple points of access.

As mobile and traditional online banking channels constantly change, authentication solutions are adapting to new regulations and channels. Fifty-nine percent of respondents to our authentication survey have been audited for compliance with the 2011 FFIEC supplement regulations, demonstrating solid progress in the past year. There is still much to be done, however, as a third of currently-deployed authentication management solutions have not yet been part of a formal audit, and 8% have conducted their own audit internally, but not externally. With respect to the new guidance, 25% of respondents raise concerns because they have solutions that do not currently support out of band authentication.

With new electronic channels developing, financial institutions will depend on strong integration and on a variety of authentication methods to mitigate risk and fraudulent activity. Financial institutions will seek authentication solutions that have a policy engine that integrates out-of-the-box with fraud detection systems, and eventually, with anti-malware systems. As mobile device capabilities evolve, financial institutions will leverage its credential management abilities, profiling, and reputation. If the user can manage his/her credentials from a mobile device while the bank determines risk through profiling and reputation of the mobile device, customers will continue to have a seamless experience when logging into a session remotely.

VENDOR LANDSCAPE AND RANKINGS

CEB TowerGroup identified vendors for this analysis based on expert opinion, product maturity, size of installations, and technological innovation. This technology analysis includes Authentify, CSC, Equifax, Experian, HID Identity Assurance, PhoneFactor, RSA, Symantec, TeleSign and VASCO. CEB TowerGroup included profiles of selected authentication solutions. In the case of Experian and RSA, we technically featured more than one solution, because they are commonly bundled as a package and sold together.

By combining our qualitative and quantitative data from interviews with industry experts, financial institutions and vendors, CEB TowerGroup identified 21 attributes that define a “best-in-class” authentication/ identity management solution. These attributes are grouped into four categories that highlight a firm’s user and enterprise needs. Vendor rankings are based on our proprietary five point rating scores on each of the 21 “best-in-class” attributes. The top vendors were designated as best-in-class performers based on their composite scores in each of the technology categories below.

BEST-IN-CLASS TECHNOLOGY CATEGORIES

Executives investing in authentication management solutions technology should use The Technology Anatomy on page 27 to select the vendor that best aligns with their firm’s needs and business objectives.

Vendors are listed in alphabetical order.

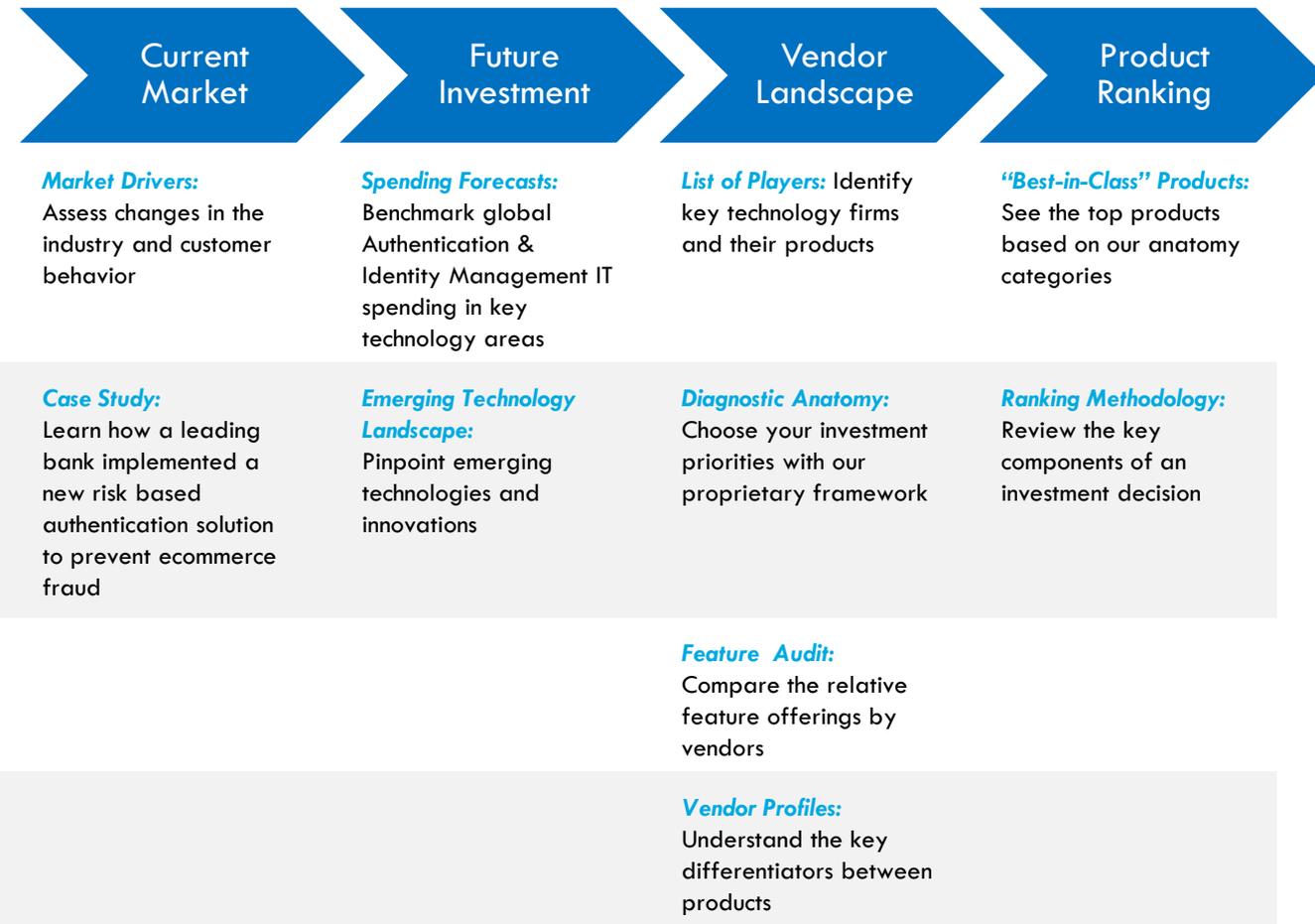
- **CUSTOMER ENGAGEMENT** includes those attributes that facilitate the authenticating customer’s comprehension of and successful interaction with the solution. *Leaders include CSC’s ConfidentID Mobile, HID Identity Assurance’s 4TRESS, and RSA’s Authentication Services.*
- **USER WORKFLOW SUPPORT** includes those attributes that administer credentials and authentication policies, as well as the ability to leverage these across channels.
Leaders include PhoneFactor’s PhoneFactor, RSA’s Authentication Services, and TeleSign’s TeleSign 2FA.
- **ENTERPRISE OPERATIONS** includes those attributes that address the solution diversity, technical implementation, and solution reporting for security and compliance roles. *Leaders include RSA’s Authentication Services, TeleSign’s TeleSign 2FA, and VASCO’s DIGIPASS.*
- **ENTERPRISE SUPPORT** includes those attributes that influence the enterprise’s tactical fit and strategic alignment with the vendor.
Leaders include RSA’s Authentication Services, TeleSign’s TeleSign 2FA, and VASCO’s DIGIPASS.

› **Mission Statement: CEB TowerGroup technology analysis process provides a customer-driven, transparent, and unbiased review designed to drive informed business decisions.**

- **Current Market:** Provides a view of industry and customer changes and best practices for technology investment and implementation.
- **Future Investment:** Forecasts IT spending and identifies emerging technologies and innovations.
- **Vendor Landscape:** Provides an overview of key vendors, product features, and market position.
- **Product Rankings:** Highlights best-in-class attributes and shows a comparative perspective of leading products.

TECHNOLOGY ANALYSIS OVERVIEW

Technology Analysis Presentation Roadmap



ROADMAP FOR THE PRESENTATION



Current Market



Future
Investment



Vendor
Landscape



Product Rankings

› **The steady decline in identity fraud was derailed by the financial crisis in 2008. Economic turmoil combined with the rapid growth of online and mobile banking now necessitate greater investment in fraud prevention.**

- Fraud incidence and loss both declined after the FFIEC published its 2005 *Guidance on Authentication in an Internet Banking Environment*, before surging to new highs in the wake of the 2008 Financial Crisis.
- Although fraud decreased substantially in 2010, half of financial institutions report that losses increased again in 2011, compared with just 15% who said that losses decreased.
- A quarter of those institutions who reported a 2011 increase in losses saw costs go up by more than 5%.

CEB TOWERGROUP RETAIL BANKING AND CARDS PRACTICE

© 2012 The Corporate Executive Board Company. All Rights Reserved.

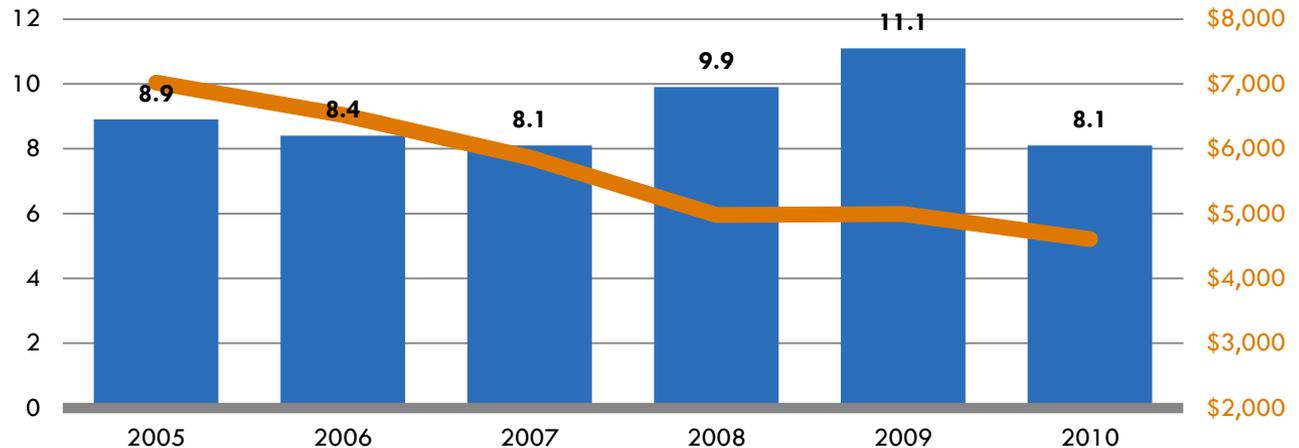
COMBAT INCREASING FRAUD

US Adult Victims of Identity Fraud

In Millions, 2006 – 2010

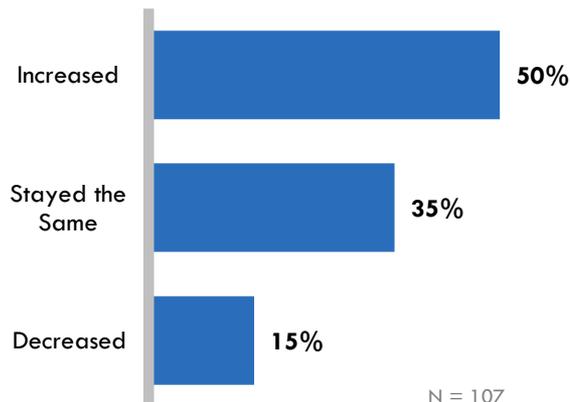
Average Cost Per Fraud Victim

In USD, 2006 – 2010



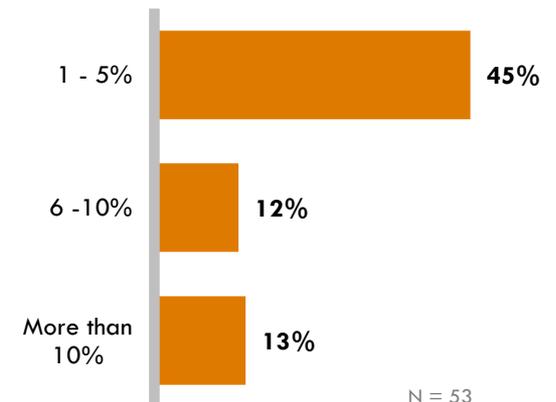
Change in Fraud Losses

Percentage of Respondents, 2010 vs. 2011



Percentage Change in Financial Losses

Percentage of Respondents per Range, 2010 vs. 2011



Source: CEB TowerGroup Research

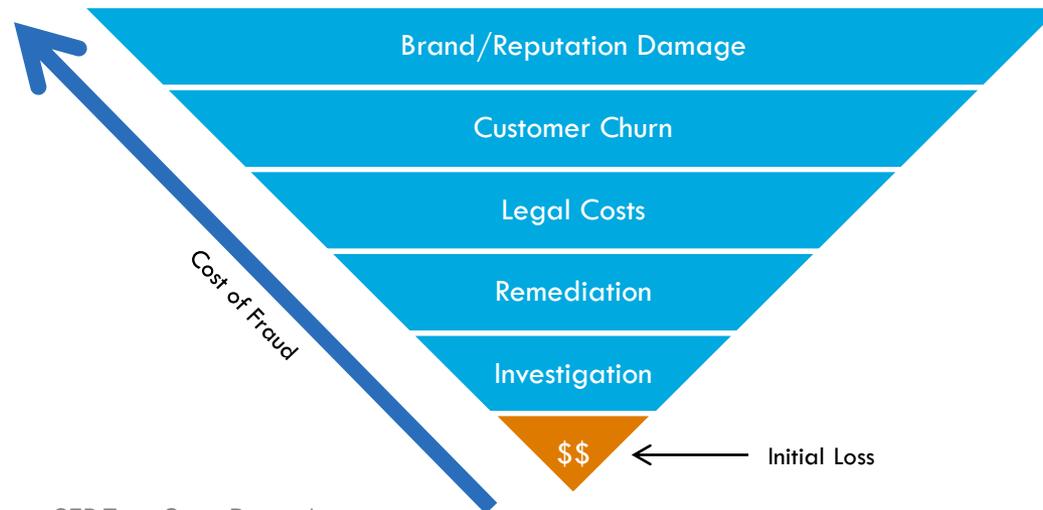
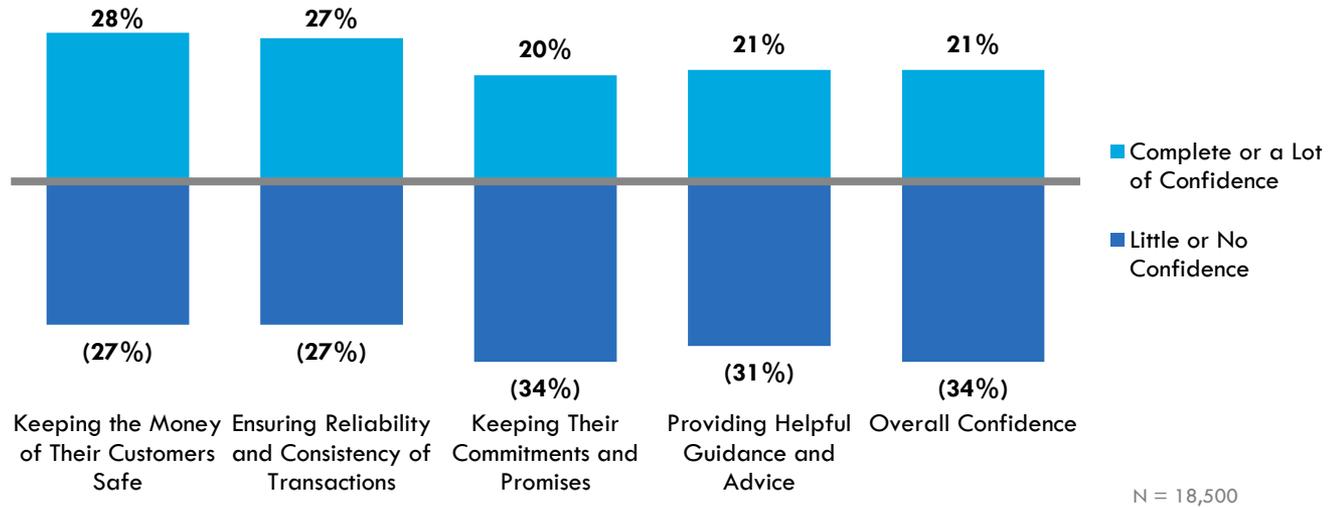
Consumer confidence, already low, is further eroded by banks' failure to prevent fraud.

- Consumers who have little or no confidence in their financial services providers outnumber those that do by a 3 to 2 ratio.
- The price of ineffective authentication and identification far exceeds the immediate monetary loss due to fraud.
- Ultimately, the loss of customer confidence that often results in attrition and reputation damage is the most costly result of failed fraud prevention.

UNDERSTAND THE FULL IMPLICATIONS OF FAILED AUTHENTICATION

Confidence in Financial Services Providers

Percentage of North American Consumers Who Feel Confident in the Capabilities of Their Financial Services Providers

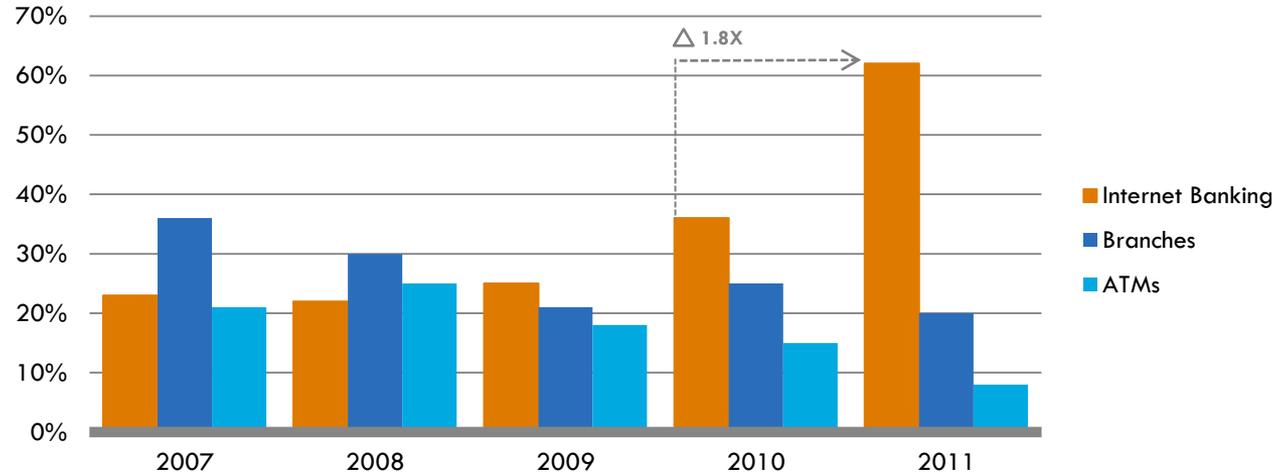


» **Rapid growth in the popularity of online banking has created new challenges in authentication and identification.**

- Internet Banking has rapidly become the preferred method of banking among all age groups, nearly doubling in popularity between 2010 and 2011.
- Security concerns related to authentication and identification are most pressing when controlling customer access to financial products and services.
- Access is the banking function that is most likely to be performed online, as nearly half of customers prefer to access their accounts online.

EFFECTIVELY MANAGE NEW CHANNEL GROWTH

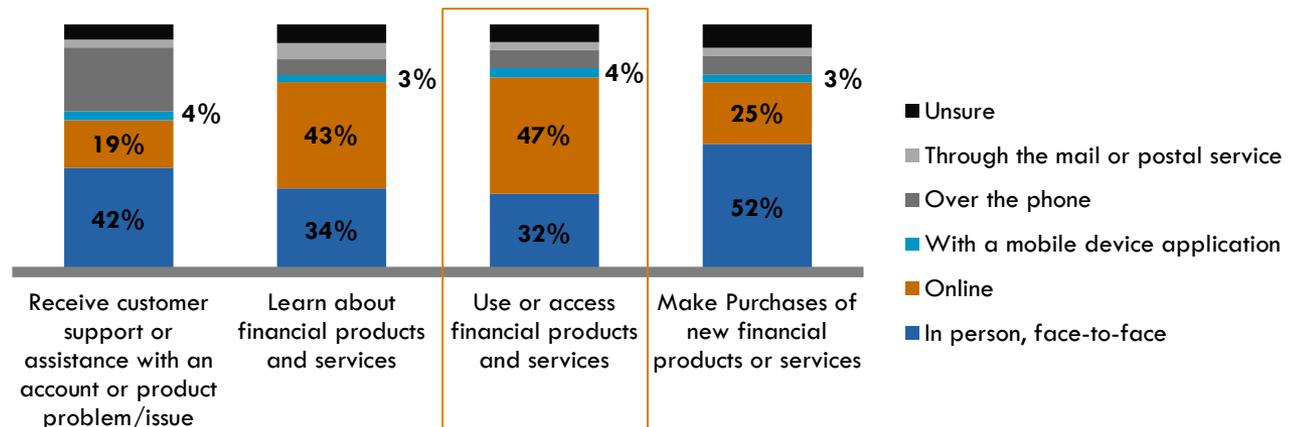
Preferred Banking Method
All Age Groups, 2007-2011



Source: American Bankers Association

Reported Channel Preferences for Specific Banking Functions

Percent of Respondents, 2012



Source: CEB TowerGroup Research

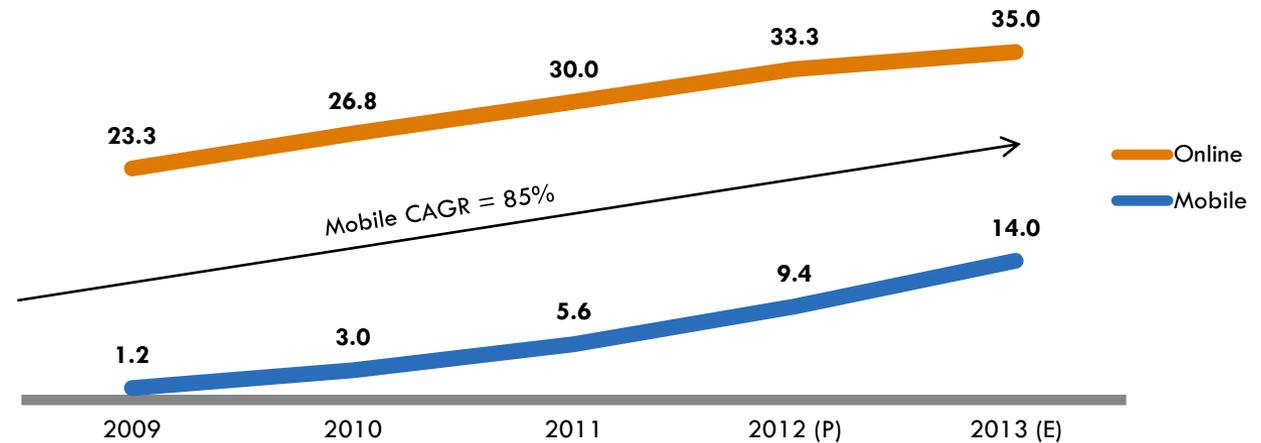
› **Mobile banking is quickly becoming one of the most critical access channels in the industry.**

- The volume of US mobile banking transactions will grow 85% annually between 2009 and 2013 as consumers continue to adopt this technology.
- Online banking transactions will increase by a multiple of 1.5 between 2009 and 2013.
- The number of mobile banking transactions in 2013, on the other hand, will skyrocket to over 10 times the number of mobile transactions in 2009.

LOOK BEYOND TRADITIONAL ONLINE BANKING

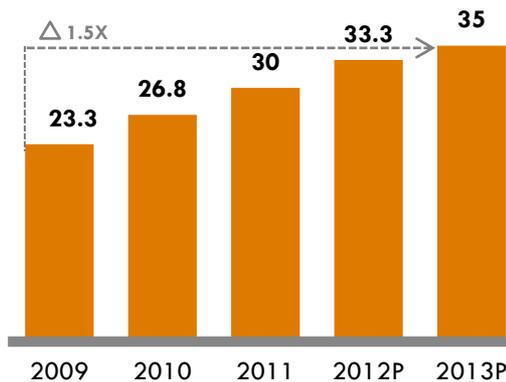
US Mobile and Online Banking Channel Growth

Billions of Transactions, 2009-2013P



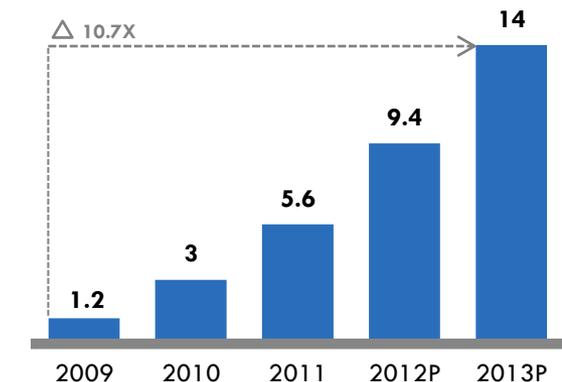
US Online Banking Channel Growth

Billions of Transactions, 2009-2013P



US Mobile Banking Channel Growth

Billions of Transactions, 2009-2013P



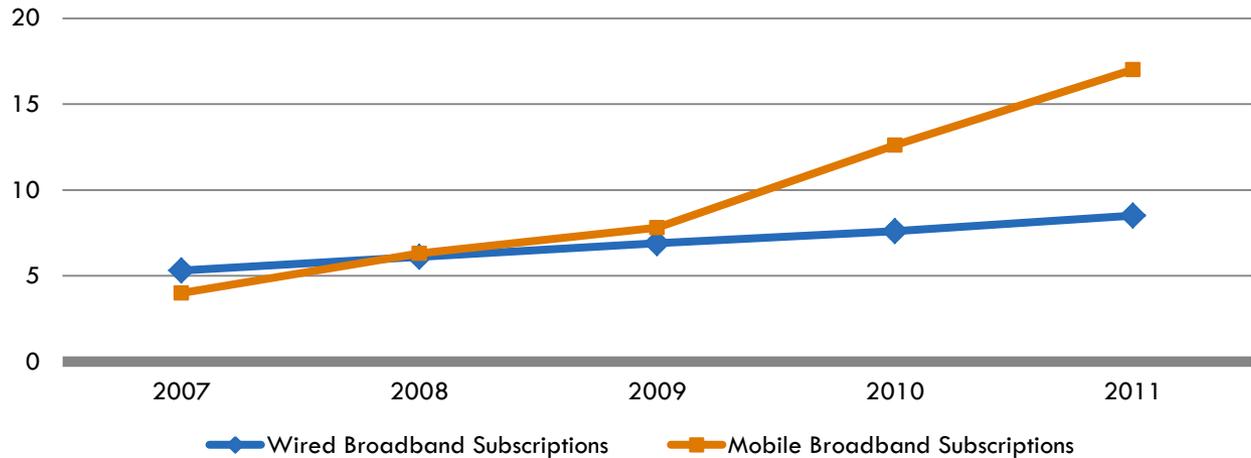
› **Rapid increase in mobile broadband usage as an alternative channel will likely raise potential security issues for financial institutions.**

- In 2011, twice as many people used mobile broadband subscriptions than used wired broadband subscriptions.
- The global average penetration rate for mobile broadband reached 17% in 2011. Growth was highest in emerging countries, but overall adoption remains much higher in Europe and in the Americas.

PREPARE FOR A MOBILE FUTURE

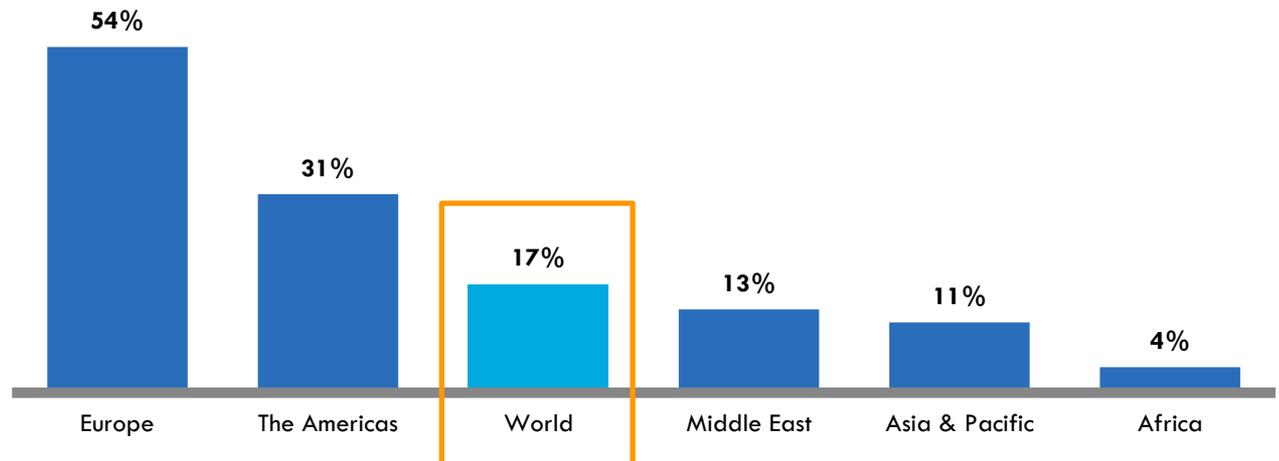
Global Broadband Internet Usage

Broadband Subscriptions per 100 Inhabitants, 2007-2015E



Mobile Broadband Penetration by Region

Percentage of Mobile Broadband Subscribers, 2011



» **As mobile and traditional online banking channels change, authentication solutions must adapt to new regulations and channels.**

- New FFIEC compliance standards must be met by 2011, and while 59% of solutions have been audited by external professionals, almost a third (33%) have not been part of a formal audit.
- Meanwhile, half of authentication solutions support multiple factors of authentication, but 42% support only two factors, and 8% only support one factor.
- Importantly, only 8% of authentication solutions support multiple out-of-band channels and devices, and 25% do not support out-of-band authentication all together.

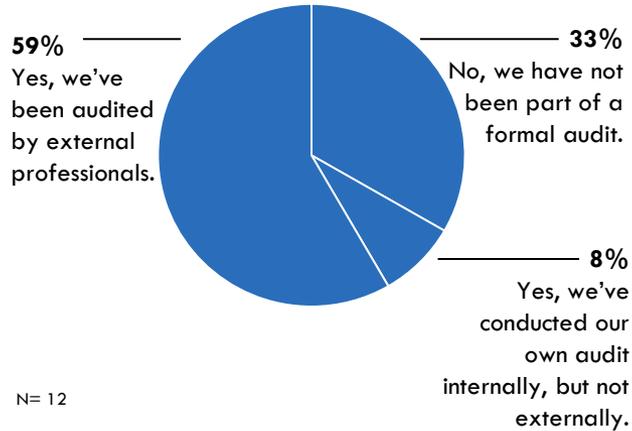
CEB TOWERGROUP RETAIL BANKING AND CARDS PRACTICE

© 2012 The Corporate Executive Board Company. All Rights Reserved.

KEEP UP WITH AUTHENTICATION CHANGES

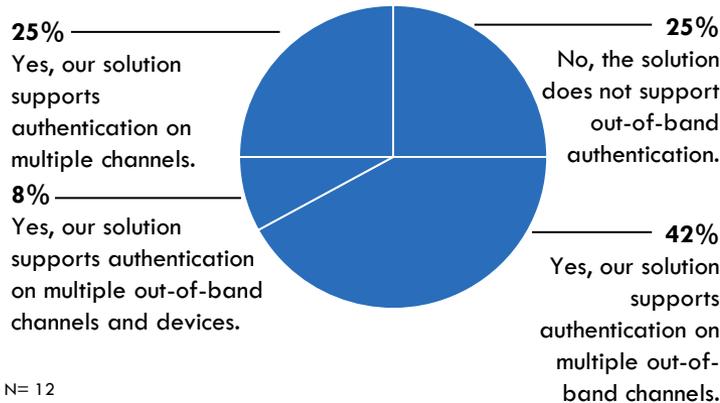
Has your AIM solution been part of an FFIEC compliance audit since the 2011 supplement to the authentication guidance?

Percentage of Respondents, 2012



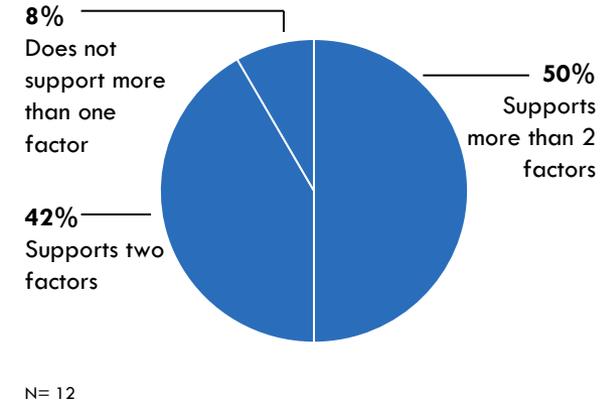
Does your solution provide authentication using out-of-band channels and devices?

Percentage of Respondents, 2012



Does your solution support multiple factors of authentication?

Percentage of Respondents, 2012



› **Glover Bank¹ felt major limitations on eCommerce caused by unwieldy authentication that cramped customer loyalty.**

- Glover Bank's password-based authentication did not distinguish between legitimate and potentially fraudulent transactions.
- Customers were irritated when they had to enter a password for each transaction, and their frustration decreased the likelihood of future online purchases.

CASE STUDY: AUTHENTICATION GONE WRONG

Business Objectives

- › Strike a balance between strong security and customer convenience when authorizing Card Not Present eCommerce transactions.
- › Provide a hosted solution with accurate, real-time detection, minimal impact to customers, and no data migration.

Former Solution

To comply with VISA and MasterCard 3D Secure requirements, Glover Bank used a password-based authentication product.

For customers' first purchase, they entered personal information and created a password. For each subsequent purchase, the system would require customers to re-enter their password.

They could skip authentication three times before their account was shut down.



Glover Bank¹ At a Glance

- 1.4 million customers
- 200 branches
- 600+ ATMs
- 24/7 call center
- Online banking

This solution had three systematic shortcomings...



1 The system required a password for each purchase, regardless of risk. This was a major annoyance for legitimate customers.



2 The authentication provider did not incorporate new data quickly, which caused problems for some customers.



3 The system did not learn from past transaction behavior, so Glover Bank could only react to new fraud trends, rather than plan for them.



¹Pseudonym

Streamlined authentication yields dual benefits of higher customer satisfaction and efficient operational processing.

A TURNAROUND IN AUTHENTICATION MANAGEMENT

Risk Based Authentication

Reduce fraud losses in real time through a Bayesian Risk Engine and policy-based rules

Evaluates each transaction and uses customer history to determine risk

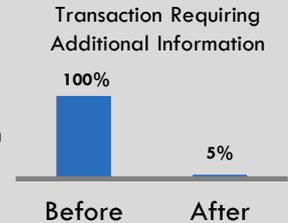
Identifies high risk transactions

Learns from past behavior to address emerging threats like Man-in-the-Middle and Man-in-the-Browser Trojans

Receives daily batch with updated customer information to ensure real-time accuracy

Benefits Realized

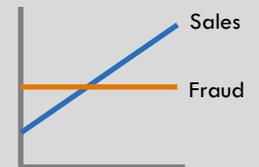
1 95% of transactions are authenticated without requiring additional information



2 Less than 1% of challenged transactions are false positives



3 50% increase in sales volume of 3D secure transactions without an increase in fraud losses.



4 90% drop in calls to the call center, so IT resources can be used elsewhere



5 Higher customer satisfaction, because the bank only intervenes with legitimate risks



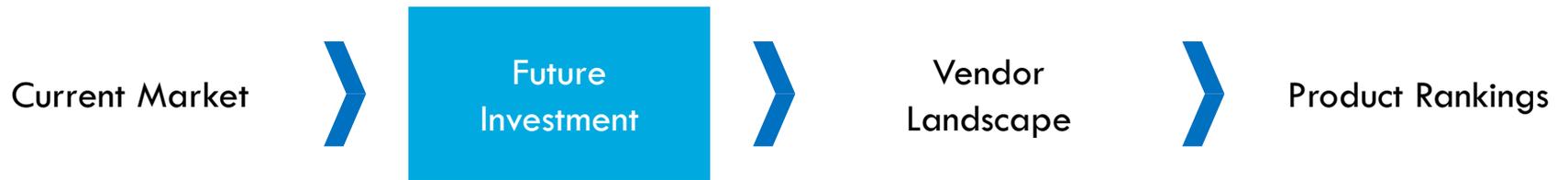
¹Pseudonym

CEB TOWERGROUP RETAIL BANKING AND CARDS PRACTICE

© 2012 The Corporate Executive Board Company. All Rights Reserved.

Source: RSA, CEB TowerGroup Research

ROADMAP FOR THE PRESENTATION



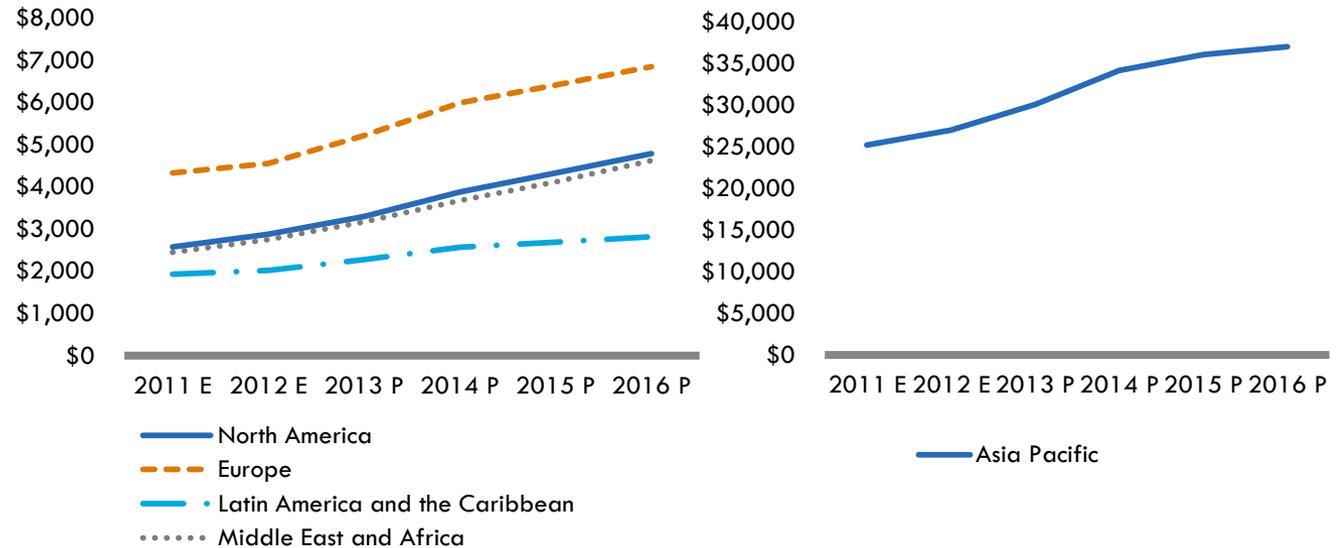
Authentication and Identity Management IT spending in the developed regions of Europe and North America is forecasted to be mainly driven by current banking consumers diversification of banking relationships.

- New spending growth in developing regions is expected to be driven by inclusion of previously unbanked persons into the formal banking system.

REGIONAL FORECAST OF AUTHENTICATION SPENDING

Regional Forecast of Authentication Technology Spending

In Millions USD, 2011(E) – 2016(P)

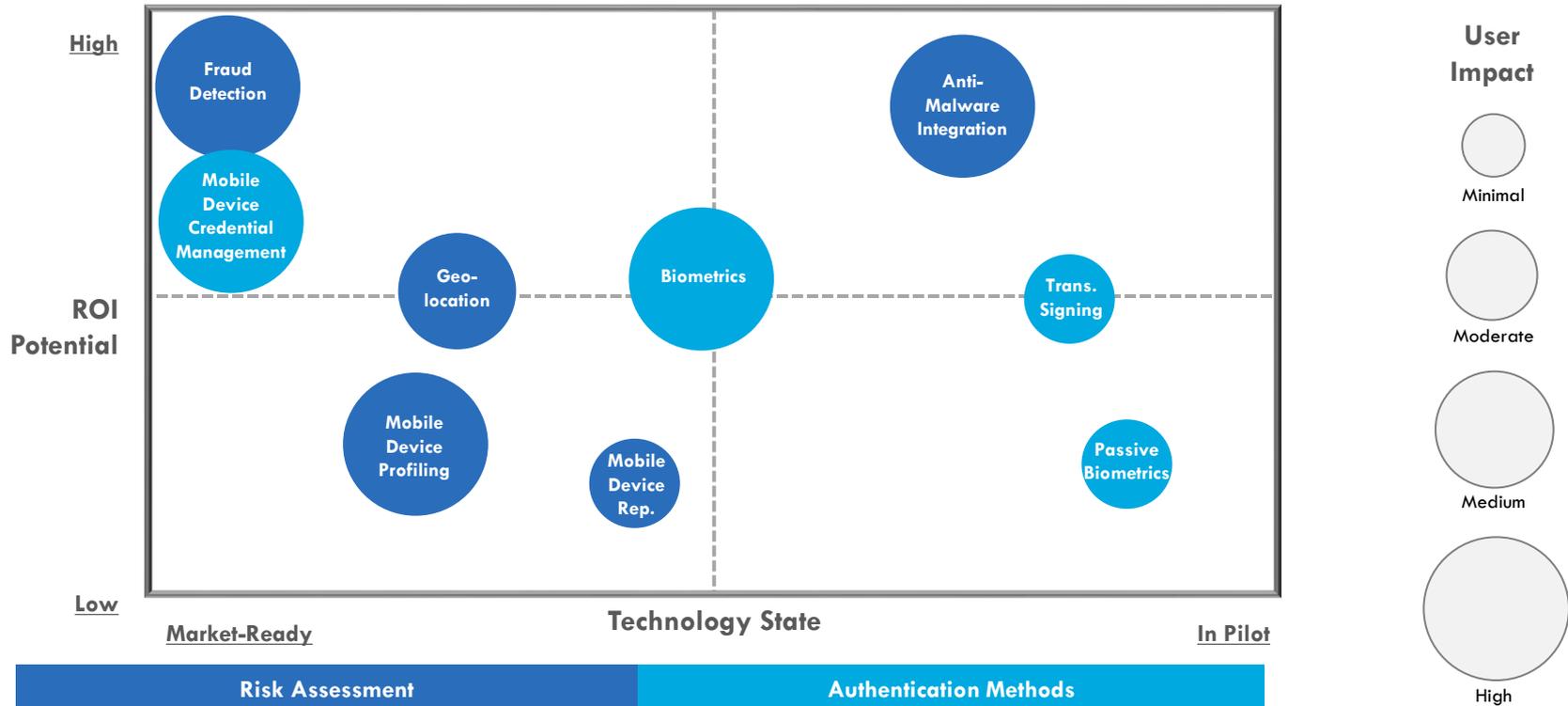


Regional Spend (In Millions of USD)	2011 E	2012 E	2013 P	2014 P	2015 P	2016 P	CAGR
North America	\$2,576	\$2,881	\$3,297	\$3,880	\$4,328	\$4,785	13.2%
Europe	\$4,327	\$4,551	\$5,217	\$5,994	\$6,408	\$6,850	9.6%
Latin America and the Caribbean	\$1,929	\$2,020	\$2,279	\$2,569	\$2,691	\$2,818	7.9%
Middle East	\$2,453	\$2,754	\$3,171	\$3,678	\$4,119	\$4,625	13.5%
Asia Pacific	\$25,237	\$27,031	\$30,122	\$34,202	\$36,098	\$37,056	8.0%

Note: E indicates estimated values; P indicates predicted values; CAGR: compound annual growth rate.

Source: CEB TowerGroup Research

EMERGING TECHNOLOGIES IN AUTHENTICATION MANAGEMENT



Risk Assessment	Authentication Methods
<ul style="list-style-type: none"> • Fraud Detection: the ability to identify and prevent fraudulent activity by requiring additional authentication • Geo-Location: the ability to determine the customer's physical location to validate his or her identity • Mobile Device Profiling: the identification of a device by multiple hardware and software attributes • Mobile Device Reputation: the understanding the activities of a single device in the financial ecosystem • Anti-Malware Integration: the capacity to detect malware on the device via signature or suspicious activity 	<ul style="list-style-type: none"> • Mobile Device Credential Management: the end user's ability to manage his/her credentials from a mobile device • Biometrics: the voice, facial and tactile recognition methods to identify a customer • Transaction Signing: an additional layer of transaction manifest to secure an authentication session • Passive Biometrics: the identification of a customer's voice through deep analytics that recognize voice without requiring a specific password or phrase

DEFINITIONS

- **ROI Potential:** Measures the relative returns an institution can expect to receive from an investment in the technology
- **Technology State:** Measures the technology's level of development
- **User Impact:** Measures the level of benefit the technology will have on the authentication user

ROADMAP FOR THE PRESENTATION

Current
Market



Future
Investment



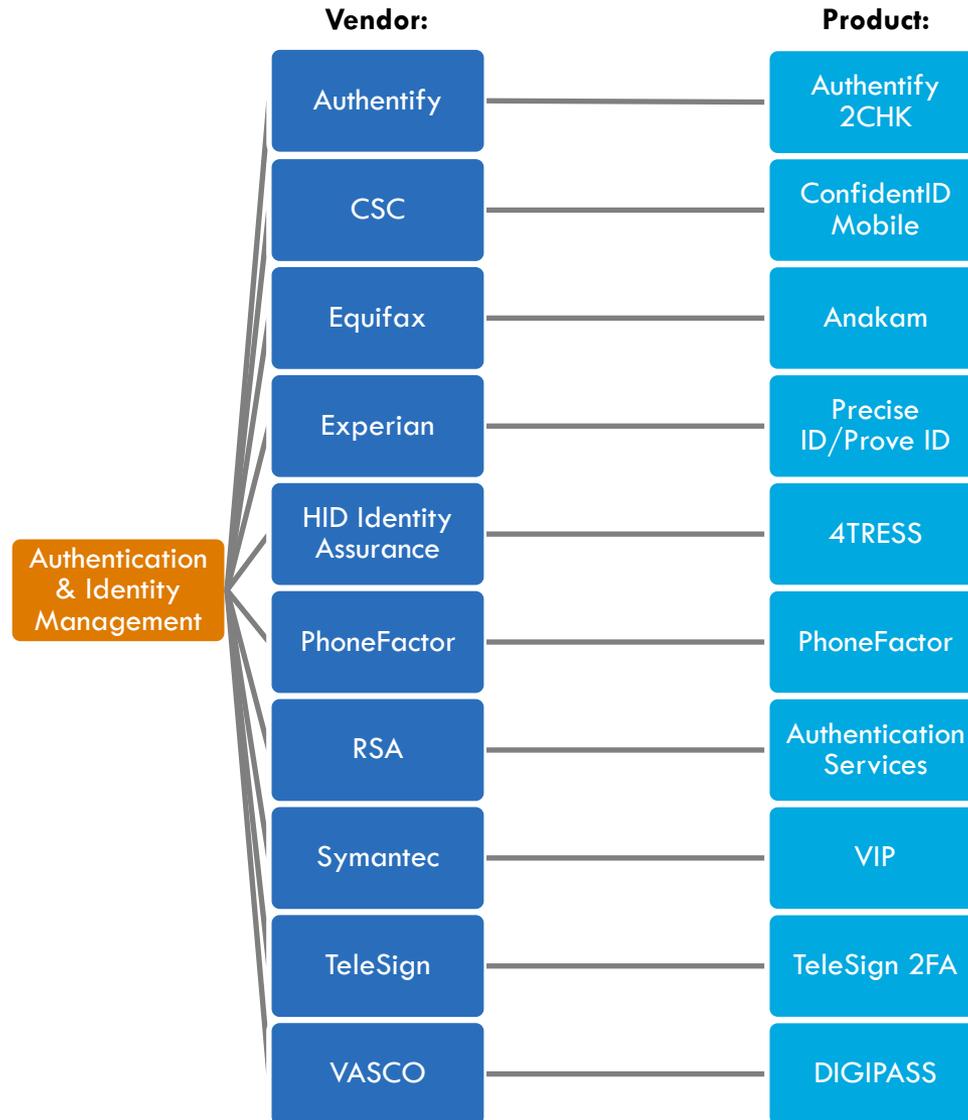
Vendor
Landscape



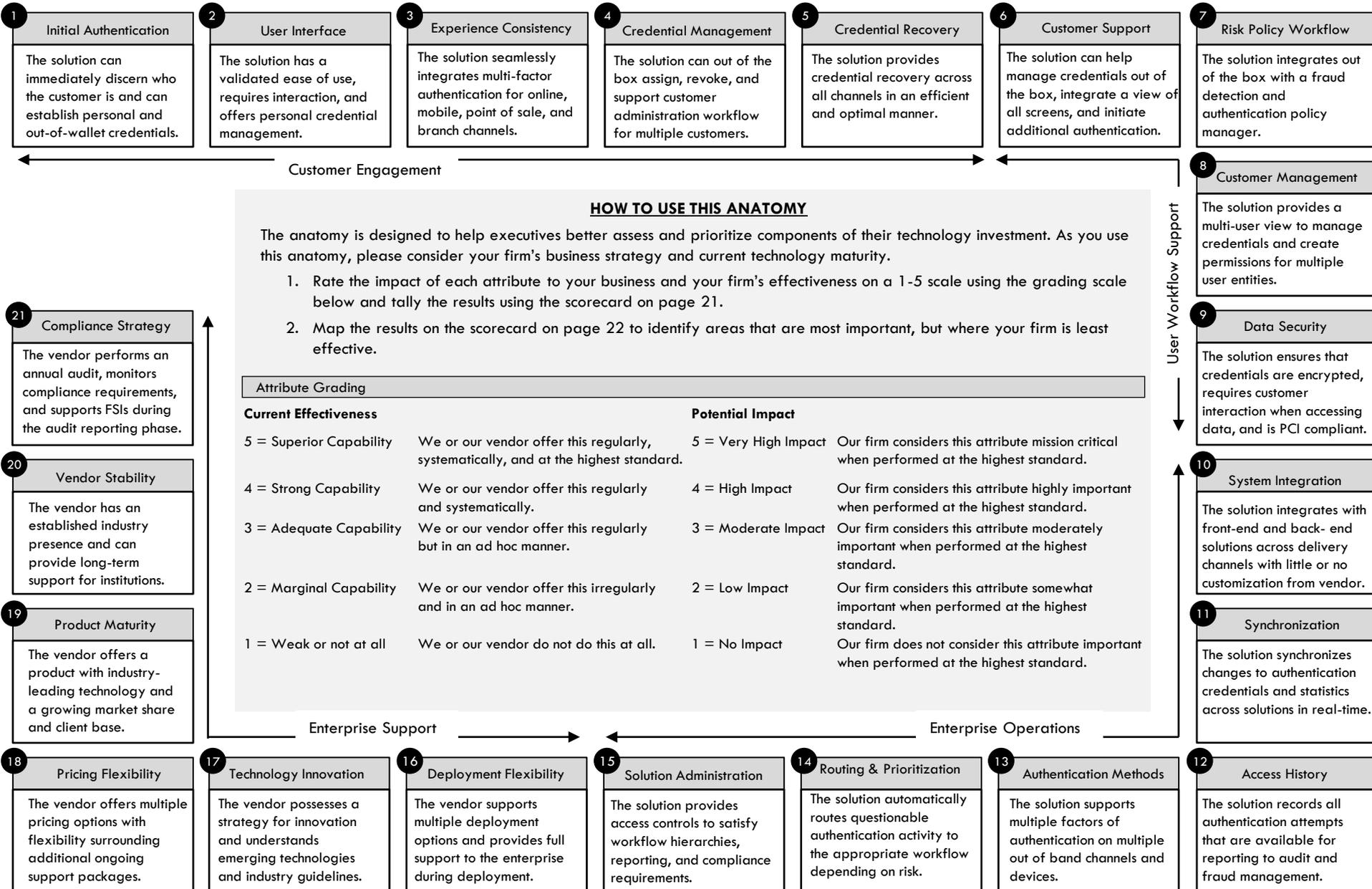
Product
Rankings

CEB TowerGroup identified 10 vendors for this analysis based on expert opinion, product maturity, size of installations, and vendor stability.

MAPPING THE VENDOR LANDSCAPE



AUTHENTICATION SOLUTION DIAGNOSTIC ANATOMY



Score Your Technology Needs with the Anatomy Scorecard.

- Financial services executives should complete the scorecard using the authentication solution anatomy diagnostic tool.

AUTHENTICATION SOLUTIONS SCORECARD

<u>Attribute Categories</u>	<u>Alignment Attributes</u>	<u>Current Effectiveness</u>	<u>Potential Impact</u>
Customer Engagement	1. Initial Authentication		
	2. User Interface		
	3. Experience Consistency		
	4. Customer Credential Mgmt.		
	5. Credential Recovery		
User Workflow Support	6. Customer Support		
	7. Risk Policy Workflow		
	8. Customer Management		
	9. Data Security		
Enterprise Operations	10. System Integration		
	11. Synchronization		
	12. Access History		
	13. Authentication Methods		
	14. Routing and Prioritization		
	15. Solution Administration		
Enterprise Support	16. Deployment Flexibility		
	17. Technology Innovation		
	18. Pricing Flexibility		
	19. Product Maturity		
	20. Vendor Stability		
	21. Compliance Strategy		

Source: CEB TowerGroup Research

› Retail banking executives should map their attribute scores from rating their impact and effectiveness on the previous page on this matrix to identify the most important areas to their vendor selection.

AUTHENTICATION SOLUTIONS SCORECARD

		Areas of Focus				
Potential Impact	5 =Very High					
	4 =High					
	3 = Moderate					
	2 =Low					
	1 =No Impact					
		1 =Weak	2 = Marginal	3 = Adequate	4 =Strong	5 = Superior
		Current Effectiveness				

FEATURE AUDIT DEFINITIONS

Authentication Platform	
Features	Definitions
Separate Customer Credential Database	The solution has a separate customer credential database to create data segmentation for security.
Integrate with KYC	The solution integrates with Know Your Customer analytics and monitoring.
Customer (FSI) Management Reports	The solution can create and maintain customer management reports. Both out of the box and customer reports created by the FSI are available.
Risk-Based Workflow (Native)	The solution provides or integrates seamlessly with a risk-based workflow that automatically queues items based on perceived risk.
Credential Distribution Strategy	The solution scrambles and splits credentials and distributes them randomly to protect against attackers.
User Alerts	The solution has built-in native alerts that can identify the user who performed actions or activities.
User Guides	The solution includes a self-explanatory guide to the workflow and intricacies of the solution.
Multi-Application Framework	The solution includes a framework that is designed to support authentication for multiple applications.
Data Security	The solution has encrypted credentials that require customer interaction when accessing data.
Authentication Self-Service	
Credential Management Workflow	The solution can manage credentials natively within the workflow.
User Risk Tolerance Management	The solution can identify, assess, and prioritize perceived risk of an authentication attempt and manage it in the self-service portal.
Credential Reset	The solution can support a user who wishes to report a lost or stolen credential or create a new credential.
Account Access Administration	The solution allows appropriate users to access and manage accounts through the self service portal.
User Permission Administration	The solution supports a permission based hierarchy through the self-service portal.
Authentication “Factors”	
“What You Know”	The solution can authenticate your identity by determining what you know.
“What You Have”	The solution can authenticate your identity by determining what you have.
“What You Are”	The solution can authenticate your identity by determining what you are.
“Where You Are”	The solution can authenticate your identity by determining where you are.
Out-of-Band Delivery	The solution supports multiple streams of data from various channels in order to authenticate and validate a user's identity.

FEATURE AUDIT DEFINITIONS CONTINUED

Authentication Methods	
Features	Definitions
Knowledge-based Questions	The solution asks the customer knowledge-based questions in order to authenticate their identity.
One-time Passcode	The solution provides the customer with a one-time passcode via SMS or email to authenticate their identity.
Voice Biometric	The solution offers analytics that authenticate the customer through voice.
Tactile Biometric (e.g. fingerprint)	The solution offers analytics that authenticate the customer through physical touch.
Visual Biometric (e.g. face)	The solution offers analytics that authenticate the customer through facial recognition.
Shared Image	The solution provides site verification to the consumer by presenting a custom image.
Reputation-Based (e.g. IP, Phone Number)	The solution can score a device based on a collection of opinions that other entities hold about the object.
Device Profiling	The solution can authenticate the customer by analyzing important information about their device.
Physical Token	The solution offers a hardware security device that authorizes the customer through two factors.
Software Token	The solution offers a software security device that authorizes the customer through two factors.
SMS	The solution sends an SMS with a code to a mobile device and the customer inputs the code to authenticate their identity.
Mobile App	The solution offers a mobile application that authenticates the user.
Mobile App Integration	The solution integrates with a mobile application to authenticate the user.
Location-Based	The solution can use the customer's location to authenticate them.
Authentication Channels	
Customer Support	The solution can authenticate the customer through a portal or help desk.
Mobile	The solution can authenticate the customer through the mobile channel.
Online	The solution can authenticate the customer through an online channel.
Banking Centers	The solution can authenticate the customer through the banking center.
ATM	The solution can authenticate the customer at the ATM.

FEATURE AUDIT DEFINITIONS CONTINUED

Threat Vector Addressed	
Features	Definitions
Phishing	The solution prevents an attacker from acquiring information such as usernames and passwords.
SMiShing	The solution prevents an attacker from retrieving the customer's confidential SMS code.
Man in the Middle	The solution prevents an attacker from hijacking a valid session and committing fraud.
Banking Trojans	The solution prevents an attacker from stealing banking information through downloads and phishing schemes.
Man in the Browser	The solution uses browser security features to prevent attackers from infecting and modifying web browsers.
Stolen Credentials	The solution prevents an attacker from stealing a credential and internally reports that credential as invalid.
Lost Device	The solution can support and delete a credential when a device is identified as stolen.
Spoofed Mobile App	The solution prevents a mobile application from being hacked or imitated.

Feature Type	Definition
<input checked="" type="radio"/> Standard Native Feature	The feature is standard to the system and is offered as an out-of-box functionality of the base product.
<input type="radio"/> Premium Native Feature	The feature is part of an optional module to the solution developed by the vendor, and is offered for an additional fee on top of the base price.
<input type="radio"/> Emerging Feature	The feature is emerging and will be offered in the next 12 months.
<input type="radio"/> Developing Feature	The feature is in the development stage and will be offered in the next 12-24 months.

FEATURE AUDIT

	Features	RSA Authentication Services	% of Vendors Offering as Standard Feature	
Authentication Platforms	Separate Credential Database	●	60%	
	Integrate with KYC	●	90%	
	Customer Mgmt. Reports	●	100%	
	Risk-Based Workflow	●	70%	
	Integrate with Risk Assessment Workflow	●	70%	
	Credential Distribution Strategy	●	50%	
	User Alerts	●	90%	
	User Guides	●	100%	
	Multi-App. Framework	●	90%	
	Data Security	●	100%	
	Authentication Self-Service	Credential Mgmt. Workflow	●	70%
		User Risk Tolerance Mgmt.	●	40%
Credential Reset		●	70%	
Account Access Admin.		●	70%	

	Features	RSA Authentication Services	% of Vendors Offering as Standard Feature
Authentication "Factors"	"What You Know"	●	100%
	"What You Have"	●	90%
	"What You Are"	●	40%
	"Where You Are"	●	60%
	Out-of-Band Delivery	●	90%
	Authentication Methods	Know. Based Quest.	●
One Time Passcode		●	80%
Voice Biometric		●	30%
Tactile Biometric		●	30%
Visual Biometric		●	10%
Shared Image		●	30%
Reputation Based		●	80%
Device Profiling		●	50%
Hard Token		●	50%
Soft. Token		●	60%
SMS		●	80%
Mobile App		●	80%
Mobile App. Integration		●	80%
Location Based		●	40%

FEATURE AUDIT CONTINUED

	Features	RSA Authentication Services	% of Vendors Offering as Standard Feature
Authentication Channels	Customer Support	●	90%
	Mobile	●	80%
	Online	●	90%
	Banking Centers	●	80%
	ATM	●	50%
Threat Vector Addressed	Phishing	●	80%
	SMiShing	●	60%
	Man in the Middle	●	80%
	Banking Trojans	●	70%
	Man in the Browser	●	80%
	Stolen Cred.	●	80%
	Lost Device	●	70%
Complies with and Will Pass Audit for	Spoof Mobile App	●	60%
	ADA	●	80%
	FFIEC	●	100%
	HIPAA	●	90%
	NIST	●	100%
	PCI	●	100%
	SAS 70 II	●	80%

Feature Type	Definition
● Standard Native Feature	The feature is standard to the system and is offered as an out-of-box functionality of the base product.
● Premium Native Feature	The feature is part of an optional module to the solution developed by the vendor, and is offered for an additional fee on top of the base price.
○ Emerging Feature	The feature is emerging and will be offered in the next 12 months.
○ Developing Feature	The feature is in the development stage and will be offered in the next 12-24 months.



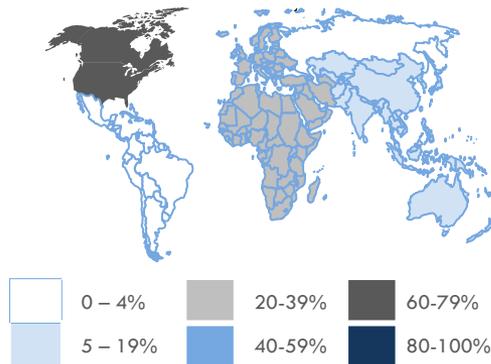
Key Statistics

Company Type: Public
HQ: Bedford, MA
Parent Company: EMC
Founded: 1982
Employees: 2,200
Revenue: \$20 billion
Client Base: 35,000 customers

Distribution of Clients by Asset Size

<\$1 Billion	\$1-10 Billion	\$10 – 50 Billion	>\$50 Billion
	Not Disclosed		

Distribution of Clients by Region



Source: CEB TowerGroup Research, RSA

CEB TOWERGROUP RETAIL BANKING AND CARDS PRACTICE

© 2012 The Corporate Executive Board Company. All Rights Reserved.

AUTHENTICATION SERVICES

RSA

Company Overview:

Founded in 1982, RSA manages organizational risk, safeguards mobile access, and secures virtual and cloud environments. In 2006, RSA was acquired by EMC and now serves as its security division that provides security, risk and compliance management solutions.

Product Overview:

RSA Adaptive Authentication is a risk-based authentication and fraud detection platform, while RSA Authentication Manager allows organizations to deploy and manage security tokens and risk-based authentication across users, applications and agents from a central platform. Both Adaptive Authentication and Authentication Manager are offered as hosted and on-premise authentication management solutions.

Product Demonstration Highlights:

- **Self Service Portal:** RSA Authentication Manager offers a web portal that features various self-service options where users can test or register for tokens and reset their PINs. This self-service portal also allows administrators to approve pending requests, thus reducing the number of calls requiring IT support.
- **Self Learning Risk Engine:** RSA Adaptive Authentication and RSA Authentication Manager both leverage RSA's Risk Engine technology which utilizes a risk and rules-based approach to assign a risk score to each login or transaction. The RSA Policy Manager enables the easy creation of rules such as initiating an additional authentication challenge when the risk score exceeds an acceptable level, as determined by each organization.
- **Data Security:** RSA focuses on security and encryption through a sophisticated permission-based hierarchy administration. Both RSA Authentication Manager and RSA Adaptive Authentication can be deployed for PCI compliance. Authentication Manager is based on the Advanced Encryption Standard (AES) algorithm, a recognized standard that is continuously challenged by cryptologists to ensure strength and dependability.

CEB TowerGroup View:

RSA's Authentication service earned best-in-class rankings in all four categories, demonstrating a comprehensive set of authentication methods, and the service and management consoles required to administer user authentication for organizations of all sizes. Their adaptive model provides a policy engine driven by integration with fraud detection engines, customer rules, and RSA's own risk engine. The recent acquisitions of NetWitness, Silver Tail Systems and Archer Technologies ensure that these risk assessment technologies are well supplied with current threat information to complement the user-level metrics needed to make intelligent decisions. Other vendors have been able to gain traction in the market with offerings focused on emerging technologies, but RSA's commitment to core authentication functionality ensures they will continue to be an industry leader.

ROADMAP FOR THE PRESENTATION

Current Market



Future
Investment



Vendor
Landscape



Product Rankings

CREATING OUR “BEST-IN-CLASS” PRODUCT RANKINGS

Phase 1

Utilizing qualitative and quantitative data, CEB TowerGroup identified 21 attributes that define a “Best-in-Class” Authentication solution, which are grouped into four categories.

Phase 2

Recognizing that all attributes are not equally important, CEB TowerGroup divides them into tiers to reflect their level of importance as mission critical, strong priority or differentiators.

Phase 3

Certain products are recognized as “Best-in-Class” after scoring each product based on its performance at an attribute level.

CATEGORIES		<p>Customer Engagement</p> <p>Those attributes that facilitate the authenticating customer’s comprehension of and successful interaction with the solution.</p>	<p>User Workflow Support</p> <p>Those attributes that administer credentials and authentication policies, as well as the ability to leverage these across channels.</p>	<p>Enterprise Operations</p> <p>Those attributes that address the solution diversity, technical implementation, and solution reporting for security and compliance roles.</p>	<p>Enterprise Support</p> <p>Those attributes that influence the enterprise’s tactical fit and strategic alignment with the vendor.</p>	
	ATTRIBUTES	Mission Critical	<ul style="list-style-type: none"> Initial Authentication User Interface 	<ul style="list-style-type: none"> Customer Support Risk Policy Workflow 	<ul style="list-style-type: none"> System Integration Authentication Methods 	<ul style="list-style-type: none"> Technology Innovation Compliance Strategy
		Strong Priority	<ul style="list-style-type: none"> Experience Consistency Customer Credential Management 	<ul style="list-style-type: none"> Customer Management 	<ul style="list-style-type: none"> Routing and Prioritization Solution Administration 	<ul style="list-style-type: none"> Product Maturity Vendor Stability
		Differentiator	<ul style="list-style-type: none"> Credential Recovery 	<ul style="list-style-type: none"> Data Security 	<ul style="list-style-type: none"> Synchronization Access History 	<ul style="list-style-type: none"> Deployment Flexibility Pricing Flexibility
		<p>“Best-in-Class” Customer Engagement</p>	<p>“Best-in-Class” User Workflow Support</p>	<p>“Best-in-Class” Enterprise Operations</p>	<p>“Best-in-Class” Enterprise Support</p>	

› **Retail Banks should use the ranking matrix in combination with the Authentication Solution Anatomy to select the vendor that best aligns with their firm's needs.**

- Vendor rankings are based on our proprietary 5-point rating system for each of the 21 attributes in our Authentication Solution Anatomy (see page 20).

RANKING MATRIX

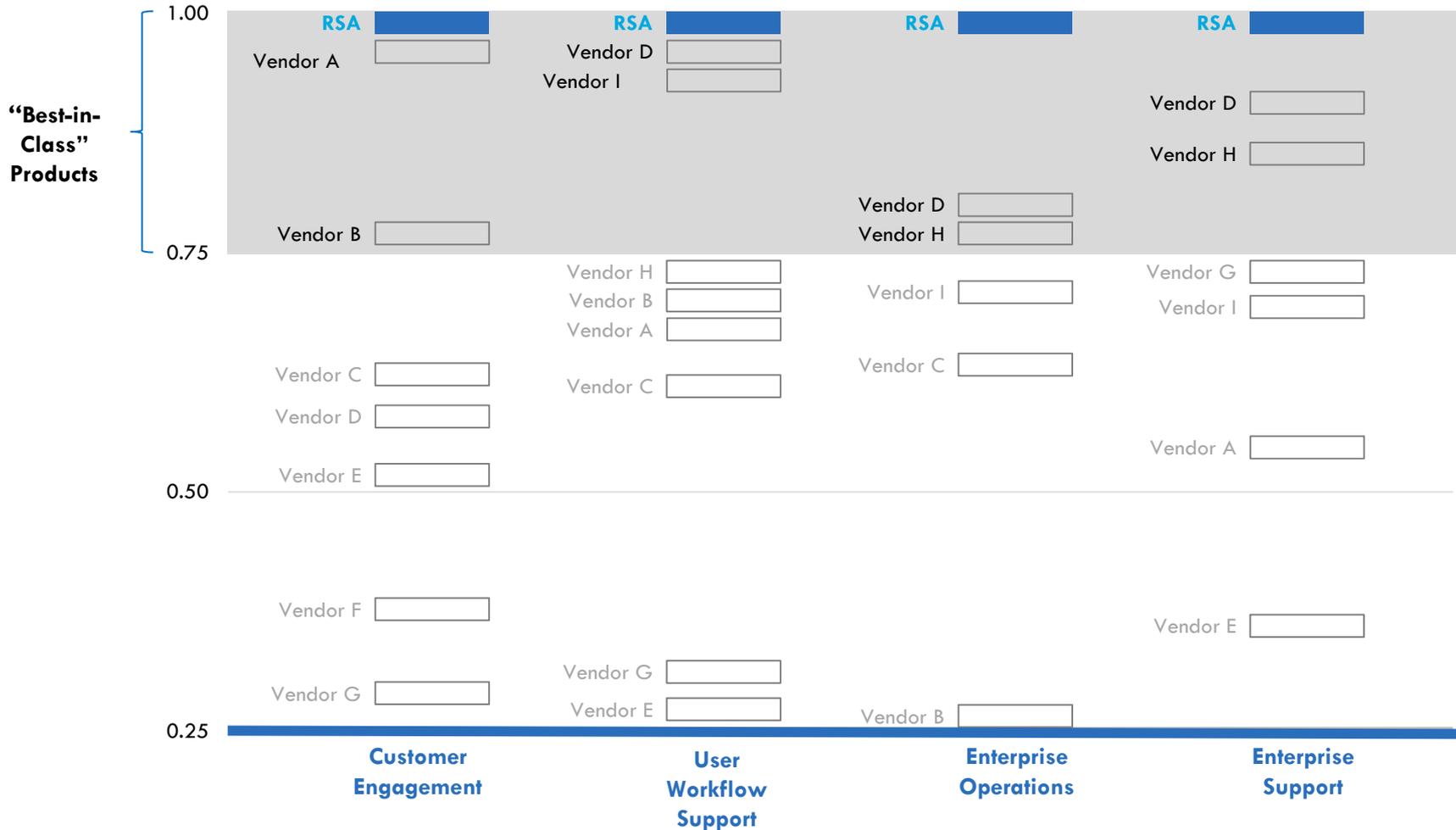
Listed Alphabetically by Vendor

 = Best-in-Class in Anatomy Category

Vendor	Product	Customer Engagement	User Workflow Support	Enterprise Operations	Enterprise Support
Vendor A	Product A	4.29	3.94	4.31	4.25
Vendor B	Product B	4.62	4.53	4.42	4.17
Vendor C	Product C	4.57	4.41	4.71	4.15
Vendor D	Product D	4.45	4.15	4.33	4.42
Vendor E	Product E	5	4.47	4.21	4.56
Vendor F	Product F	3.86	4.71	4.77	4.67
RSA	Authentication Services	5	4.71	5	4.90
Vendor G	Product G	4.19	4.18	4.38	4.73
Vendor H	Product H	4.52	4.71	4.79	4.83
Vendor I	Product I	4.10	4.56	4.78	4.79

MAPPING THE VENDOR LANDSCAPE

“Best-in-Class” Product Rankings
 Normalized Scores, 0.0-1.0 Scale



› **RSA Authentication Services received “Best-in-Class” in Customer Engagement, User Workflow Support, Enterprise Operations, and Enterprise Support.**

- Customer Engagement includes those attributes that facilitate the authenticating customer’s comprehension of and successful interaction with the solution.
- User Workflow Support includes those attributes that administer credentials and authentication policies, as well as the ability to leverage these across banking channels.
- Enterprise Operations includes those attributes that address the solution diversity, technical implementation, and solution reporting for security and compliance roles.
- Enterprise Support includes those attributes that influence the enterprise’s tactical fit and strategic alignment with the vendor.

CEB TOWERGROUP RETAIL BANKING AND CARDS PRACTICE

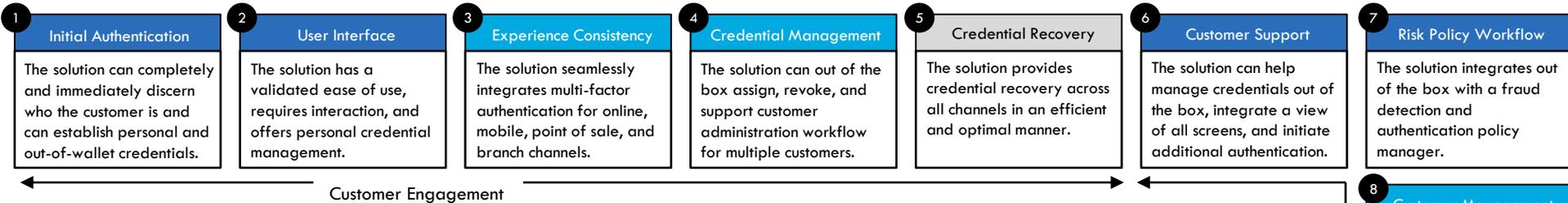
© 2012 The Corporate Executive Board Company. All Rights Reserved.

“BEST-IN-CLASS” ACHIEVEMENTS FOR RSA

Listed Alphabetically by Vendor

Vendor	Scoring Analysis
<i>Customer Engagement</i>	<ul style="list-style-type: none"> ▪ Initial Authentication: Using risk engine self-learning technology, RSA Authentication Services evaluate each online activity in real time and tracks over one hundred device and transaction attributes in order to authenticate a customer. ▪ Experience Consistency: RSA is consistent across all channels, so organizations can customize RSA Authentication Services and integrate the solutions into customer-facing interfaces through the RSA SecurID authentication engine.
<i>User Workflow Support</i>	<ul style="list-style-type: none"> ▪ Customer Management: RSA Authentication Services help to manage credentials out of the box and initiates additional authentication factors such as invisible authentication, out of band authentication, challenge questions, and site-to-user authentication. ▪ Customer Support: With a robust self-service portal called RSA Credential Manager, customers can report lost or unavailable tokens, report a forgotten PIN, or test a token. A customer may be granted emergency access to reset their PIN, which greatly reduces the number of calls and trouble tickets to the help desk and thereby increases efficiency. ▪ Data Security: Built upon the Advanced Encryption Standard (AES) algorithm, RSA Authentication Services have credentials that are strongly secured. The aggregated risk engine ensures that credentials are not personally identifiable.
<i>Enterprise Operations</i>	<ul style="list-style-type: none"> ▪ System Integration: RSA Authentication Services offer a sophisticated API structure that allows banks to customize integration out of the box with SSL-VPN products, a Configuration Wizard, web access management, and application delivery solutions. ▪ Solution Administration: Used as an auditing and accounting tool, RSA Authentication Services include report templates that can be easily tailored to administrative needs. For auditing purposes, administrators can define server events to capture to save time.
<i>Enterprise Support</i>	<ul style="list-style-type: none"> ▪ Vendor Stability: Founded in 1982 and acquired by EMC in 2006, RSA is a strong and stable vendor in the financial services industry that is now a publicly traded company on the NYSE. Constantly striving to expand its market, RSA acquired NetWitness Corporation, a provider of network security analysis solutions, in 2011 to add to its diverse portfolio. ▪ Technology Innovation: RSA recently added behavioral analysis to the risk engine analysis on its Authentication platform, and a new mobile channel protection module to cater to more mobile browsers.

AUTHENTICATION SOLUTION DIAGNOSTIC ANATOMY



Scoring Methodology

To arrive at a vendor ranking, CEB TowerGroup developed a proprietary scoring metric outlined by the attributes in this anatomy that highlights the major elements of an enterprise investment decision. This metric assumes that every element is not equally important, and therefore assigns a higher level of importance to those attributes critical to an authentication solution. The remaining attributes are then divided further into two tiers to reflect their level of importance, highlighted below.

Tier 1 Attributes – “Mission Critical”

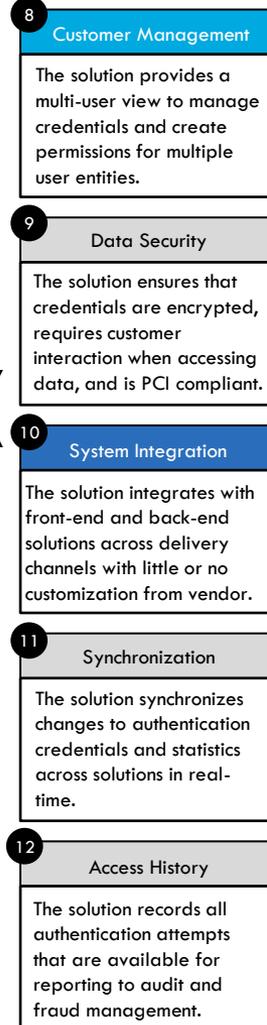
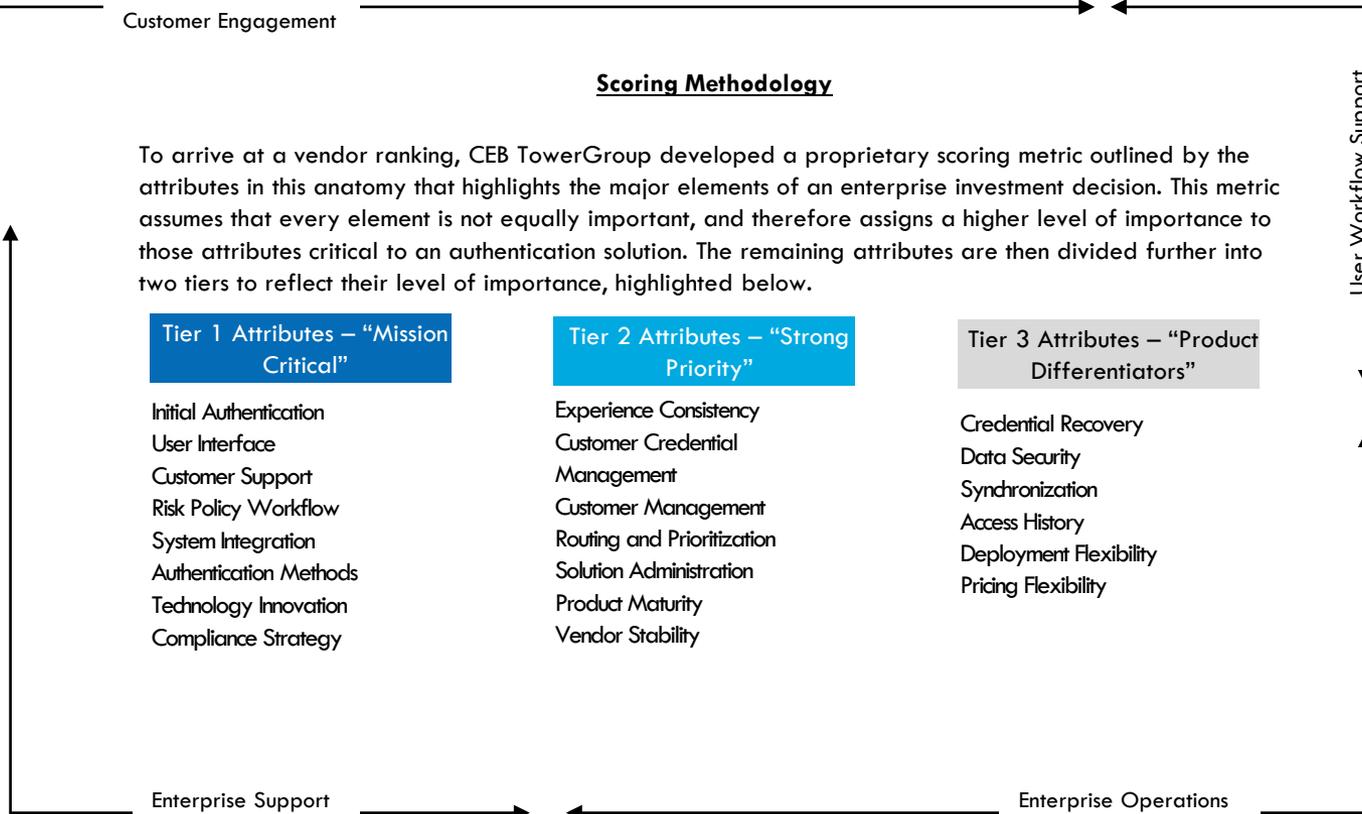
- Initial Authentication
- User Interface
- Customer Support
- Risk Policy Workflow
- System Integration
- Authentication Methods
- Technology Innovation
- Compliance Strategy

Tier 2 Attributes – “Strong Priority”

- Experience Consistency
- Customer Credential Management
- Customer Management
- Routing and Prioritization
- Solution Administration
- Product Maturity
- Vendor Stability

Tier 3 Attributes – “Product Differentiators”

- Credential Recovery
- Data Security
- Synchronization
- Access History
- Deployment Flexibility
- Pricing Flexibility



CEB TowerGroup developed a unique and proprietary scoring methodology that highlights the key priorities for an executive's investment decision.

- Every vendor product featured in this report is scored against each of the 21 attributes outlined in the Authentication Solution Diagnostic Anatomy on a standardized 1-5 scale.
- We calculate the weighted average of a product's attribute scores in each of the 4 categories of the anatomy to arrive at an overall category score.

UNDERSTANDING OUR SCORING METHODOLOGY

Sample Technology Analysis Internal Anatomy Scoring Guide

Illustrative

Anatomy		Category	Customer Engagement	Enterprise Operations
		Attribute Title	Initial Authentication	Authentication Methods
Attribute Definition			<i>The solution can completely and effectively discern who the customer is and can establish personal and out of wallet credentials that are immediately available online or through a mobile device.</i>	<i>The solution supports multiple factors of authentication on multiple out of band channels and devices.</i>
Scoring Metric	5		The solution can completely and effectively discern who the customer is and can establish personal and out of wallet credentials that are immediately available online or through a mobile device.	The solution supports multiple factors of authentication on multiple out of band channels and devices.
	4		The solution can establish credentials for multiple authentication factors through an immediately available single channel using internal KYC processes.	The solution supports more than one factor of authentication on multiple out of band channels.
	3		The solution can establish credentials for multiple authentication factors through a single channel but is not immediately available.	The solution supports one factor of authentication on multiple out of band channels and devices.
	2		The solution discerns identity by relying on personal information and access to multiple channels to complete enrollment.	The solution supports one factor on multiple channels.
	1		The solution discerns identity by relying solely on personal information provided during enrollment.	The solution supports one factor of authentication on one channel.
Attribute Score:			5.0	3.0

