

# Wells Fargo White Paper: Merchant Techniques for Advanced Fraud Protection



## Table of Contents

<b>Executive Summary .....</b>	<b>3</b>
<b>Overview of Online Commerce Payments Fraud .....</b>	<b>4</b>
<b>Getting a Grip on Fraud .....</b>	<b>5</b>
<b>Identification: Recognizing High-Risk Transactions .....</b>	<b>5</b>
<b>Prevention: 21 Best Practices for Minimizing Fraud .....</b>	<b>6</b>
<b>Damage Control: Responding to Fraud and Other Chargeback Issues .....</b>	<b>9</b>
<b>Wells Fargo’s Service Offerings .....</b>	<b>10</b>
<b>Wells Fargo RiskAssessor Fraud Management Service .....</b>	<b>10</b>
<b>24-Hour Automatic or “Lights Out” Fraud Management.....</b>	<b>11</b>
<b>Unique Transaction Identifier for Simplified Chargeback Processing .....</b>	<b>11</b>
<b>Steps for Chargebacks .....</b>	<b>13</b>
<b>Enhanced Reporting .....</b>	<b>13</b>
<b>Consolidated Processing for Multiple Payment Types .....</b>	<b>13</b>
<b>Single Source Provider .....</b>	<b>13</b>
<b>Wells Fargo Payments Expertise and Recognition .....</b>	<b>14</b>
<b>Start-up Simplicity.....</b>	<b>14</b>
<b>Value Proposition Summary.....</b>	<b>14</b>
<b>Reduced Cost .....</b>	<b>14</b>
<b>Increased Security and Reduced Risk .....</b>	<b>15</b>
<b>Increased Revenue.....</b>	<b>15</b>
<b>Getting Started.....</b>	<b>15</b>

## Executive Summary

This white paper provides information on essential fraud control methods and services for businesses that accept orders and payments over the Internet. It was created by Javelin Strategy and Research, an objective third-party research firm, with the help of Wells Fargo's payments experts and builds on facts collected from merchants, industry experts, law enforcement groups, and other recognized resources.

Online fraud is the result of individuals or groups of persons who make purchases over the Internet with the intent of cheating the merchant. Unlike shoplifting in brick and mortar stores, merchants lose more than just the value of the stolen goods: they also suffer a chargeback of the full purchase price and shipping costs. Online merchants are more vulnerable because fraudsters are able to make faster purchases, sometimes over multiple locations in rapid succession, with no paper trail, no visual contact with the store, and as a result, little risk of being caught or successfully prosecuted.

Fraud-fighting techniques are only worthwhile if they stay one step ahead of the criminal. To control and manage fraud, merchants need to carefully evaluate the techniques and services presented in this document, beginning with the following steps as presented in the chapter entitled "Getting a Grip on Fraud:"

- **Identification:** Recognizing high-risk transactions
- **Prevention:** 21 best-practices for minimizing fraud
- **Damage control:** Responding to fraud and other costly chargeback issues

This chapter details the most common characteristics of fraudulent transactions, enabling the merchant to isolate and scrutinize specific online purchasers and behavior patterns. Additionally, 21 best practices for online fraud management are described in detail, some more essential or universally applicable than others; for example, obtaining real-time authorization and address verification. Finally, once fraud occurs (and it will), proven methods for minimizing the damage of loss of revenue and for decreasing operations expense are detailed.

**More than half of those who are online in the US shopped via the Internet in 2002. (Jupiter Research, 2002) Electronic commerce in the consumer sector alone is forecasted to jump from \$72B in 2002 to \$217B in 2007. -Forrester research, 2002**

"The "Wells Fargo's Service Offerings" chapter presents the capabilities of *Wells Fargo RiskAssessor<sup>SM</sup>*, an advanced fraud management solution which is bundled within its proprietary online payments processing solutions. This unique fraud management system identifies potentially fraudulent transactions that might otherwise go undetected (see graph on next page), while on average approving 96% of all online purchasers. Special emphasis is placed upon rapid and simplified response to customer disputes, so that legitimate customers with transaction problems can be differentiated from the online thief who must be immediately stopped.

Online purchases have grown significantly, opening up new markets and increased sales volumes that were barely imaginable only a decade ago. Merchants that follow the recommendations of fraud control experts as summarized in this white paper can be confident of minimizing losses and safely increasing revenues.

## Overview of Online Commerce Payments Fraud

The rapid growth of electronic commerce provides criminals with new and anonymous opportunities to plunder the profits of honest businesspeople. If electronic channels represent a significant growth and profit opportunity for merchants, the inherent risk of fraud is of equal concern. Business owners are wise to aggressively apply fraud containment techniques as described in this document.

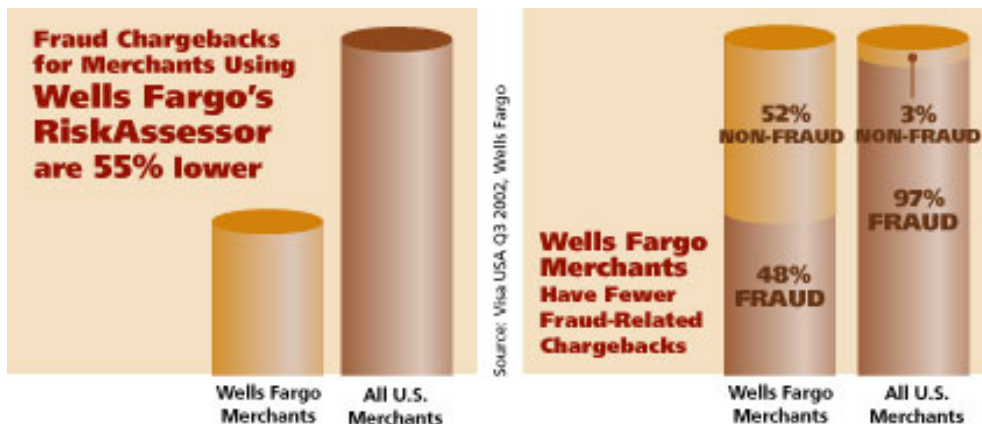
**According to Visa USA, fraud in traditional channels averages \$.07 on every \$100 in card transactions. Comparatively, card fraud through online channels is estimated to be between four to ten times higher, based on research from a variety of sources.**

Most consumer credit card disputes result in losses that are absorbed by the merchant. Merchants face a costly one-two punch, losing both the revenue from a fraudulent transaction as well as the shipping and material cost of the merchandise that was passed on to the fraudulent buyer. Merchants beset with excessive chargebacks are also likely to be hit with further action by card acquirers or associations, such as being charged higher transaction fees, having funds held in reserve, or even facing termination of service.

In the early days of the Internet, the techniques employed by fraudsters were simple. Much has changed, and online fraud has grown in volume, sophistication, and variety. Today, most online fraud comes from one of the following four categories:

- **Friendly fraud**, with a legitimate cardholder's friend or relative placing orders with a card that has been borrowed for illicit purposes. These transactions are later charged back by the cardholder.
- **Opportunistic individuals**, who stumble onto valid payment information and then commit fraud. Such individuals may follow their initial success with more organized activity.
- **Organized fraud rings**, which are large, highly sophisticated groups that often operate from locations outside the US. These groups change methods and locations constantly to thwart the latest fraud-prevention methods.
- **Internal fraud**, committed by employees of companies with "secure" cardholder data. Even the merchant's own employees may be involved, giving them insiders' access not only to valid payment data, but also to the latest methods of foiling prevention techniques.

Effective fraud prevention lowers the true cost of sales while acting as insurance against catastrophic fraud outbreaks that have brought about the demise of growing and stable businesses alike. Businesses with higher fraud risk must make a build or buy decision to determine if they can battle fraud on their own or if expert services, such as those described in the chapter entitled "Wells Fargo's Service Offerings," would be the most cost-effective solution.



## Getting a Grip on Fraud

The management of online fraud requires a blend of art and science, in pursuit of perpetrators with a seeming ability to constantly evolve their methods. This chapter contains a list of important fraud prevention techniques, some of which are only appropriate for merchants with relatively high fraud risk. Many of the methods are built into or replaced by Wells Fargo's RiskAssessor service and therefore are not required by businesses that use this advanced fraud management solution. Wells Fargo's proprietary fraud fighting services, introduced in the subsequent chapter, are designed to incorporate and build on the following three-step process:

- **Identification:** Recognizing high-risk transactions
- **Prevention:** 21 best-practices for minimizing fraud
- **Damage control:** Responding to fraud and other costly chargeback issues

**“With the explosive growth of the Internet, and e-commerce in particular, online criminals try to present fraudulent schemes in ways that look, as much as possible, like the goods and services that the vast majority of legitimate e-commerce merchants offer. In the process, they not only cause harm to consumers and investors, but also undermine consumer confidence in legitimate e-commerce and the Internet.” –US Department of Justice**

### Identification: Recognizing High-Risk Transactions

To effectively defend themselves against fraud, merchants must first learn to recognize its most probable indicators. While sophisticated profiling systems exist for this purpose, merchants that have the time, data, expertise, money, and experience to fight fraud on their need to begin by applying common sense. While characteristics of fraud are constantly changing, the following are among the most common characteristics of fraudulent transactions:

- Larger-than-normal orders. Because stolen cards have a limited life span, maximizing the value of each transaction processed is a typical behavior by the online thief.
- Orders that include several of the same items. Merchants need to ask themselves the obvious: would an individual normally buy a dozen or more of a certain item?
- Orders from first-time buyers.
- International orders, especially those that originate from high-fraud regions of the world. Currently, Nigeria, Indonesia, and Eastern Europe are producing a disproportional amount of online fraud in the US.
- “Rush” or “overnight” orders.
- Orders from those using free email services, such as hotmail.com or junos.com.
- Multiple purchases from same IP address on the same day.
- Orders shipped to a single address but made on multiple cards.
- Multiple transactions on one card or similar cards with a single billing address but multiple shipping addresses.
- Orders of high-priced products that are easy to resell, like electronics, jewelry, online digital content and event tickets.
- Any order that looks too good to be true.

## **Prevention: 21 Best Practices for Minimizing Fraud**

Effective fraud prevention can be time consuming and complex, yet businesses must process Internet transactions rapidly and cost-efficiently in order to prosper. The following techniques are not applicable to every online transaction or every merchant, yet every company that sells online should be aware of them. Some of these methods are universal best practices, while others can represent a short-term, do-it-yourself alternative to services such as *Wells Fargo RiskAssessor*, and therefore may not be the cheapest or most effective route for the long term. Merchants in high-risk categories (such as those who offer easily-resalable goods, expensive merchandise and services, tickets, digital content or sell internationally) have the most to gain by implementing the techniques described in this chapter. Fraud prevention is complex, and a proven partner can provide expertise as well as day-in, day-out support to reduce risk. The 21 best practices are divided into three categories:

- **Universal:** required procedure for all merchants that sell online, every time
- **Higher-Risk Practices:** for higher-than-average risk conditions
- **Highest-Risk Practices:** for situations with the greatest risk of financial loss

**Universal:** These best practices should be standard procedure for all merchants that sell online and are usually required to obtain the lowest transaction fees.

**Use real-time authorization:** Obtaining a real-time authorization for a transaction from a credit card company is a good starting point for detecting and preventing fraudulent transactions. This will ensure that the credit card has not been reported as lost or stolen, that it is a valid card number, and that it has an available credit limit for purchase. Be aware that this is not foolproof. Sometimes the authorization can be a false positive, resulting in a loss to the merchant.

**Keep authorizations current:** Obtain a new authorization if the original expires before shipment, e.g., if more than 7 days has elapsed between the authorization date and the shipment. For example, if an item is on back order, get another authorization prior to shipping in order to verify that the cardholder is still approved for the transaction.

"The boom in e-commerce has opened up fertile ground for fraud," said Hugh Stevenson, associate director of the Federal Trade Commission's Bureau of Consumer Protection, in testimony before the US Senate Finance Committee. "The Commission's experience is that fraud operators are always among the first to appreciate the potential of a new technology to exploit and deceive consumers," Stevenson said.

**Use address verification system (AVS):** An address verification system runs during the payment card authorization process, generally matching the billing address provided by the customer with the billing address on file for that credit card by comparing the address to the zip code on file. AVS plays a significant role as the first-line defense for all online fraud detection tools, including *Wells Fargo RiskAssessor*, and can help guard against friendly fraud and other fraud categories. AVS is not a cure-all solution, however, and each business should implement it differently based on their products, customers, geographic markets, and more. Note also that typically merchants must use AVS to be assured of receiving the best transaction rate from credit card associations.

**Check card verification codes:** Card verification codes (known as CVV2 for Visa®, CVC2 for MasterCard®, and CID for American Express®) are a way of verifying that a credit card is valid. American Express places the four-digit code on the front of the card above the account number. Visa and MasterCard use a three-digit number that appears at the end of the account number on the back of the card. CVV2 services should be

used, but not relied upon entirely, since they are not effective in all cases. However, merchants who request card verification codes may deter fraud simply by asking for them.

**Review unusually large orders:** Pay special attention to large orders, following these three standard procedures:

- **Institute an automatic review procedure for any transaction that is well above average.** For example, if an average sale is \$75, an automatic review could be instituted for any transaction over \$150.
- **Scrutinize every large order.** Look closely for inconsistent information such as different bill-to and ship-to addresses.
- **Pay extra attention to orders that are sent by overnight delivery.** Legitimate Internet shoppers generally won't pay for overnight or rush delivery. Seasonal patterns (e.g., floral deliveries on Mother's day) are an exception to this rule.

**Review orders for inconsistencies or obvious mistakes:** Make sure information from one field matches others, and watch out for unlikely misspellings in areas such as a city name or state.

**Ensure control of cardholder data:** Use security measures such as encryption and firewalls to protect internally maintained cardholder data records from misuse.

**Use recognizable, commonly known merchant account names** for customer billing. Non-recognition of the name of the merchant by the shopper often results in a chargeback. Typically these can be resolved after the shopper is contacted and notified of the merchant's identity. An accurate merchant account name on the cardholder statement will reduce this type of chargeback significantly.

**“Without a system for the effective prevention and management of fraud, merchants have become blindsided or even incapacitated by those who commit fraud through online channels.” –Javelin Strategy and Research**

**Use fraud-warning notices:** Place fraud-warning notices, buttons and images on your order forms and your website content. Let consumers know that fraudsters will be prosecuted to the fullest extent of the law. These warnings act similarly to security notices placed on homes, storefronts or offices, discouraging thieves from attacking online stores that appear to be protected.

**Manage shipments for cost recovery:** Use shippers that keep good records for easy tracking of delivery and receipt. Get extra protection on shipping costs, insure the shipment with a freight forwarder or an independent insurance company, and always declare the full invoice or shipment value.

**Higher-Risk Solutions:** for merchants or transactions with higher-than-average risk, these methods can be selectively implemented.

**Implement customer registration procedures:** Develop opportunities for customer registration, membership and transaction record archives in order to capture information that can later be used to positively validate a customer's identity. When trying to detect fraudulent orders or to recover fraud losses, more data is always better. (This conflicts with the concept of asking for no more information from a customer than needed, so use balance.) Lastly, it is helpful to build an overall profile of good transaction behaviors in order to more accurately identify bad ones.

**Utilize your own negative file:** Develop and maintain a database of names, addresses, zip codes, card numbers, companies, IP addresses, and phone numbers that have been associated with previous cases of fraud. Monitor authorization declines, identify trends and use it to constantly update negative file records.

Compile a zip code listing that pinpoints areas in which high fraud has occurred. Keep negative files and all cardholder information encrypted and behind a secure firewall, and remember that while a merchant's own negative file is helpful, a file from a large-scale partner will add millions of transactional and personal records to the process for greater effectiveness.

**Determine card-issuing bank:** For any sale over a pre-determined level, request the name and phone number of the card issuing bank, along with the exact name and billing address of the cardholder. Customers who don't know the bank's name may be using a stolen card.

**Use Internet Protocol (IP) number trace software:** IP matching verifies that the address of the computer being used to place the order is within 500 miles of the ship-to address. This can be a very effective tool, especially when the ship-to and bill-to addresses are different. If the IP is in Kazakhstan and the ship-to is in Kansas, there is a higher probability that the transaction is fraudulent. Note that IP addresses are increasingly disguised, and some criminals are even able to send messages via an unsuspecting individual's broadband-connected computer to mask the true IP address.

**“To enhance profitability in the competitive e-commerce market, your business needs a secure and robust payment infrastructure that can handle the unique risks of card-not-present sales.” -Visa International**

**Monitor all international transactions:** Be aware of the differences between international and domestic transactions, and pay special attention to all international transactions. These include non-US IP addresses, non-US credit cards, and non-US ship-to and bill-to addresses. Information passed through an international transaction (such as the format of the cardholder's address) differs from the information passed through a domestic transaction. Manual monitoring is highly recommended.

**Document all contacts:** For greater protection and more evidence against a fraudulent buyer, document all contacts you have with customers (and especially for approved but somewhat high-risk transactions).

**Stay informed:** A number of websites help merchants spot credit card fraud, including those found at the Visa and MasterCard websites and the Department of Justice. (<http://www.internetfraud.usdoj.gov>)

**Highest-Risk Practices:** for companies or individual sales that represent the greatest risk. While these methods are sometimes reserved for the most extreme cases of risk, some merchants who are paying much higher transaction fees or are in risk of losing a payments relationship may need to implement these methods more widely until a rampant fraud problem is brought under control through improved procedures or the addition of more sophisticated fraud control services.

**Use rules-based detection:** Merchants use rules-based detection software or services to define a set of criteria that identify potentially fraudulent transactions. The set of rules can be based on factors such as physical locations, amounts, past experiences, velocity levels, the number of transactions of different types, names, addresses, and various other factors developed in risk analysis models. These criteria should always maintain negative file information such as stolen credit card numbers, bad shipping addresses and telephone numbers, email addresses, names or aliases (e.g., “Donald Duck”). Systems will automatically screen orders and automate the decision to accept, review or reject the order. This is one of many capabilities provided by *Wells Fargo RiskAssessor* service as described in the following chapter.

**Cross-reference cardholder's information:** Cross-reference the cardholder's telephone number and address, to get an indication that the cardholder exists and lives where they say they do. Sites such as [www.switchboard.com](http://www.switchboard.com) offer data compiled from public phone directories, <http://www.anywho.com/> will do a reverse search on a phone number, and CDs can be purchased with databases of such information. Consider the cross-reference only as possible verification, and remember that data will not be available for unlisted phone numbers. Guides are not always accurate or up-to-date, so this step should be used merely as a part of the overall process, especially for merchants that want to solely manage fraud in-house.

**Contact the cardholder:** Call or email the cardholder to reconfirm the purchase order. Often, the telephone number on the otherwise authentic-looking purchase order will be counterfeit. On suspicious orders, the merchant can send an email to the cardholder stating that his or her order cannot be completed until the cardholder contacts the merchant.

**Consider predictive statistical modeling software:** Merchants have the option of implementing their own scoring software to fight fraud. This type of software is used by those with high-risk, high-value products to analyze data from many online transactions to create a profile of fraudulent behavior. Using data from historical databases, the software creates a mathematical formula and applies it in real time to incoming transactions in the form of a risk score. For many merchants, this may be more costly and less effective than having a third-party provide the same service.

**Online credit card fraud could comprise 52 per cent of all US card fraud in 2003, at a loss of USD 1.23 billion, up from 47 per cent of a potential loss of USD 1.82 billion to total card fraud in 2002, according to Celent Communications.**

### **Damage Control: Responding to Fraud and Other Chargeback Issues**

Because payment fraud is nearly inevitable for merchants who sell online, the capability to rapidly and efficiently respond to an inquiry from a financial institution or cardholder is essential. The first step in the damage control process is to eliminate the possibility that the transaction was a legitimate purchase by a cardholder with no fraudulent intent (e.g., a good customer): perhaps the customer simply had a problem with the transaction such as non-receipt of shipment, or the item was received but the cardholder tried to return it and it was subsequently lost in transport.

Even in the best situations, the manual research and respond process can be anything but simple: merchants must have an internal process for retrieving and updating records, combined with an external process for interacting with payments providers to minimize chargebacks and related expenses, as well as the capability to work with law enforcement agencies. *Wells Fargo RiskAssesor* service simplifies this process, but, in any case, merchants should respond to fraud, chargebacks or even a legitimate customer inquiry, as follows:

- **Respond immediately** to a customer's and/or financial institution's request for information about a transaction. It is to your advantage to quickly satisfy customer concerns and resolve disputes so that chargebacks from legitimate customers can be differentiated from fraudulent transactions.
- **Insist on working with processors and other service providers that will interact with you using a single electronic channel** (rather than using fax, paper, phone, or other methods, at their discretion). Consistent and efficient communication allows for easier monitoring and tracking, improving your ability to quickly and cost-effectively respond.
- **Maintain a single identification record for each transaction**, in order to reduce administration costs while increasing your ability to quickly and accurately retrieve transaction-related data.

- **Use all available law enforcement resources** (such as the FBI, local police, or county sheriff) rather than unnecessarily limiting yourself to just one agency, particularly for large losses. Because expertise, database coverage and available resources are subject to ongoing change, working with more than one group will result in higher success in fraud prosecution as well as prevention. There are two especially good online resources: the Internet Fraud Complaint Center (IFCC) is a partnership between the FBI and the National White Collar Crime Center (NW3C) and can be accessed at [www1.ifccfbi.gov/index.asp](http://www1.ifccfbi.gov/index.asp), while the National Fraud Information Center is at [www.fraud.org/info/repofrm.htm](http://www.fraud.org/info/repofrm.htm).

## Wells Fargo's Service Offerings

### **Wells Fargo RiskAssessor<sup>SM</sup> Fraud Management Service**

The proprietary *Wells Fargo RiskAssessor* screens, assesses, and flags fraudulent transaction data that might otherwise go undetected through standard processing channels. *Wells Fargo RiskAssessor* works on the merchant's behalf to reduce financial loss through such sophisticated capabilities as comparison of buyer data (for example, card number or email address) against massive data on confirmed or probable fraud suspects.

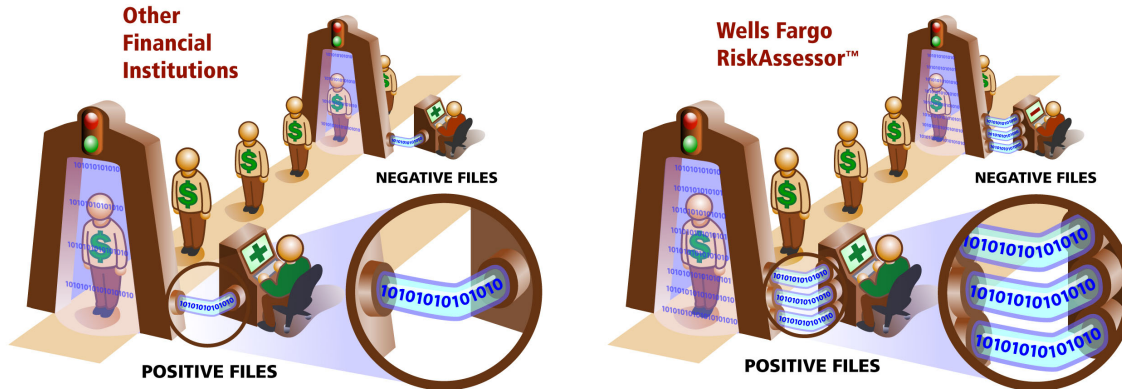
Using data from the third quarter of 2002, online fraud chargebacks for the average merchant using RiskAssessor were 55% lower than those for all online merchant transactions reported by Visa USA. *Wells Fargo RiskAssessor* also uses its depth of positive data to help make sure good customers aren't insulted and turned away, approving, on average, a full 96% of online cardholders.

**"Because our business sells high-value goods over the Internet, I spent months researching payments providers before choosing Wells Fargo's SecureSource Suite. We have been able to keep fraud from becoming an issue while realizing the service and stability that we were looking for." -Mike Atchie, Chief Executive Officer, 1-800-Plasmas**

*Wells Fargo RiskAssessor* proprietary advantage is two-fold:

- First, a team of experts constantly updates the actual models used to identify transactions that closely resemble those which are often fraudulent. *Wells Fargo RiskAssessor* scrutinizes highly predictive key variables such as domestic and international address validation, domestic and international IP address verification and order velocity.
- Second, Wells Fargo's advantage comes from the sheer volume of financial relationships that it has built since 1852. Fraud detection methods vary in their effectiveness, especially in proportion to their volume of historical transaction data. Wells Fargo's depth of processing experience is significant, with millions of data records based on significant, in-depth electronic processing experience.

Since 1995, when Wells Fargo became the first bank to process online payment transactions for merchants, they have tested and implemented over 100 online models for fraud prevention and, as a result, they are able to anticipate a far-reaching variety of fraudulent transaction patterns and methods. An advanced fraud screening capability is particularly important for merchants that are venturing into new and unknown markets. The risk-decisioning engine evaluates fraud risk for credit cards and debit cards, while also checking funds availability for electronic checks. The fraud reduction system not only reduces risk of financial loss, it also saves time during the all-important purchase authorization process, allowing decisioning in less than one second as transactions come through the system.



**More data equals better fraud detection  
with higher approval of valid orders**

Wells Fargo actively manages the system of sophisticated and effective rules that determine the accuracy of risk criteria. The team of risk analysts monitors and detects fraud to identify patterns and then incorporates these patterns into the *Wells Fargo RiskAssessor* system on a real-time basis. Because fraudsters are constantly on the move, Wells Fargo analysts are continuously working to identify trends and update the system, protecting merchants against potential losses.

**24-Hour Automatic or “Lights Out” Fraud Management**

Wells Fargo has the unique ability to completely automate the decision management process for merchants who want to implement automatic or “lights out” approval or decline decisions of all transactions.

- Merchants can unilaterally accept Wells Fargo’s systematic and proven recommendations for approvals and declines and thus rely on tested models for fraud prevention while avoiding constant manual intervention.
- In contrast, many other processing vendors simply provide numerical values that depict the perceived risk of each transaction, while requiring the merchant to manually approve or decline each flagged transaction.
- To further expand the automation and customization capabilities of its fraud management systems, Wells Fargo gives merchants the ability to change key elements of its standard risk-evaluation system as appropriate, in order to set the criteria for transaction acceptance, rejection, or if desired, manual review.

**Unique Transaction Identifier for Simplified Chargeback Processing**

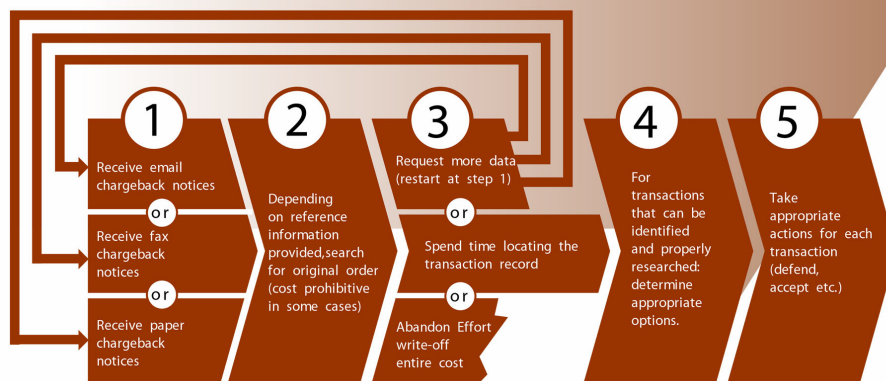
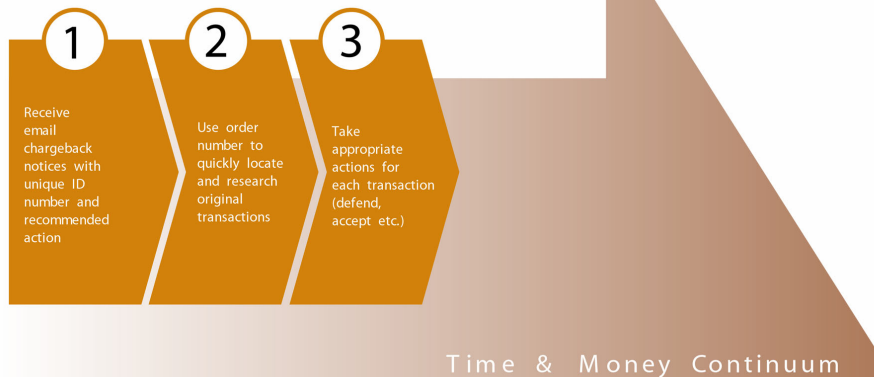
Wells Fargo has pioneered a Unique Transaction Identifier to allow merchants to track and manage every online transaction, including those initiated by credit card and debit card, as well as emerging payment methods such as e-check and singular international payments vehicles. As shown in the diagram on the next page, Wells Fargo’s Unique Transaction Identifier follows the transaction from authorization to final settlement, and reduces several costly research steps during the chargeback process.



Chargebacks are designed to protect cardholders from unauthorized transactions against their account. Thus, when a merchant receives a chargeback, time-consuming and often-problematic research must be conducted to prove that the merchant appropriately handled the transaction and that the customer received the intended and desired product or service as per specific bylaws established by credit card associations. Large merchants will realize particular benefit from more rapid identification of the transaction, while smaller merchants will find value in the recommended actions steps that accompany each chargeback notice.

When a chargeback occurs, Wells Fargo uses email to notify the merchant of the chargeback, the reason for the chargeback, the response deadline, and of particular value to smaller or newly online merchants, includes specific recommendations for reversing or challenging the particular chargeback. This information is referenced to the Unique Transaction Identifier in order to allow the merchant to more quickly identify any records in their own database and to take appropriate action. Wells Fargo's Unique Transaction Identifier simplifies this research process by providing a pervasive reference point for immediate access to the transaction details that typically exist in a variety of places. This number is assigned when the transaction first occurs, and large merchants, in particular, will benefit by having easy access to needed transaction data at all stages of the research process.

### Wells Fargo Chargeback Resolution Process



### Chargeback Resolution Process with other Providers

## **Steps for Chargebacks**

Wells Fargo helps merchants quickly process and respond to chargebacks to minimize losses. Due to identity theft and other growing issues, merchants are finding themselves in need of the same protection that originally caused chargeback systems to be created for the benefit of shoppers. Wells Fargo's Unique Transaction Identifier allows merchants to rapidly produce the data necessary to meet requirements for proving the date of the purchase, items or services purchased, authorizations obtained, and verification of shipment or fulfillment.

Without this integrated processing and tracking system, many merchants simply have no other realistic choice than to accept the chargeback as a costly by-product of doing business online despite the fact that the merchant may not be in error or violation of the card association chargeback bylaws.

## **Enhanced Reporting**

To more successfully and cost-effectively manage fraud and chargebacks, merchants must have more relevant, real-time, and simplified online reporting systems. With consolidated and enhanced reporting, fraud tracking and account reconciliation is simplified while requiring comparatively less review time. Reports are built on such standards as Extensible Markup Language (XML) for easier integration with online systems.

## **Consolidated processing for multiple payment types**

Another outstanding feature of Wells Fargo's chargeback system is consolidated processing and reporting of several different payment methods including VISA, MasterCard, American Express, Discover® and even electronic checks. This approach to integrated support and control further simplifies the fraud management process for the merchant. Typically, merchants who manage routine issues such as chargebacks with major card types and processing partners might find themselves logging on to several unique web sites, each with their own log-in information, user interface and underlying data structure, depending on which card the shopper originally used.

## **Single Source Provider**

Growing companies face a vicious cycle as they expand in search of higher profitability. Increased expansion and risk can cause merchants to seek relationships with a larger number of payment service vendors and solution providers. Wells Fargo provides service from a single provider in order to minimize the cost and complexity of managing fraud-related issues and procedures. Additionally, the single relationship positively impacts both fraud-screening abilities and the costly chargeback resolution process by using the greater depth of profiling, reporting, and tracking data, all through one proven processing provider.

**Wells Fargo's overall share of business to consumer e-commerce payments market is now nearly 10%, according to the U.S. Department of Commerce.**

## Wells Fargo Payments Expertise and Recognition

Wells Fargo is the nation's first and leading Internet bank, with over 4.5 million Internet banking customers, ranging in size from individual consumers to Fortune 500 corporations. In payments processing experience lends more than just a great reputation: it provides the very depth of data that is used to approve, reject or otherwise manage each transaction and thus drives down the risk, cost, and complexity of accepting online payments. Wells Fargo has over a 25-year history in the credit card payments business, and particularly Internet payments since 1995. Wells Fargo was the first bank to provide person-to-person payment services through eBay and today accounts for 95-99% of the domestic Web auction market.

As a diversified financial services company, Wells Fargo offers banking, insurance, wealth management, estate planning, investments, mortgage, and business services and is recognized as a leader enjoying a #1 status in retail banking, small business lending, agricultural lending, insurance agency sales, home equity lending, and in particular, secure online financial services.

### Start-up Simplicity

Getting a grip on online fraud is safe and simple with Wells Fargo – no matter what your size or complexity of business. *SecureSource<sup>SM</sup>* Suite solution, Wells Fargo's solution for small businesses with more basic requirements, helps control costs by providing a bundled payments solution. *Wells Fargo Global Payment Gateway<sup>SM</sup>* service provides a breadth of options for larger businesses with more complex fraud management capabilities, systems interface requirements, or international business needs. Additional software or upfront costs are not required and standard integration services (which can cost larger merchants \$100,000-200,000 or more with competing processors) are provided.

## Value Proposition Summary

**“Mail order/telephone order (MO/TO) and e-commerce merchants who choose to process transactions in the card-not-present environment must understand that there is a greater need for protection against fraud exposure and associated losses. This is primarily because card-not-present merchants can be held financially responsible for a fraudulent transaction, even if the card issuer has approved it.” -Visa International**

### Reduced Cost

One of the biggest benefits to merchants using Wells Fargo's proprietary payments processing service is the reduced total cost of operation. Advanced fraud protection is similar to both insurance and extended customer support services, as noted in the following:

- Automatic fraud screening aids merchants in minimizing losses, building on Wells Fargo's extensive fraud-prevention methodology and historical data file.
- Chargebacks are rapidly managed by utilizing Wells Fargo's Unique Transaction Identifier to research transactions, resulting in a higher percentage being represented to the cardholder's bank. This results in fewer losses for the merchant. Chargebacks for cards including VISA, MasterCard, American Express, and Discover are processed through a single system, saving time for the merchant and thus reducing costs.

- Program administration is minimized through simplified, integrated reports, thereby freeing employees to focus on other activities that improve revenues or strengthen customer relationships.

### **Increased Security and Reduced Risk**

Wells Fargo extends its recognized risk management services into new channels and global marketplaces, allowing companies to realize greater revenue while managing several areas of amplified uncertainty. Increased transaction security is built on an expansive historical database, technical expertise, and rigorous fraud management screening methodology:

- Tested fraud detection programs that minimize risks of selling in new channels markets.
- Reduced chance of incidents that could seriously damage the merchant's trust and public reputation.
- Modifications to fraud screening systems based on anticipated and actual changes in online crime practices.

### **Increased Revenue**

Merchants who sell online will only be able to steadily and profitably increase their revenues if the right fraud management solutions are in place. There is no denying that fraud occurs at a higher rate in online channels. By implementing the extra protection of *Wells Fargo RiskAssessor* (exclusively bundled into *SecureSource Suite* and available with *Wells Fargo Global Payments Gateway*) merchants will realize important benefits:

- Lightened workload. By letting Wells Fargo experts manage fraud prevention, merchants keep their own focus on increasing sales and profit margins.
- Uninterrupted progress toward the goal of increasing sales online, both in the US and international channels.
- Ability to accurately approve more valid orders through the use of the *Wells Fargo RiskAssessor* fraud management system.

### **Getting Started**

Accepting online payments doesn't have to bring unacceptable risk or unanticipated cost. Wells Fargo's website can clearly explain the popular *SecureSource Suite*, *Wells Fargo Global Payment Gateway* and other products that are designed to control online fraud issues. Wells Fargo also has advisors that will guide you through the process by asking about your products and services, target markets, customer profile and other areas, all to present you with the exact capabilities that your business needs to profitably grow. Smaller merchants will benefit from a number of standardized systems setups and reporting options that minimize the up-front effort; and they can be up and running in just a matter of minutes after completing a simple activation process. Larger companies will find that Wells offers a number of flexible options to assimilate with more exact requirements for integration, reporting, and other system and operational requirements that can be custom-tailored to their unique specifications.

Getting started is easy. Simply visit Wells Fargo at [www.wellsfargosecure.com](http://www.wellsfargosecure.com) or call toll-free 866-269-5545. If you already have a current banking relationship with Wells Fargo, call your Wells Fargo Relationship Manager.

Wells Fargo enables merchants to focus on what they do best, operating and expanding their businesses while Wells manages the risk and complexity of online financial transactions. Don't miss out on the rapid



growth of electronic commerce. Partner with Wells Fargo, the leading financial institution in electronic commerce, to realize increased revenue and profit without unnecessary cost and risk.

© 2003 Wells Fargo Bank, All Rights Reserved, Member FDIC Equal Housing Lender.