



## FRAUD PREVENTION: A VERISIGN GUIDE

FRAUD PREVENTION  
What Every Merchant Should  
Know about Internet Fraud





**CONTENTS**

+ Introduction	2
+ Why Every Merchant Should Be Concerned about Internet Fraud	4
+ Liability for Internet Fraud	5
+ Internet Fraud: What It Is and How It Happens	6
+ Stolen Consumer Identities	6
+ Stolen Merchant Identities	7
+ Access to Payment Networks	7
+ Who Is at Risk for Online Fraud	8
+ Fraud Risk Matrix	8
+ What Banks and Card Associations Are Doing to Prevent Online Credit Card Fraud	9
+ Protecting Your Business against Fraud	9
+ Transaction Level	10
+ Account Level	11
+ Network Level	11
+ Let Customers Know That Your Store Is Safe for Purchases	12





## FRAUD PREVENTION: A VERISIGN GUIDE



### CONTENTS

- + Save Time and Money While Protecting Your Business with VeriSign Fraud Protection Services 12
- + Fraud Protection Services—Purchase Options 13
- + Detailed Service Descriptions 13
- + VeriSign Fraud Protection Services Upgrade Options 16
- + What You Need to Get Started 16



Where it all comes together.™

## Introduction

---

e-Commerce is booming and has become an essential sales channel for businesses both domestically and internationally. The profitability and reach of an online business is hard to beat in the offline world. And offline businesses that don't have an online presence are at a serious competitive disadvantage. Unfortunately, e-commerce has also become an attractive revenue source for criminals who perpetrate Internet fraud. As an Internet merchant, you need to be aware and informed so that you can take steps to protect your business. Online payments security and fraud prevention is everyone's responsibility.

VeriSign® has put together the following guide to help you better understand fraud and what you can do to prevent it. This guide covers the following topics:

- Why every merchant should be concerned about Internet fraud
- Liability for Internet fraud
- Internet fraud; what it is and how it happens
- Who is at risk for online fraud
- What banks and credit card associations are doing to prevent online credit card fraud
- Protecting your business against fraud
- Let customers know that your store is safe for purchases
- Save time and money while protecting your business with VeriSign Fraud Protection Services

## Why Every Merchant Should Be Concerned about Internet Fraud

---

It's simple, a single fraud incident can put a merchant out of business. And every merchant is at risk for fraud. So it just makes good business sense to be aware and informed of your exposure and what you should do to protect your business.

As a merchant doing business online, you should be particularly concerned about fraud. Internet fraud is more prevalent than "brick-and-mortar" fraud and much more difficult to detect. Offline merchants can see who they are doing business with, look at their credit card, and watch them sign the receipt. In the online world however, customers are virtual and never sign a paper receipt, so authentication becomes a challenge. Moreover, in the online world, hackers can break into your network without you being aware of it to steal money, products, and sensitive information. They can also break into your network to steal customer identities and commit crimes against other merchants, using your business as a launch pad for further crimes.

Moreover, it's easier for a criminal to "break-in" to an online store than an offline store, and much easier for them to break in undetected. In the online world, criminals have multiple access points for break-ins, because the merchant store is networked internally

### *Internet Fraud Is a Significant Problem:*

- One in six consumers has been the victim of credit card fraud
- One in 12 consumers has had their identity stolen

and networked to other businesses. A criminal who breaks into a physical store is also much more visible and easy to detect than criminals who break in through the Web and erase their footprints.

Because of this, online transaction fraud is 17 times higher than in-store fraud, according to Gartner Group estimates. Fraudulent transactions make up 1.06 percent of total online transactions versus only 0.06 percent of offline transactions. And these figures don't include the cost of additional labor and fees associated with fraud investigations and merchant fines. The problem impacts consumers as well: one in six online consumers has been the victim of credit card fraud, one in 12 has had their identity stolen.

Perhaps the most disturbing facet of fraud is its high growth rate. As system complexity increases and technology advances, criminals have better access to more merchant goods and merchant cash. In 2002, the FBI reported Internet fraud complaints had tripled from the year before.

The threat of online fraud is so pervasive that the government has begun mandating security requirements for businesses that handle financial information online. Today these regulations apply mainly to the banking community, but, as an Internet merchant, you access the financial networks for each transaction made on your site. Because of this, security at the point of sale is becoming an increasing concern for both credit card associations and the government.

Security must therefore be a key merchant concern, and running efficient security operations that don't impact your bottom line is essential.

## Liability for Internet Fraud

---

In the offline world, you can take steps to safeguard your transactions by getting a signature and authorization—thereby shifting the liability of the transaction to the card issuer. In the online world, the liability for a fraudulent transaction always rests squarely with you, the merchant. Online transactions are considered “card not present” transactions and are inherently riskier. The financial implications for a merchant who processes a fraudulent online transaction can be significant:

- Inventory loss and shipping costs for physical goods that are fraudulently purchased and delivered.
- Chargeback penalties assessed by the acquiring bank of \$15-\$30 per fraudulent transaction.

But the economic impact to your business doesn't stop with liability for fraudulent purchases. Due to the greater risk of online purchases, merchant acquirers assess discount rates for online transactions that are typically 30 percent to 60 percent higher than offline or brick-and-mortar rates. In addition, according to Gartner Group estimates, merchants reject an estimated five percent of all transactions out of suspicion of fraud, while only two percent of transactions are actually fraudulent. The result is a significant amount of lost sales (up to three percent of sales volume) in an attempt to reduce fraud risk. In worst case scenarios, the credit card associations have even begun assessing six figure penalties for hacked merchant sites known to be a source of Web crime.

*A single fraud incident can put a merchant out of business*

In addition to losing product and paying chargeback penalties, your business also faces these additional costs due to fraud:

- Higher discount rates assessed as a result of processing fraudulent payments.
- Labor cost for the merchant to investigate and resolve the chargeback.
- Five- to six-figure card association fines or cancellation of a merchant's account when card fraud rates are consistently high.

## Internet Fraud: What It Is and How It Happens

---

All Internet payment fraud is based on stolen consumer or merchant identities. It also requires access to payment networks to complete the fraud. The result is product theft, identity theft, and cash theft.

## Stolen Consumer Identities

---

Credit card information can be stolen in several ways, not all of them online. Ironically, a common source of information for digital crime is discarded paper credit card receipts. These receipts often include the complete credit card number along with the card expiration date, information that is sufficient for most online and telephone credit card transactions. Criminals also use handheld "skimmers" to digitally scan credit card numbers in seconds from the cards themselves. This can happen to unsuspecting customers in restaurants or at cash registers. Lastly, criminals can obtain credit card information virtually by hacking into customer databases.

Criminals hack into a network infrastructure via misconfigured Web servers or other vulnerabilities in the network, shopping cart, or hosting provider. Hackers have also learned how to use technology in their favor. Automated code programs called "spiders" or "port scans" enable criminals to identify these vulnerable points in your network.

Once criminals have access to credit card information, they can use it to purchase goods and services for themselves or for resale. This is what is known as "product theft." Credit card information can also be combined with readily available social security numbers and address information to open new credit cards under the criminal's name and address. This is what is typically known as consumer "identity theft" and can ruin a consumer's credit record.

### *Estimated Fraud Costs by Fraud Type*

- Product theft=\$1-\$1,000 per event
- Identity theft=\$1,000-\$10,000 per event
- Cash theft=\$10,000+ per event

## Stolen Merchant Identities

---

Just as offline criminals break into a cash register, online criminals “break into” your virtual cash register by stealing your access information to impersonate you. This is what is typically known as merchant “identity theft.” Similar to consumer information theft, criminals obtain merchant information from both online and offline sources. Theft can be internal—employees or building visitors simply copy login and password information from sticky notes attached to computers. Criminals also break into buildings or go through a business’s garbage to steal this information. Online merchant identity theft involves hacking into your database or back-end systems to obtain payment gateway account password and user information.

This information is used to obtain unauthorized access to your payment gateway account, also known as “merchant account takeover” or “hijacking.” Account takeover allows criminals to steal cash directly from your business by issuing credits or other payments to themselves.

## Access to Payment Networks

---

Stolen identities are the first component of Internet payment fraud, but criminals must have access to payment networks to complete the fraud. Criminals get access to payment networks through two primary channels: 1) your Web site checkout page and 2) your payment gateway account.

Your checkout page is a public Web address available to everyone globally, 24 hours a day, seven days a week. The great benefit of a Web checkout page is that you can do business with anyone in the world and your store is always open. But this convenience also raises security issues. In one common fraud scheme, criminals access your checkout page to test stolen credit card numbers to see if they are valid, a process known as “carding.” Another scheme involves the use of “generators,” or software programs that automatically generate and submit spoofed card number sequences to your checkout page until they get a “hit” or an actual credit card number. Without the proper security controls, your checkout page can be an attractive destination for criminals.

More sophisticated forms of fraud actually involve taking over control of your payment infrastructure. In hijacking or merchant account takeover, criminals use merchant identity information in order to impersonate you and access your payment gateway account. Once inside your account, they have full administrative control, and can use this access to steal cash or for other criminal activity. Stealing cash is simple. Once the merchant has accessed your payment gateway, the criminal credits funds from your account to his or her own accounts. Criminals can also use your payment gateway to obtain valid credit cards to use for other forms of theft—in effect, using your business to commit crime and costing you thousands of dollars in authorization charges, chargebacks, and chargeback penalties. Hijacking a merchant account is not limited to external hackers. Current or former employees can also be a source for this form of fraud.



## Who Is at Risk for Online Fraud

It is important to emphasize that every merchant is at risk. Fraud can happen to any merchant at any time, and a single fraud incident can be enough to put a merchant out of business. That said, some merchants are at greater risk for certain types of fraud than others. VeriSign has put together the following “risk matrix” to identify some of the higher-than-average risk categories.

Fraud Risk Matrix	
Merchant Type	
Merchants without robust security defenses	Criminals that take advantage of sophisticated spidering techniques using intelligent agents that allow them to search the Internet for merchants with network vulnerabilities. Criminals then use this information to break into your network in order to steal your account access information for hijacking or merchant takeovers. This means that unless you have a strong network defense in place, you are a prime target.
High-visibility merchants	It's a double-edged sword. Merchants need to be visible to attract customers, yet fraud attempts are higher for merchants who advertise heavily or are in the news. And criminals know that merchants who are experiencing higher than normal transaction volumes have less time to defend against fraud.
Products/Services Sold	
Merchants that sell high-ticket physical goods that are easily resold	These items include luxury goods, computers, and other electronic equipment.
Merchants that sell goods that can be downloaded from the Internet	The purchase of these goods doesn't require physical address information, making it easier for criminals to disguise a fraudulent transaction.
Customer Base	
Merchants that sell internationally	It is difficult to validate the address or identity of foreign buyers, and it is more difficult to investigate and prosecute fraudulent activity from an overseas source.
Sales Season	
Merchants that have a heavy proportion of 4th quarter sales	Criminals know that you have limited time for fraud protection measures when sales volumes are high. Sales double in the 4th quarter; Internet fraud triples.
Merchants that run special promotions	Criminals watch for advertisements of special promotions. They know that you have limited time for fraud protection measures when sales volumes are high.



## What Banks and Card Associations Are Doing to Prevent Online Credit Card Fraud

---

Balancing the online consumer experience with stronger authentication methods has traditionally been difficult. Consumers shop via the Web for convenience and speed, but historical authentication requirements have been cumbersome, time consuming, and ineffective.

New Buyer Authentication programs, such as Mastercard® SecureCode and Verified by Visa®, provide more streamlined and customer friendly authentication via passwords. These programs enable you to gain liability protection by prompting consumers to share a password with their card issuers at checkout—similar to providing a PIN number for ATM transactions. Transactions in which consumers authenticate themselves to issuers effectively shift liability from the merchant to the issuer. Beginning April 1, 2003, merchants are not held liable for fraudulent transactions if they have been processed using Buyer Authentication.

VeriSign's new suite of Fraud Protection Services makes it easy for you to take advantage of this powerful new system as customers, acquiring banks, and processors begin to deploy it. (Check with your Internet Merchant Account provider directly to determine if they have deployed Buyer Authentication.) Through Fraud Protection Services, one seamless integration gives you access to both Verified by Visa and MasterCard SecureCode with your VeriSign Payflow® service.

## Protecting Your Business against Fraud

---

In spite of the growing threat fraud represents to merchants, there are ways to significantly reduce your exposure to fraud. There are essentially three levels of exposure to fraud on the Internet: the individual transactions themselves, access to your payment gateway account, and access to your network. Protecting your business from fraud requires that you address each of these levels in an integrated manner. Your VeriSign Payflow service comes standard with several important fraud protection features, but you need to activate them and use them in order to protect your online business. VeriSign Fraud Protection Services offer additional security features plus a single fraud management interface that allows you to access and monitor all of your fraud protection functions easily and conveniently.

## Transaction Level

---

Ensure that each transaction you accept and process is a valid transaction. You should also be careful not to deny suspicious transactions that are actually valid. Validation at the transaction level includes:

- Authenticating buyers when possible. This includes understanding who your repeat customers are. Keeping lists of repeat customers who have legitimately transacted at your site is important not only for fraud control, but also for understanding purchasing patterns and building customer loyalty. Make sure all customer information is encrypted and stored safely. Also, take advantage of MasterCard and Visa's Buyer Authentication programs described above to authenticate customers and benefit from the liability shift.
- Screening order content for fraud patterns. There is a wealth of information associated with each transaction that can help you understand the risk level. Activate the address verification service and card security code features that are standard with your Payflow service. Other screens such as IP address checks and shipping address validation will also help bring more certainty to a transaction with new customers. Also, keep a list of information associated with "bad" or fraudulent orders and check transactions against them. Similar to your list of "good" or repeat customers, bad lists help you streamline the checkout process. To effectively manage all of the risk information associated with a transaction it is important to use a rules engine. A rules engine automates the process of transaction screening so that you quickly fulfill orders for good customers and proactively block risky orders. VeriSign Fraud Protection Services allows you to cost-effectively deploy a rules engine as well as benefit from VeriSign's robust and continuously updated lists of high-risk indicators.
- Reviewing suspicious transactions. Finally, review each transaction that is suspicious to make sure you are doing business with a legitimate customer. Effective screening is essential to ensure that you have all the information necessary to make decisions regarding questionable customer orders before they are fulfilled. Online merchants today reject 5 percent of all transactions because they do not have the time or information to save a good sale from a suspicious one. VeriSign Fraud Protection Services allows you to automatically and continuously review only the suspicious orders, before you process them—giving you time to make an informed decision.

Although these steps are time- and resource-intensive, the security of your business depends on them. VeriSign Fraud Protection Services automates this manual process so protecting your online business from fraud is fast and hassle-free. And our "plain English" Fraud Manager interface is seamlessly integrated with your VeriSign Payflow service, so it's easy to set up and use, and you don't need any programming or fraud experience.

## Account Level

---

Make sure that only authorized users have access to your payment gateway account, and be alert for suspicious account access patterns. Protection at the account level includes:

- Locking down administrative access. Activate the “transaction settings” features that are standard with your VeriSign Payflow service. These settings allow you to limit access to high-risk administrative transactions, such as issuing credits. You should also change your account password on a regular basis. With VeriSign Fraud Protection Services, you can perform these functions along with other fraud prevention functions and features easily and conveniently using the single Fraud Manager interface that integrates seamlessly with your VeriSign Payflow service.
- Monitoring account level activity for suspicious patterns. Watch your account for signs of unauthorized access that could indicate merchant account takeover. Account Monitoring from VeriSign Fraud Protection Services offers affordable, customized, live account monitoring staffed by experienced fraud professionals. The service maintains rolling profiles of participating merchant accounts to uncover suspicious pattern indicators. Account Monitoring can help you catch account takeover before it does any damage—whether the takeover is due to a hacker or fraudulent employee usage of your service.

## Network Level

---

Ensure your network or “perimeter” is defended against unauthorized access. Protection at the network level includes:

- Locking down network access. Activate the “allowable” IP address feature that is standard on your VeriSign Payflow service. This ensures that only IP addresses you select have access to your network. With VeriSign Fraud Protection Services, you can access this and other fraud protection features from a single interface, easily and conveniently.
- Updating all patches on servers and operating systems. Invest in regularly scheduled security audits or port scans to identify network vulnerabilities. VeriSign Fraud Protection Services offers a free network scan from Qualys\*, included with every basic or advanced VeriSign Fraud Protection Services package.
- Monitoring firewall activity. Enterprise level e-commerce companies should also monitor their perimeter security on a 24-hour basis. Through VeriSign’s Managed Security Services, you can get customized perimeter security monitoring.

\*Qualys is a valued partner of VeriSign. Qualys provides an on-demand security audit service delivered over the Web that enables merchants to effectively discover and manage their network vulnerabilities and maintain control over their network security with centralized reports and one-click links to verified remedies.



## Let Customers Know That Your Store Is Safe for Purchases

Fraud prevention is the first step in ensuring the success and profitability of your online business, but it's just as important that you let your customers know your store is a real business that is safe to do business with.

In the offline world, customers can visit your store to assure themselves that it is a real business. And when they give their credit cards to you, they can see who they're giving it to. In the online world, it's a lot harder to know who you're doing business with. That's why Internet shopping cart abandonment rates are so high. VeriSign Secure Site Services give your customers peace of mind when making a transaction on your Web site. With VeriSign Secure Site Services, you get premium business authentication, SSL encryption services, and the premiere trust seal on the Web today. Displaying the VeriSign Secured™ Seal on your site lets your customers know that you are who you say you are.



## Save Time and Money While Protecting Your Business with VeriSign Fraud Protection Services

For many owners of small- and medium-sized businesses and for IT staff of enterprise-level companies, time is money. Protecting your business against the devastating consequences of even a single fraud attempt requires a significant time commitment and ties up valuable resources—time and resources that are better served in building and growing your business.

VeriSign has designed its suite of Fraud Protection Services based on VeriSign merchant feedback and the needs of the online business community. And as the market leader in Internet security, VeriSign maintains its position by proactively enhancing its products and services and anticipating new types of fraud attempts. This ensures that VeriSign technology continues to define state-of-the-art for online protection. VeriSign Fraud Protection Services not only provide you with the highest quality protection services at affordable prices, but also save you time and money.

We've made choosing the right VeriSign Fraud Protection Services package for your business easy. And it's simple to upgrade, so you only buy what you need, when you need it.



## Fraud Protection Services—Purchase Options

Service	Merchant Type	Key Benefits
Package Options:		
Basic	Designed for merchants with low transaction volumes	Maximum ease and convenience
Advanced	Designed for merchants with Mid- to high-level transaction volumes	Maximum customization and protection
Upgrade Options:		
Account Monitoring Service	All merchants	Account activity monitoring Seven days a week
Buyer Authentication Service	All merchants	Card association liability protection for authenticated shoppers
Managed Security Services	Enterprise-level merchants	Customized perimeter security

## Detailed Service Descriptions

### + Basic Fraud Protection Package

This package offers you a fast and convenient way to protect your online business—no fraud experience required. It provides essential Fraud Protection Services in a simple wizard-based upgrade module.

This package includes:

**VeriSign Fraud Manager Interface:** A single, consolidated Web interface in plain English, integrated with VeriSign Manager that allows you to quickly and easily manage all of your fraud protection features, without complicated “risk scores.”

**VeriSign Basic Fraud Filters:** Instantly and automatically screen your customer orders for potentially fraudulent transactions without impacting your customers’ checkout process.

**VeriSign Account Security Management Tool:** Integrates standard VeriSign account control security features into the Fraud Manager interface for added management convenience. Also allows you to control how administrative transactions are processed through your account.



### + Advanced Fraud Protection Package

This package offers maximum customization and fraud protection. This package includes everything in the Basic Fraud Protection Package plus:

**VeriSign Advanced Fraud Filters:** powerful, comprehensive, real-time, automated transaction screening. Filters are transparent to your site customers.

- Geographical location screening filter: State of the art filter that protects against “identity spoofing.”
- High-risk list filters: A complete suite of filters that reviews for high-risk zip codes, high-risk IP addresses, high-risk countries, and more.
- Merchant-specified lists filter: Build and manage your own bad and good customer lists. This feature automatically blocks “bad customer” purchase attempts at checkout and speeds loyal “good customers” through.



## Package Feature Comparison

	Basic Fraud Protection Package	Advanced Fraud Protection Package
<b>VeriSign Fraud Manager</b>		
Transaction review module	YES	YES
Audit trails on all reviewed transactions	YES	YES
<b>Fraud Filters</b>		
<b>Unusual Order Filters</b>		
High dollar-size filter	YES	YES
High item number filter	YES	YES
Shipping/billing mismatch filter	YES	YES
<b>High-Risk Payment Filters</b>		
AVS failure filter	YES	YES
CSC failure filter	YES	YES
High risk BIN filter		YES
<b>High-Risk Address Filters</b>		
High-risk zip code filter	YES	YES
Freight-forwarder filter	YES	YES
U.S. Postal Service address validation filter		YES
IP address risk list match		YES
Email service provider risk list match		YES
Geo Location filter		YES
<b>High Risk Customer Filters</b>		
Bad email list filter		YES
Bad credit card list filter		YES
<b>International Order Filters</b>		
High-risk country filter		YES
International/shipping/billing address filter		YES
International IP address filter		YES
International AVS filter		YES
<b>Accept Filters</b>		
Good email list filter		YES
Good credit card list filter		YES
<b>Account Security Features</b>		
Security audit from Qualys*	YES	YES
Allowed IPs (account access restrictions)	YES	YES
Transaction settings (control credits)	YES	YES
Password management	YES	YES
<b>Premium Service Features</b>		
Buyer authentication	YES	YES
Account monitoring	YES	YES

\*Qualys is a valued partner of VeriSign. Qualys provides an on-demand security audit service delivered over the Web that enables merchants to effectively discover and manage their network vulnerabilities and maintain control over their network security with centralized reports and one-click links to verified remedies.



## VeriSign Fraud Protection Services Upgrade Options

---

### + Account Monitoring Service

Add this service to either the Basic or Advanced Fraud Protection Package for premium protection against payment account takeover and hacking. Provides customized transaction monitoring by trained VeriSign security professionals. Also includes:

- Fraud Contact Line: Contact line that allows you to query fraud specialists about suspicious account activity
- Comprehensive investigation services for fraudulent transactions:
  - Investigation of VeriSign Internet log files and audit trails relevant to your account
  - Packaging of all relevant data to assist in funds recovery process with bank
  - FBI notification and data packaging to assist in prosecution of the perpetrator

### + Liability Protection with Buyer Authentication Service (Verified by Visa and MasterCard SecureCode)

Add this service to either the Basic or Advanced Fraud Protection Services Package for seamless integration of Buyer Authentication as it becomes commercially available from your processor or acquirer.

### + Managed Security Services

Add this service to either the Basic or Advanced Fraud Protection Services Package for fully customized, end-to-end, enterprise-level protection of your perimeter infrastructure. Provides a 24/7 private security staff without the costly overhead and time-consuming management requirements of an in-house staff. Services include:

- Managed Firewall service
- Managed Intrusion Detection service
- Managed Virtual Private Network service
- Technical Help Desk service

For more information on VeriSign Managed Security Services please visit <http://www.verisign.com/consulting/managed/index.html>.

## What You Need to Get Started

---

Secure e-commerce requires you to establish an online processing system that will allow you to accept secure online payments. VeriSign's secure, cost-effective, and customized payment solutions are designed so you can easily buy what you need, when you need it, with the option to upgrade or add services anytime, as your business grows. In three easy steps, you can complete everything you need to accept online payments on your Web site.



### 1. Choose a payment processing service

**Payflow Pro.**® Designed for merchants who want maximum customization, control, and scalability.

**Payflow Link.**® Designed for merchants who are just getting started on the Web or who have low transaction volumes.

### 2. Set up an Internet Merchant Account

All online businesses need to operate with an Internet Merchant Account, primarily for depositing and refunding online payments. VeriSign has made getting one an easy process. As you register for either Payflow Pro or Payflow Link, we will provide you the option to apply for an Internet Merchant Account with our preferred Merchant Account provider.

### 3. Customize your payment processing service with additional services

Protect your business and your customers from fraud

**VeriSign Fraud Protection Services.** From simple automated credit card fraud screening to enterprise-grade perimeter security services, VeriSign can save you time and money while protecting your business.

Accept repeat payments from your customers

**Payflow Recurring Billing Service.** A fast, cost-effective way to accept repeat payments for installment plans, monthly fees, or other subscription-based services.

Offer your customers an alternative to credit card payments

**Payflow ACH Payment Service.** Make sure you don't lose any sales opportunities by offering your customers ACH, a convenient and reliable alternative to credit card payments.

That's it! You've now got everything you need to start accepting payments online, conveniently, reliably, and securely.

#### + For More Information

For more information about VeriSign Payment Services including VeriSign Fraud Protection Services, please call us at (888) 847-2747 or (650) 426-3898 (select option 1), send an email to [paymentsales@verisign.com](mailto:paymentsales@verisign.com), or visit the VeriSign Payment Services section of our Web site at <http://www.verisign.com/products/payment.html>.

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