



WHITE PAPER

---

# Multilayer Security: Enabling a Sustainable Alternative to Paper-Based Customer Communications



**CONTENTS**

+ Introduction	3
+ The Opportunity for Innovative Paperless Offerings	3
Green Financial Services	3
E-Retail	4
Paperless Medicine	4
+ Are Consumers Ready to Forego Paper?	4
+ Multilayer Security—The Enabler for a Successful Paperless Strategy	4
Authenticating the Website: SSL Certificates	5
Protecting the Transaction: SSL Encryption	5
Protecting Consumer Identity: Two-Factor Authentication	5
Protecting Against Fraud: Fraud Detection	6
Bringing it all Together	6
+ Secure, Paperless Communications are a Win-Win-Win	6
+ Conclusion	7
+ Glossary	8
+ Learn More	8
+ About VeriSign	8



# Multilayer Security: Enabling a Sustainable Alternative to Paper-Based Customer Communications

## + Introduction

Companies of every ilk stand to potentially save millions by moving the bulk of their paper-based communications with customers online. For instance, one recent article estimated that a major bank could save \$100 million or more in annual savings if every customer chose electronic statements.<sup>1</sup>

However, consumer concerns about online security can create a barrier to realizing the savings—both hard costs of paper, printing, and postage as well as the reduced environmental impact. A new green banking study by Javelin Strategy & Research highlights the issue. Its findings show that 3 out of 4 consumers still opt to receive paper statements instead of electronic ones.<sup>2</sup> In healthcare, despite heavy consumer interest, privacy concerns plague initiatives such as online medical records.<sup>3</sup>

To achieve any significant reduction in cost and environmental impact, organizations must address the threat of cyber fraud in a way that is immediately conspicuous to customers as meeting a higher standard of security. To ensure the continuum of protection consumers and the companies they do business with need, organizations must address consumer identity protection, confidential data protection, Website authentication, and fraud detection.

A multilayer security approach delivers the end-to-end solution needed to comprehensively target these security issues. By layering technology such as Secure Sockets Layer (SSL) certificates, two-factor authentication, and fraud detection, companies can protect the customer, the transaction, and the business. Companies adopting this layered approach are primed to gain greater customer loyalty, increase the variety of transactions, and attract new customers, while supporting sustainability, improving security, and reaping cost savings.

## + The Opportunity for Innovative Paperless Offerings

U.S. businesses spent \$800 billion on direct mail correspondence to potential and existing customers in 2006.<sup>4</sup> The opportunity to drastically reduce these costs is at hand. Companies across industries are finding innovative ways to eliminate paper—from electronic statements to e-tickets, from PDF receipts to online health records.

### Green Financial Services

Banks, insurance companies, brokerages, and others within the financial services industry stand to reap dramatic savings by moving consumers to electronic communications. In addition to electronic statements where paper-based costs of \$1 to \$2 per customer per month can be eliminated, online applications are another area of savings. Aite Group

<sup>1</sup> "Chase Bank's \$25,000 Sweeps for Going Paperless," Jim Breune, *Netbanker*, February 14, 2007

<sup>2</sup> "The Four E's of Green Banking: Educate, Enable, Make it Easy—and Be Earnest," Javelin Strategy & Research, June 2, 2008

<sup>3</sup> "Online Health Records Raise Privacy Concerns," Kathleen Kerr, *Newsday*, March 3, 2008

<sup>4</sup> "Follow the Paperless Trail," Ted Samson, *InfoWorld*, September 06, 2007

*Sixty-one percent of adult Americans said they were very or extremely concerned about the privacy of personal information when buying online, an increase from 47 percent in 2006.*

—“Consumer Fraud and Identity Theft Complaint Data, January-December 2007,” *The Federal Trade Commission, February 13, 2008*

estimates that for every new account opened online and not through another venue, financial service providers could save \$50.<sup>5</sup> With millions of applications for all forms of financial products made online each month, the potential savings are impressive.

#### E-Retail

Even brick-and-mortar retailers are devising unique ways to save paper while enhancing customer service. For instance, at Apple stores, customers can opt to have their receipt sent to them via e-mail instead of having it issued in paper form on the spot.<sup>6</sup> This and other strategies such as paperless coupons can optimize customer touch points while saving paper costs.

#### Paperless Medicine

Healthcare is traditionally one of the more paper-intensive industries, with enormous volumes of file folders, medical charts, X-rays, lab results, and other documents. Electronic records can reduce errors, cut administrative costs, and save time. With a legal right to inspect their medical records, consumers could gain easier access to their complete records through online means. A Harris Interactive survey showed that 91% of consumers want access to their electronic medical records (EMRs).<sup>7</sup>

The above examples represent only a small fraction of all the potential areas where paperless alternatives can deliver significant savings while improving customer service and satisfaction. Other sectors such as transportation, hospitality, government, and more are forging ahead with equally creative and compelling paperless offerings.

### + Are Consumers Ready to Forego Paper?

The question is, are consumers ready for paperless? Customer adoption of paperless initiatives is the ultimate linchpin to realizing the magnitude of savings possible—and support for larger green initiatives. To the dismay of many company strategists, adoption rates have not yet met expectations and often plateau at a disappointing level. For example, in a 2008 IBT Market Pulse Survey, 90 percent of the bankers surveyed have implemented paperless options such as online applications and electronic statements. But just 16 percent report that a majority of their customers participate in the programs.<sup>8</sup>

Yet studies show that consumers are increasingly interested in the convenience and ecological benefits of going paperless. Why is interest high but actual participation low? The answer is fear—the fear of identity theft, fraud, and monetary losses.

This fear, rooted in media reports of identity theft and cyber fraud, keeps many consumers clinging to what they consider to be a safer alternative: paper. And despite the fact that reports show that most data is compromised through offline channels not via the Internet,<sup>9</sup> consumers continue to be wary of receiving their confidential information electronically.

### + Multilayer Security—The Enabler for a Successful Paperless Strategy

How can companies assure consumers that it's safe to communicate confidential information online? By introducing an end-to-end security environment that addresses

<sup>5</sup> “Online Banking Paying Off,” Mike Sachoff, *WebProNews*, June 1, 2007

<sup>6</sup> “Follow the Paperless Trail,” Ted Samson, *InfoWorld*, September 06, 2007

<sup>7</sup> “Benefits of Electronic Health Records Seen as Outweighing Privacy Risks,” Beckey Bright, *The Wall Street Journal*, November 29, 2007

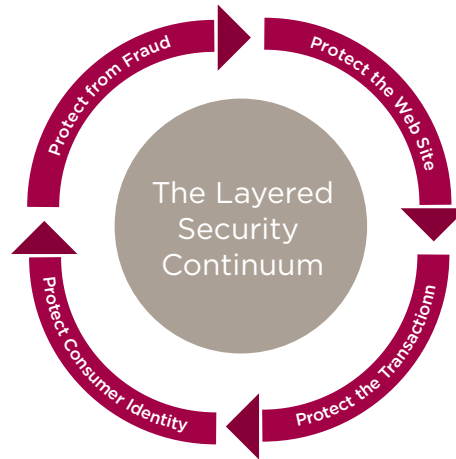
<sup>8</sup> “Green Banking: Reality or Hype?” Paula Damiano, *Bank Systems & Technology*, May 14, 2008

<sup>9</sup> “New Research Shows Identity Fraud is Contained and Consumers Have More Control than they Think,” The Council of Better Business Bureaus and Javelin Strategy & Research, January 31, 2006

the true end-to-end online security problem. While proven point products can be effective, no single security measure is foolproof. What’s needed is a multilayer security solution that delivers a more secure customer experience by protecting against fraud and theft at multiple levels.

Smart companies are actively pursuing and promoting to their customers a continuum of new and extended security technologies that provide the end-to-end, trusted foundation for paperless customer communications. These organizations are putting leading-edge solutions into place around four areas essential to ensuring the safety of consumers’ online communications: authenticating the Web site, protecting the transaction, protecting the consumer’s identity, and fraud detection/protection.

Figure 1: The Layered Security Continuum



#### Authenticating the Website: SSL Certificates

The Secure Sockets Layer (SSL) certificate enables the consumer to verify the identity of the certificate owner and ensure that the Website is indeed authentic and not a phishing scam. Many consumers are aware that the “https” in their browser’s address bar indicates that the site has authenticated itself with an SSL certificate. However, the lock icon and the https address alone do not indicate who issued the SSL Certificate or whether the certificate is trustworthy. More advanced SSL certificates provide additional cues that help to extend trust online, such as turning the address bar green or displaying the name of the certificate owner.

#### Protecting the Transaction: SSL Encryption

SSL technology establishes a private communication channel where data can be encrypted during online transmission, protecting sensitive information from electronic eavesdropping. Most Internet users are familiar with the tiny lock icon that appears on pages that have been encrypted by SSL. Companies should look to use [Server-Gated Cryptography \(SGC\)-enabled SSL certificates](#) that support 128- or 256-bit SSL encryption (depending on the Web browser, operating system, and host server.) Both the strong 128-bit encryption and the stronger 256-bit encryption offer levels of protection to Web site visitors that are trillions times stronger than 40-bit encryption. SGC certificates are the only SSL certificates that enable every client system to benefit from the strongest encryption it is capable of achieving.

### Protecting Consumer Identity: Two-Factor Authentication

**Two-factor authentication (2FA)** relies on two different factors to authenticate consumer identity. Using more than one factor is also known as strong authentication and can ensure a significantly more secure experience for consumers. A criminal who steals only the first factor will not be able to forge the second factor and will be unable to authenticate. And vice versa, anyone stealing the second factor will not know the first and will be likewise unsuccessful. Two-factor authentication solutions can take the form of point-to-point products where consumers use a different credential for each Website they visit or a shared authentication network where consumers use the same credential across multiple sites.

Compared to a standalone 2FA solution, a **shared authentication network** delivers an extremely user-friendly and effective method of two-factor authorization that encourages and rewards consumer adoption. It enables 2FA to be both easy to use (regardless of the consumer's level of technology sophistication) and convenient, allowing the consumer to use the same credential across participating sites.

### Protecting Against Fraud: Fraud Detection

While SSL and 2FA are proactive and visible forms of security, fraud detection is invisible to the consumer. **Fraud detection** technology works behind the scenes to detect anomalies that could signal potential fraud. It “learns” how each user behaves and only becomes visible to the user when additional authentication is needed based on pre-determined parameters.

### Bringing it all Together

SSL authenticates the business to the consumer—consumers can validate visually that they are visiting a trusted and authentic site before they enter their personal information. Two-factor authentication and fraud detection authenticate the consumer to the business with strong authentication and fraud prevention. Deploying these complementary technologies in tandem ensures the highest level of security and confidence—key to enabling more consumers to switch to paperless online alternatives.

With a layered approach to online security, companies can promote and demonstrate that they offer a highly secure, electronic alternative to paper for their customers. By helping eliminate the concern about privacy and security, companies clear the way for consumers to embrace the full benefits of online communications and drive adoption rates to new levels.

### + Secure, Paperless Communications are a Win-Win-Win

The impact of encouraging increasing numbers of customers to switch from paper to electronic communications can be enormous. For companies, the cost savings alone justifies the effort to bolster security with a layered approach. Organizations stand to save hundreds of thousands or millions of dollars each year in reduced paper, printing, and postage costs.

At the same time, fraud costs can also be reduced, as customers receiving electronic communications can spot fraud more quickly than waiting for the mail, enabling the company to react before more losses can accumulate. One study shows that customers receiving paper detect fraud after an average of 114 days, compared to online customers who detect fraud after an average of 18 days. This is reflected in average fraud losses, with \$4,543 for paper users and a much lower \$551 for their “green” counterparts.<sup>10</sup>

<sup>10</sup> “Banking Strategies,” Javelin Research, October 2005

<sup>11</sup> “Online Bill Payment Drives Share of Wallet, Loyalty for Banks,” *Payments News*, April 2007



Customer satisfaction and competitive differentiation also get a boost. Studies show that the more bills paid through a bank's site, the higher the satisfaction from customers.<sup>11</sup> In a study by Javelin, forty-three percent of consumers said they are more likely to do business with companies they perceive to be green.<sup>12</sup> At the same time they are helping to reduce the impact on the environment, consumers gain other benefits as well: convenience, greater security, anytime access, and time savings.

And both companies and consumers can feel good about reducing the impact on the environment. According to PayItGreen, if 20 percent of households (22,876,800 households) were to switch to electronic bills, statements, and payments, every year the collective impact would:<sup>13</sup>

- Save 150,939,615 pounds of paper
- Save 1,811,275 trees
- Avoid filling 8,597,328 household garbage bags with waste
- Avoid filling 6,141 garbage trucks with waste
- Avoid using 102,945,600 gallons of gasoline to mail bills, statements, and payments
- Avoid producing 3,920,802,916 pounds (1,960,402 tons) of greenhouse gas emissions

Finally, paperless communications supported by multilayer security can contribute to larger sustainability initiatives, enabling companies to more thoroughly address applicable regulatory and good citizenship issues.

#### + Conclusion

The opportunity is enormous for companies that can move far greater numbers of customers to paperless alternatives. These savvy organizations create a distinct advantage from both a cost perspective and the perception of customers that the company is committed to acting in an ecologically responsible way.

Enterprises that embrace multilayer security for paperless communications build the foundation of trust consumers need to break the paper habit. These forward-thinking companies are not only driving significant improvement to their own bottom line, but shaping the future of online transactions with secure, innovative services.

12 "The Four E's of Green Banking: Educate, Enable, Make it Easy — and Be Earnest," Javelin Strategy & Research, June 2, 2008

13 Project Performance Corp for the PayItGreen Alliance, [www.payitgreen.org](http://www.payitgreen.org), 2008



## + Glossary

**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.

**2-Factor Authentication, Strong Authentication, Multi-Factor Authentication** – All of these terms refer to the authentication practice of requiring confirmation of something you know such as a username and password and something you have such as a smart card, token or certificate.

**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.

**Extended Validation SSL** – Requires a high standard for verification of SSL Certificates dictated by a third party, the CA/Browser Forum. In Microsoft® Internet Explorer 7, Web sites secured with Extended Validation SSL Certificates cause the URL address bar to turn green.

## + Learn More

For more information about VeriSign® layered security solutions for paperless customer communications, please call 650-426-5310 or email: [identityandauthenticationservices@verisign.com](mailto:identityandauthenticationservices@verisign.com)

## + 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](http://www.Verisign.com) for more information.**