



WHITE PAPER

---

# VeriSign® Identity Protection (VIP) Services

Five Business Strategies for Reducing the High Cost of Online Consumer Authentication





**CONTENTS**

+ Introduction	3
+ Strategy 1: Use improved security to differentiate your brand and build brand loyalty.	4
+ Strategy 2: Understand your customers' online usage and match security to the value of their transactions.	5
+ Strategy 3: Participate in a network that allows consumers to use a single credential across multiple sites or applications.	6
+ Strategy 4: Choose a solution that enables interoperability across customers, sites, and networks, regardless of hardware or software.	7
+ Strategy 5: Offload capital expenditures and operational costs to a trusted provider.	8
+ Glossary	9
+ Learn More	10
+ About VeriSign	10



**TWO-FACTOR AUTHENTICATION**

*Two-factor authentication is a process by which an organisation protects access to data by verifying the identity of the person attempting to access its resources—whether by Web site, phone, or other device. Two-factor authentication is stronger than user name/password authentication because it uses more than one method (or factor) to authenticate the user’s identity. It typically involves the combination of something a person knows, such as a user name/password or PIN (the first factor) with something a person has, such as a token, USB device, credit card, or mobile phone (the second factor). Frequently, this second factor generates one-time passwords (OTP), which are valid for only one use and must be entered upon signing on to the site or application.*

# Five Business Strategies for Reducing the High Cost of Online Consumer Authentication

Online services provide organisations with additional channels to generate revenue, strengthen branding, and meet customer demand for anytime, anywhere services. However, as online identity theft, fraud, and credit card data breaches become increasingly sophisticated, user names and passwords are insufficient to verify or authenticate users’ identity and protect high-value transactions. In this high-stakes environment, passwords are simply too easy to steal, guess, or lose. Industry regulators are already addressing this fact: The Federal Financial Institutions Examination Council (FFIEC), for example, has passed regulations mandating stronger forms of authentication to protect consumers.

To address risk and compliance issues, many organisations are deploying two-factor consumer authentication solutions. These solutions require significant investment in planning, deploying, managing, and maintaining not only the authentication infrastructure, but also the second-factor authentication credentials. Adding to the challenge is the requirement to provide two-factor authentication across multiple delivery channels (e.g., computers, mobile phones, and television) and to an extremely diverse user population.

In deploying a two-factor consumer authentication solution, organisations must continually balance cost, complexity, risk, and user convenience. The following strategies address these considerations while helping reduce the high cost of two-factor authentication.

## Five Strategies for Reducing Two-Factor Authentication Costs

Strategy	Strategy Benefits
<b>Use improved security to differentiate your brand and build brand loyalty.</b>	<ul style="list-style-type: none"> <li>+ Helps attract new customers and strengthen existing relationships.</li> <li>+ Reduces customer churn.</li> <li>+ Helps reduce paper-based costs and enables reallocation of personnel to core business functions by encouraging online usage.</li> </ul>
<b>Understand your customers’ online usage and match security to the value of their transactions.</b>	<ul style="list-style-type: none"> <li>+ Reduces the number of applications requiring two-factor authentication.</li> </ul>
<b>Participate in a network that allows consumers to use a single credential across multiple sites or applications.</b>	<ul style="list-style-type: none"> <li>+ Makes two-factor authentication more accessible, thereby driving mass adoption.</li> <li>+ Simplifies the user experience.</li> <li>+ Helps minimise deployment costs.</li> </ul>
<b>Choose a solution that enables interoperability across customers, sites, and networks, regardless of hardware or software.</b>	<ul style="list-style-type: none"> <li>+ Helps lower purchase and integration costs.</li> <li>+ Provides freedom to create best-of-breed solutions (vs. being locked in to a proprietary solution).</li> <li>+ Increases credential choices for consumers and distribution options for organisations.</li> </ul>
<b>Offload capital expenditures and operational costs to a trusted provider.</b>	<ul style="list-style-type: none"> <li>+ Helps reduce upfront capital expenditures.</li> <li>+ Helps reduce operational costs and total cost of ownership.</li> <li>+ Accelerates time to market.</li> <li>+ Provides better reliability and scalability.</li> </ul>



According to a 2006 survey,<sup>1</sup> 33% of U.S. consumers and 39% of European consumers consider information security when selecting a brand, and 25% will go elsewhere if they perceive a threat to their personal information.

**+ Strategy 1: use improved security to differentiate your brand and build brand loyalty.**

This strategy helps attract new customers and strengthen relationships with existing customers. At the same time, it encourages online usage of low-cost, high-margin services, rather than more costly face-to-face interactions.

Brand trust and loyalty are critical to a company's success, and organisations devote large portions of their budget to build and support their brand. Organisations recognise that brand equity and business opportunities can crumble instantly as a result of negative publicity associated with a privacy breach or data theft. While improved security helps prevent brand corrosion, it can also be used to enhance brand loyalty and reduce churn.

Organisations can differentiate their brand, demonstrate respect for customers, and give customers peace of mind by using security mechanisms that help create a user-friendly, trusted, and safe online experience. They can also distribute branded security credentials (e.g., security tokens) that subtly reinforce the brand with every use. Finally, organisations can establish trust and strengthen their online identity (especially in the case of less-well known organisations or new entrants to online business) by using security credentials and security branding from a trusted provider of security.

<sup>1</sup> *Secure the Trust of Your Brand: Assessing the Security Mindset of Consumers*, conducted by the CMO Council and Opinion Research, as reported in ClickZ, [http://www.clickz.com/showPage.html?page=clickz\\_print&id=3623088](http://www.clickz.com/showPage.html?page=clickz_print&id=3623088)

**USING ONLINE SERVICES TO REDUCE COSTS AND GO GREEN**

*In many cases, the one-time cost of developing online applications and deploying two-factor authentication is less than the ongoing cost and complexity of manually performing paper-based tasks or providing in-person customer service. Online services may also help organisations meet environmental goals related to paper usage and disposal. Some sources even indicate that online, or “green”, transactions help fight fraud. In one report, “paper” customers detect fraud after an average of 114 days, while “green” customers detect fraud after an average of 18 days.<sup>2</sup>*

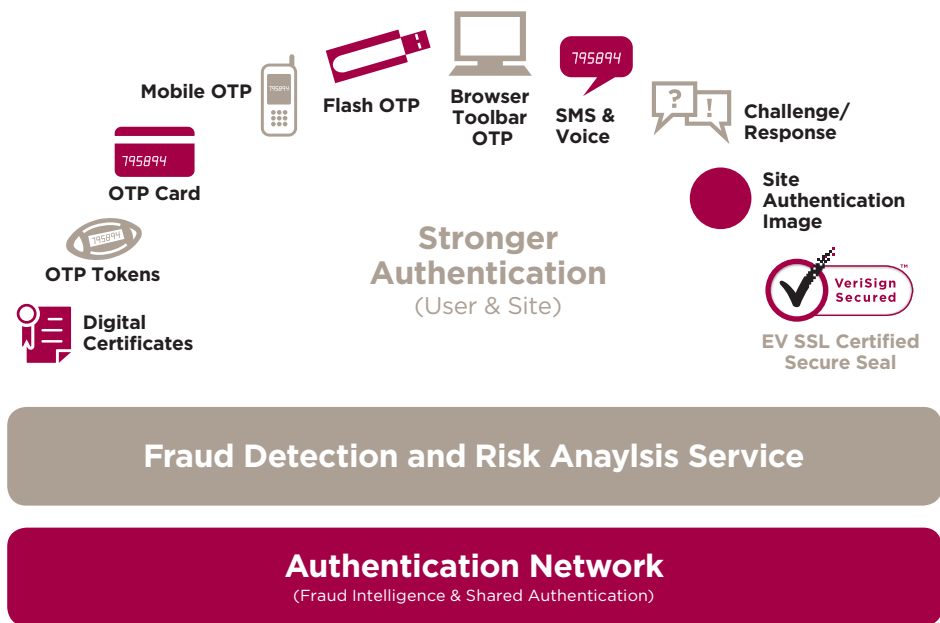
**+ Strategy 2: Understand your customers’ online usage and match security to the value of their transactions.**

This strategy optimises the allocation of security resources and helps reduce costs by eliminating expenditures on security mechanisms and credentials that are stronger than necessary.

One authentication scenario does not fit all customers. By understanding the value of transactions conducted by a particular customer or on a specific online application, organisations can use a layered approach to security. With this approach, organisations can selectively apply graduated levels of security to match specific customers’ usage. Doing so helps reduce costs by limiting two-factor authentication to those users who truly require it. For example, Secure Sockets Layer (SSL) encryption or user ID/password authentication costs less and may be sufficient for some types of online interactions (e.g., low-dollar online purchases), while high-value transactions (e.g., regular transfers of thousands of dollars between institutions) would require two-factor authentication.

The key is to work with a vendor that offers a range of complementary security mechanisms to meet diverse needs, and importantly, one that has the expertise to help implement customer-appropriate security policies and mechanisms. Then, once authentication architecture is in place, its cost can be distributed appropriately across all the applications, services, or business centers that it supports.

**Complete Solution for Consumer Authentication**



<sup>2</sup> Javelin Strategy and Research, *Paper Statements: Expensive and Less Secure*, October 26, 2005

## SHARED VALIDATION FOR CONSUMERS

*Today's consumer has the burden of remembering dozens of passwords and carrying multiple authentication credentials in order to conduct business online. Shared validation addresses this problem by giving customers a single authentication credential that can be used for multiple channels, organisations, or sites—similar to credentials used in ATM networks.*

### + Strategy 3: Participate in a network that allows consumers to use a single credential across multiple sites or applications.

This strategy helps minimise deployment costs, simplifies the user experience, and creates new partnership opportunities. It also drives general adoption of two-factor authentication by making it more accessible to more organisations and customers, similar to the way ATM usage was enhanced when banking customers could use their bank's ATM card on any other participating network.

In this scenario, multiple organisations share a single, third-party infrastructure for authenticating user credentials. Because all organisations on the network use the same authentication infrastructure, a customer can use the same authentication credential with every organisation on the network. This approach, called “shared validation”, not only simplifies the user experience, but also allows organisations to offer two-factor authentication without investing in authentication infrastructure or even having to distribute or manage credentials. In addition, organisations can partner authentication infrastructure or even having to distribute or manage credentials. In addition, organisations can partner with other organisations on the network to create new business and marketing strategies (for example, by accepting another organisation's credential on a site in exchange for advertising discounts).

To enable two-factor authentication, organisations simply insert vendor-provided code (called a Web services application programming interface, or, API) to enable communication with the third-party vendor's authentication infrastructure. (Organisations maintain full control over customer information and security policies.)

Then, depending on budget and business goals, organisations have the following options for enabling credential usage on their site:

- **Accept credentials issued by network members:** This is the easiest, most cost-effective approach to shared validation and enabling two-factor authentication. In this scenario, the organisation does not distribute or manage its own authentication credentials. Instead, customers use a credential obtained from another organisation on the network (see next paragraph) or a third-party. The customer can use this credential on any site in the network.
- **Issue credentials directly:** In this case, an organisation directly provides customers with branded authentication credentials such as tokens for its site. It may also distribute branded credentials to designated customers of other organisations on the network. In doing so, organisations not only extend brand reach, but also collect a rebate every time a person uses the credential on another site. Relying parties can scale up to become issuers as their circumstances change.



**SHARED VALIDATION FOR CONSUMERS**

According to its Web site, OATH is “an industry-wide collaboration to develop an open reference architecture by leveraging existing open standards for the universal adoption of strong authentication.” Many organisations are adopting OATH architectures in order to advance the drive for universal, open standards-based authentication.

**+ Strategy 4: Choose a solution that enables interoperability across customers, sites, and networks, regardless of hardware or software.**

This strategy helps to lower costs, increase deployment options, and enable shared validation.

Like everything else in the technology world, two-factor authentication infrastructures are based on a set of standards for design, operation, and interaction. If an organisation uses an authentication solution that is based on proprietary (closed) standards, it is restricted to interacting only with other networks, sites, and customers that use the same proprietary hardware, software, and credentials as it uses (i.e., from a single vendor). Typically, proprietary solutions are more costly and less flexible than other solutions.

When organisations use a solution based on open standards (see the OATH sidebar), they are not locked in to a narrow solution that requires proprietary components.

**Open Authentication Solutions vs. Closed Solutions**

Authentication Capability	Open Authentication Solution	Closed/Proprietary Solution
Organisations can participate in an extended network of organisations and customers (shared validation).	✓	
Customers can use any non-proprietary authentication device, including tokens, USB devices, credit cards, or Short Message Service (SMS) text messages.	✓	
Organisations can distribute a range of non-proprietary credential types, providing higher-cost credentials only to customers who truly need them.	✓	
Organisations can rely on other organisations to issue and manage credentials.	✓	
Organisations that first use credentials issued by other organisations can scale up to become credential issuers, and still use original credentials/devices for existing customers.	✓	
Credential issuers can use non-proprietary software and hardware to provision and manage credentials.	✓	
Organisations can more easily enable credential use across many network end-points (e.g., desktop computers, laptops, Wi-Fi access points, and set top boxes).	✓	



**+ Strategy 5: Offload capital expenditures and operational costs to a trusted provider.**

This strategy entails outsourcing consumer authentication to a third party in order to minimise or eliminate the time, cost, and complexity associated with not only planning, implementing, maintaining, staffing, and managing an in-house consumer authentication infrastructure, but also distributing and managing authentication credentials.

By outsourcing these tasks to a qualified managed services provider, organisations can minimise or eliminate up-front capital investment in authentication infrastructure as well as total cost of ownership (e.g., ongoing IT staffing and training, maintenance, and upgrades). A well-established provider can handle credential shipping and distribution and offer a variety of credential models (e.g., relying party, issuer, branded issuer). This approach enables organisations to choose the best model for their budget and business goals. In addition, organisations can begin to offer high-value online services more quickly, enabling faster return on investment in these services and more immediate response to customer demands. Finally, a managed service provider, whose core business and expertise is network security, can often provide greater scalability, reliability, and sustainability than a lone company. These capabilities help ensure that the organisation can add online services as needed, meet customer demand for 24/7 availability, and maintain and upgrade the solution to keep up with industry innovation and developments over time.

**Managed Authentication Solution vs. In-House Solution**

Two-Factor Authentication Requirement	Managed Service	In-House Solution
Deploy authentication servers and other infrastructure.		✓
Install authentication software.		✓
Distribute and manage authentication credentials.		✓
Perform ongoing maintenance, management, and upgrades.		✓
Make upfront capital investment.		✓



## + Glossary

**Application Programming Interface (API)** – Programming language that enables communication between different applications or servers.

**Authentication** – The process of confirming that something is genuine. In computer security, authentication is usually an automated process of verifying the identity of someone or something, such as a computer or application.

**Credential** – Proof of qualification, competence, or clearance that is attached to a person. A digital certificate, token, smart card, mobile phone, or installed software are credentials that may be used to enable strong- or multi-factor authentication.

**Device** – A hardware token, USB device, mobile phone, or laptop that contains a one-time password (OTP), digital certificate, or some other credential used for authentication.

**Initiative for Open AuTHentication (OATH)** – An industry-wide collaboration to develop an open reference architecture for the universal adoption of strong authentication.

**One-time password (OTP)** – A unique security code generated through a validation network by a hardware or software credential; often used as a second factor for strong authentication.

**Shared validation** – An approach to consumer authentication in which multiple organisations share a single, third-party infrastructure for authenticating credentials, thereby enabling a customer to use the same authentication credential with every organisation on the network. This approach allows organisations to offer two-factor authentication without requiring an investment in authentication infrastructure, or distribution and management of credentials.

**Token** – A physical device used to authenticate a user for access to authorised computer services. Also called a security token, hardware token, authentication token, or cryptographic token.

**Trusted provider** – A third-party organisation capable of enabling two-factor authentication across many client sites without companies having to invest time and resources in building individual solutions for each site. With a secure and trusted provider maintaining the system, companies can easily and cost-effectively scale to a larger number of sites or users as their business grows.

**Two-factor authentication (2FA)** – The authentication practice of requiring confirmation of something you know such as a user name and password with something you have such as a smart card, token or certificate. Also called strong authentication or multi-factor authentication.



**+ Learn More**

For more information about strategies to reduce the cost of consumer authentication, or to find out about VeriSign solutions for consumer authentication, please visit <http://www.verisign.com.sg/authentication/consumer-authentication/>

**+ About VeriSign**

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

**Visit us at [www.Verisign.com.sg](http://www.Verisign.com.sg) for more information.**

©2008 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the Checkmark Circle logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc., and its subsidiaries in the United States and foreign countries. All other trademarks are property of their respective owners.

00025861 5-6-2008