ESSENTIALS of Online Payment Security and Fraud Prevention

- Gain a working knowledge of e-commerce fraud prevention terminology, workflow, and strategy development
- Learn about the history of e-commerce fraud, typical fraud use cases, and the types of fraudsters that commit them
- Develop an understanding of the use and best practices for the 8 categories of fraud prevention tools along with the top 45 e-commerce fraud prevention techniques

David Montague

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:
Montague, David A., 1967–
Essentials of online payment security and fraud prevention/David A. Montague.
p. cm. – (Essentials series; 54)
Includes index.
ISBN 978-0-470-63879-8 (pbk.); ISBN 978-0-470-91512-7 (ebk);
ISBN 978-0-470-91513-4 (ebk); ISBN 978-0-470-91514-1 (ebk)
1. Electronic funds transfers–Security measures. 2. Electronic commerce–Security measures. I. Title.
HG1710.M67 2010
332.1'78–dc22 2010021354

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Acknowledgments

This book is the culmination of more than 13 years of learning, consulting, and teaching. During that time, my peers, clients, friends, and prospects have helped me develop into who I am. I owe thanks to all of them for their support and could not have written this book without them.

Most importantly I would like thank my family—Carrie, Andy, Sara, Izzy, and Hunter—for their support and patience as I spent so much of our "quality" time writing this book.

Introduction

Doing business online is no longer an oddity, but the norm, and companies desiring to remain competitive have to maintain some form of online presence. Doing business online means a company has to be able to efficiently, reliably, and securely take payments from consumers and other merchants. This book is written to provide the essential information companies need to find, assess, and select the right fraud management options they will need for their electronic commerce (*e-commerce*) channels.

As an essentials guide, the depth of coverage is intended to provide an introduction and working knowledge of e-commerce payments and fraud. This book provides the basic concepts around payment flow and management as well as the ways fraud is perpetrated, along with write-ups that define and provide best practices on the most commonly used fraud-prevention techniques. This book will not go into any detailed strategy design because strategies are proprietary and, once made public, are rendered obsolete.

Payments and fraud go hand and hand. Fraud is nothing new to the merchant. Since the beginning of time, man has always looked for the opportunity to defraud others—to gain goods or services without making payment. For the e-commerce channels, fraud is a part of doing business, and is something that is always a challenge. The merchants that are the best at preventing fraud are the ones that can adapt to change quickly.

Consumer-Present versus Consumer-Not-Present

Consumer-present (CP) and consumer-not-present (CNP) are a spin on the credit-card industries' definition of payment transactions. The credit card industry describes purchases as being either "card-present" or "card-not-present." The difference between the two is the presence of the physical card. If a merchant processes a transaction in which the consumer physically gives the card to process the order, the transaction is considered card-present. If the merchant doesn't take physical possession of the card to process the order, such as in the case of a telephone order, it is considered a card-not-present transaction. This book will be talking about a number of payment types beyond credit cards, but the concepts of card-present and card-not-present still hold true; thus the reason for the generalization of the concept to CP and CNP. Fundamentally "card-present" and "consumer-present" mean the same thing; it really doesn't matter what form of payment is being used, it is the physical presence of the consumer and payment medium that matter. These terms can be used interchangeably.

So who pays when a fraudster steals goods and services? It may surprise you to find out the merchant is left with the bill in most of the cases. For CNP purchases, the merchant is typically liable, while in CP purchases, the card association protects the merchants.

CNP includes all transactions in which the goods and services are sold to a consumer and the physical card is not given to the merchant. CNP includes three groups of transactions: phone-in orders (telephone order), catalogue orders (mail order), and e-commerce orders. Mail order and telephone orders are typically lumped together in a category we call MOTO. E-commerce typically refers to the sale of goods and services online.

This book focuses on the prevention of fraud for the CNP transaction. The payment process, fraud schemes, and fraud techniques will all focus on these types of transactions. In some cases, comparative views of

CP to CNP are made, but for the most part, I only speak to the CNP transaction.

It is important to understand the fraud-prevention techniques used in the CP world do not translate to the CNP world. There are a number of books and references available for preventing fraud in the CP space, but very few resources for the CNP space. The specific payment options and fraud-prevention techniques discussed in this book are designed specifically for the CNP space and will provide far better results for merchants.

In terms of orders processed, far more orders are processed in the CP space than the CNP space. While the CNP space represents less than one-third of the total credit card purchases annually, the e-commerce space is showing significant year-over-year growth. Today, e-commerce orders represent a very small percentage of the total CNP transactions occurring annually, but as you explore and expand into this channel, it is important that you have the processes and tools to prevent fraud losses.

In terms of fraud, the incidence of fraud in the CNP channel is far greater than the CP channel. Orders given in the CNP channel are far riskier for a merchant because the fraudster is anonymous to you.

Your Background with Fraud

If you are new to the fraud space, you are probably feeling a little overwhelmed. But don't despair—with the right tools, you can quickly make a difference for your company. Everyone assumes the other guy has a great fraud-prevention process in place, but in reality, everyone could use some help.

This book was written with the concept of a *fraud practitioner* in mind. A fraud practitioner is a person who is actively engaged in defining, managing, and monitoring fraud-prevention practices for a business. These individuals may or may not have a background in

preventing fraud, security, or criminology, but they do have a responsibility to stop fraud.

From my experience working with merchants all over the world, I have seen many different departments in an organization that are responsible for the set-up and management of fraud prevention for the business. Likewise, the individuals tasked with setting up and supporting a fraud-prevention strategy come from a variety of backgrounds, including customer service, finance and accounting, and information technology. Only some come from actual fraud, criminal, or security backgrounds.

It is important to understand that you will need input and assistance from multiple departments to build an effective fraud-prevention strategy. Customer service, sales, information technology, finance, operations, and legal departments all have a role to play. You have to integrate these departments into your plans to ensure that the impact of your new business processes and fraud-prevention techniques are well understood and can be interwoven with their goals.

Regardless of the department you report to, and your background with fraud, I have taken a lot of effort in this book to keep the concepts and explanations easy to understand. I have also provided many examples to illustrate fraud schemes and to help visualize how fraud techniques are used.

How to Use This Book

If you are new to e-commerce payments and fraud, start from the beginning of this book and work your way through it, and you will find that each chapter will build on what you learned before. When you are done, you will have a good foundation on payments and preventing fraud. For the more advanced fraud practitioner, you may use this book more as a reference tool to look up certain techniques or schemes.

Before you can successfully build an effective strategy to combat fraud, you have to understand the business processes and techniques that are available to you. In this book, I focus on the payment process, the

anatomy of fraud, and the most common fraud techniques in the industry. Beyond understanding the techniques, I discuss how you can use them and provide some best-practice advice so you can implement them.

Once you read this book, you will find yourself coming back to it as a reference to brush up on fraud-prevention techniques and how to use them.

Contents

CHAPTER 1

Understanding Online Payment Options

After reading this chapter, you will be able to:

- Discuss the payment options merchants have to do business online through mail order and telephone order.
- Describe the primary factors a company should use to evaluate and select payment options for its business.
- Describe the role and importance of credit cards and alternative payments in the e-commerce channel.

How do you begin to understand consumer-not-present (CNP) payments and fraud, and the mechanics behind it? You start with the CNP payment process. This gives you a basic understanding of the touch points and the order, people, and organizations that facilitate those touch points. Starting with a good understanding of e-commerce payments will help you see how the fraudster can manipulate these people and business processes to their advantage.

Don't shortchange yourself on understanding this process. Too often I see that fraudsters understand the business processes around payment better than the merchant does—and you can't afford that. You don't have to be an expert in e-commerce payments, but you had better understand the basics, or you will struggle in developing an effective

strategy. How will you know where the best points are to implement fraud-prevention techniques if you don't understand the payment processes? How will you know how to balance your fraud-prevention goals with the sales and administration goals if you don't understand the impact of your strategies on the payment processes?

You will also find the need to understand the payment process because you and your staff will naturally gravitate to what you know best. If you are like most merchants, you probably don't come from a law enforcement background. Depending on your background and the background of your team, you will find certain topics in developing your new fraud-prevention strategy more difficult than others.

Think about your background and others' on your team. If they came from the web site development or content teams, they will understand the buy page and shopping cart. If they came from the credit or finance side, they will understand the money flow, but not how the order is placed or filled. If they came from the call center, they will understand the order page, but not where it goes from there. You, as the fraud practitioner, are responsible for making sure everyone on the team understands how fraud touches all these points. You are also the one who has to create a seamless fraud-prevention business process that spans all these departments.

Remember, although your primary goal is fraud prevention and reduction, that is not every department's goal. Envision three major goals in a business:

1. Increase revenue.
2. Lower costs.
3. Reduce losses.

These goals can be in direct conflict, and your job is really to balance these goals to ensure maximum profitability to the company.

A good way to understand this is to look at it from a sales, finance, and operations perspective. Your finance department will focus on profitability, and profitability means looking at how much the business is

losing, how much it is spending to manage the processes today, and how revenue is impacted. In working with your finance department, you have to be prepared to explain the impact of any changes in terms of profitability.

Your operations and customer service departments will focus on managing administration costs. In working with them, you can expect to get questions about associated head counts. Does your new strategy reduce the need for people? Does it increase the head count? Does it add any costs to completing sales, such as transaction costs?

Your sales department will be focused on sales conversion, making sure it can get every possible sale it can. Those fraudulent orders still represent sales to these employees, so they are very leery of anything that might kill a potential sale. You will have to show the sales force that your efforts are not barriers to sales and are not insulting good customers.

For all of these departments, fraud is not the primary goal, so you have to be the champion to get them to feel the pain and to help in finding the right solution to stop fraud.

In Chapter 1, we discuss the payments landscape to lay the groundwork, so to speak, for fraud management.

The Payments Landscape

When most people think of online payments, they immediately think of credit card payments. While it is true that credit cards represent the majority of online payments today, there are a number of other payment options available. In all, eight categories of payment solutions exist with hundreds of service providers offering their services globally:

1. Credit card payments
2. Automated Clearing House (ACH) and bank payments
3. Payment aggregators
4. Credit-term providers

5. Cash-alternative providers
6. Advertising/promotional providers
7. Mobile payment providers
8. Invoicing payment providers

Payment methods other than credit card payments are called *alternative payments*.

Alternative payment solutions offer merchants payment methods they can offer to their consumers that don't require the use of one of the major credit card associations. Merchants and consumers look into alternative payment types for a number of reasons. Fundamentally, the market drivers are cost, security/trust, and ease of use.

The best-known alternative payment type is PayPal, which has grown exponentially and is becoming very much a mainstream payment method. If you research the market, a lot of providers out there are competing for mind share and market share. The risk for any merchant is adopting a payment type that will eventually die on the vine due to lack of adoption.

Most merchants view the alternative payment market as a limited competitive field with few real differentiators between the players. More often than not, merchants investigating alternative payments are limiting their discussion to ACH, PayPal, Amazon, and Google Checkout. In fact, there are a number of payment options and a rapidly growing number of service providers offering them.

TIPS AND TECHNIQUES

Not all alternative payment options will produce the same results; determining the right alternative payment options for your company means evaluating payment options based on regional support, consumer preference, customer base, and return on investment (ROI).

Regional Support: No one payment option is equally effective in all regions worldwide. Credit cards are accepted worldwide, but while they have dominated the U.S. and Western European e-commerce markets, they have not shown the same dominance in emerging markets such as Africa, South America, Asia, and Eastern Europe. In these markets, merchants need to support other payment options; otherwise, they will be limiting their potential customer base to only a small fraction of the overall population.

Consumer Preference: It is not enough to simply find an alternative payment method supported in the region you are doing business in; the payment method needs to be one that consumers in the region recognize, trust, and want to use. In Germany, credit cards are present and used, but they are not the preferred payment method. The preferred payment method is direct debit, *Elektronisches Lastschriftverfahren.*

Customer Base: The best alternative payment option has little value if the supported customer base isn't large enough to warrant the effort to integrate and support it. Evaluating a customer base should be done on two levels, potential and current. Consider China: 93 percent of the population of 1.3 billion people have access to direct debit, while according to *China Daily,* there were just over 100 million credit cards in circulation in China as of June 2008. In contrast, there were more than 596 million mobile phone subscribers as of June 2008. In terms of potential use, the ranking would be direct debit, mobile phones, and then credit cards. In terms of current use, the ranking would be direct debit, credit cards, and then mobile phones. Mobile payments offer excellent potential in China, but it is not the current preferred choice for paying for services in China. Does this mean you should not be looking at mobile payments? Not at all; in some regions, mobile payments are the dominant payment method, and three out of the top five alternative payment providers are working on plans to support mobile payments.

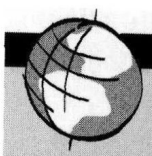
Return on Investment (ROI): The reasons why a merchant may implement alternative payments vary, from access to markets to cost reduction or easier supportability to consumer preference.

TIPS AND TECHNIQUES (CONTINUED)

In a majority of cases, merchants are able to show a favorable ROI on integrating alternative payments in a time frame that is more tactical than strategic. This is primarily attributed to increased sales from new consumer populations, lower costs than traditional credit cards, and better fraud protection.

Online customers and merchants have begun to turn to alternative payment methods for a variety of reasons ranging from lower costs, improved technology, and increased availability to security reasons. The debate is ongoing as to whether alternative payments are taking away market share from credit cards or are adding to it, but the fact remains that online credit card sales have been rising right along with alternative payment types.

According to *E-Commerce Times*, by 2012 online payments will gross USD $355 billion in value with alternative payments holding a 30 percent market share.[1] Javelin Strategy and Research predicts that overall growth for online payments is expected to reach $268 billion by 2013. Alternative payments will likely grow at a faster pace than credit cards with certain brands experiencing significant growth. More established brands are best poised to increase market share in this time of growth.



IN THE REAL WORLD

Alternative payments represent only a fraction of e-commerce total sales today, but according to Javelin Strategy and Research, about one-third of all online retail transactions ($268 billion) are predicted to be alternative payments by 2013.[a]

The probability of alternative payments growing to one-third of all sales by 2013 may be questionable, but it demonstrates the prevailing opinion that there is huge growth potential for alternative

payments. The explosive growth of alternative payments can be attributed to consumer and regional preferences. As every sale counts in these economic times, it is now more critical than ever that e-merchants understand and offer payment choices based on consumer and regional preferences.

[a] www.javelinstrategy.com/2008/11/10/new-javelin-study-forecasts-cash-based-alternative-payment-methods-growing-in-popularity-with-consumers-shopping-online/#more-1384.

Remember, not all alternative payment solutions work the same or produce the same results. To compare solutions against each other and to compare vendors, we need to group the solutions into categories of like services. In general, when you look at the competitive landscape, start by bundling alternative payment providers into a couple of categories, and then use those categories as methods to determine the payment positioning in general. From there, compare the detailed positioning of one vendor in relation to the other dominant players in each category.

Credit Card Payments

A credit card is part of a system of payments that enables the holder to buy goods and services based on the holder's promise to pay for these goods and services. The issuer of the card grants a line of credit to the consumer from which the user can borrow money for payment to a merchant. The major credit card brands—American Express, MasterCard, Visa, and Discover—have been the online payment option of choice since e-commerce was born. According to Entrepreneur.com, it's been repeatedly proven that if you don't accept credit cards on your site, you'll only capture about 15 percent of your potential sales.[2]

Credit cards are the alternative payment method to cash, and they are the dominant players in e-commerce transactions. Credit card associations charge *interchange fees* that range in value and differ from country