3-D Secure Payer Authentication: A Solution for E-Commerce Merchants

By Rick Lynch

GreenSheet 2/15

Payer authentication is the newest and most powerful tool available to e-commerce merchants today. Payer authentication provides merchants with the electronic equivalent of a signed sales receipt.

Under the umbrella of Visa's 3-Domain (3-D) Secure initiative, Internet merchants can participate in payer authentication. Visa's program is called Verified by Visa. MasterCard and Japanese Credit Bureau (JCB) also have 3-D Secure programs (licensed from Visa) called MasterCard SecureCode and J/Secure, respectively.

All three programs operate in exactly the same way; they validate that a consumer shopping on a merchant's Web site is the legitimate cardholder. Why would the payment Associations (Visa, MasterCard and JCB) want to do this? They worry about brand erosion.

Guaranteed Payment

The benefits for merchants using payer authentication are pretty substantial. First and foremost, the software guarantees merchants payment on any fully authenticated transaction, even if the transaction is later determined to be fraudulent.

Merchants will NOT be "charged back." In fact, Visa and MasterCard actually block the submitting of chargebacks to a merchant's acquiring bank, so there is not even awareness at the merchant bank level that a chargeback occurred. More importantly, the number of chargebacks that merchants record with their acquirers will drop dramatically. Typical participating merchants see a drop of 60% - 70% in their monthly chargeback rates.

Transaction Liability Shift

Even more monumental in concept than guaranteed payment is the shift in transaction liability from the merchant to the card-issuing bank. Never before in the history of card-not-present (CNP) transactions have the payment networks offered a way for merchants to avoid liability for CNP transactions that they accept. It has always been the merchant's liability. Those days are now over. This is ground-breaking stuff here, folks.

"If I Had a Nickel for Every ... "

Now, how about a little lower margin for doing business more securely? Visa says "sure." For merchants who simply install Verified by Visa software on their sites, Visa will lower their interchange rates by five basis points. I know, basis points are confusing, so what does that really mean? It works out to $0.05 for every $100 processed. A nickel doesn't seem like a lot, but it adds up when you're talking $1 million a month or more in sales.

Why did Visa do this? The card Association wants to motivate merchants to participate, and it intends for the five basis points to help offset the cost that merchants pay for their payer authentication services (typically $0.05 - $0.10 per transaction).

Common Misconceptions About Payer Authentication

Misconception #1:

"Not enough cardholders are enrolled."

This statement is 100% false because more than 300 million U.S. Visa cards are enrolled. Visa offers merchants guaranteed payment on all Visa cards* regardless of whether the cardholder is enrolled or not.

This means that from day one, with Verified by Visa enabled on their sites, merchants can cut their transaction liability by 50% - 60%, simply on their Visa transactions. Today, one out of every three online Visa transactions are fully authenticated, which means the cardholders have actively enrolled in the program.

MasterCard does not offer "attempts processing" liability coverage at this time, but the Association does guarantee payment on 5% - 10% of MasterCard transactions, and their adoption rate increases every day. When merchants combine the coverage of Visa and MasterCard, they typically receive guaranteed payment on 60% - 70% of their overall transaction volume. They also eliminate seven out of 10 chargebacks.

*A small percentage of Visa cards are not eligible for the Verified by Visa program, including some business-to-business (B2B) cards and prepaid gift cards.

Misconception #2:

"Not enough banks offer the service."

The above statement is completely untrue. Forty-five of the top 50 U.S. issuing banks, and more than 10,000 issuing banks worldwide now have the software up and running and available to cardholders.

Misconception #3:

"If it's such a good program, why aren't the 'big name' merchants doing it?"

Good Question. These merchants would like to know why you don't consider them "big names": 1800Flowers.com ; BlueNile.com ; CompUSA.com ; Cooking.com ; Crutchfield.com ; eBags.com ; eCost.com ; Etronics.com ; FogDog.com ; Hotwire.com ; JCPenney.com ; JetBlue.com ; LizClaiborne.com ; NewEgg.com ; Nickelodeon; Northwest Airlines; OfficeMax.com ; PlayStation.com ; TigerDirect.com ; Walmart.com ; WilsonsLeather.com ; Zales.com . And there are about 30,000+ others worldwide.

Misconception #4

"I've heard that Verified by Visa and MasterCard SecureCode cause higher 'abandonment' rates."

First of all, let's define abandonment. It's when a customer leaves/aborts the checkout process prior to a final submission of the order, including items for purchase, billing and shipping method, and payment information.

Pay attention to this: Payer authentication occurs after checkout (when the shopping cart sequence has been completed) but prior to authorization of the credit card (it works with both real-time and batch authorization).

Understanding the definition of abandonment explains why Verified by Visa contributes to absolutely zero "shopping cart abandonment." It simply can't happen. Fundamentally, Verified by Visa, as a process that a consumer would experience, does not begin until the checkout sequence has been completed. With that said, the initial implementation of Verified by Visa, more than two years ago, had some problems with the authentication process. But those problems have been fixed.

First and foremost, Visa no longer allows pop-up windows for the authentication screen. Due to pop-up-blocking software and the almost instinctive act of a consumer closing pop-up windows, Visa realized that this would not prove effective.

Since then the Association has mandated the "in-line" presentation method, which presents the Verified by Visa screen within the same browser window. This in-line method has proven to be dramatically more effective, reducing authentication abandonment from around 30%, down to less than 1%.

The in-line method also allows merchants to keep their brand on the same page as the authentication screen, which provides additional reassurance to shoppers that they are not targeted in a phishing scam.

Also, Visa and MasterCard strongly encourage the prominent display of the Verified by Visa and MasterCard SecureCode logos, both on the homepage and the checkout page so that it's clear to the shopper that this site is protected by these programs.

Finally, the strategic placement of consumer messaging (the fancy phrase for providing instructions and guidance to shoppers in the form of text) has been surprisingly helpful. Simply telling consumers what they can expect to have happen (e.g. "You might be prompted to enter your password if you are enrolled in Verified by Visa"), and what to do if the expected thing does not happen (e.g. "Please call this 1-800 number if you experience a delay or are unsure of how to proceed"), has been extremely helpful.

Misconception #5:

"Most consumers already have too many passwords; they'll never remember this one, too."

First of all, do you have a debit card? If the answer is "yes," then what's your personal identification number (PIN)? Don't answer that. It's a rhetorical question, and you never know who might be listening! But you get the point, right? Why is it that we can instantly recall the PIN for our debit card amid all the other passwords that we have? Because it's the key to our bank account and our money. The same goes for payer authentication; a consumer's password is the key to his or her money while shopping online.

In regard to consumer experience, it's almost identical to entering a PIN for a debit card purchase. In fact, if someone wants to make their Verified by Visa password a PIN instead of a longer password, it's perfectly acceptable.

The point is, there is already a proven and flourishing example of consumers successfully protecting their money with a password (PIN), and payer authentication works exactly the same way. Consumers simply enter it in their Web browser instead of an ATM or POS terminal.

Merchant Benefits of Payer Authentication

Guaranteed Payment

What does guaranteed payment mean? Exactly what it says. Let me make this crystal clear: If e-commerce merchants install payer authentication software on

their sites, Visa and MasterCard will guarantee that they get paid and can NEVER be charged back on fully authenticated transactions.

For a typical e-commerce merchant, this represents about 25% - 33% of Visa card volume and 5% - 10% of MasterCard card volume. If that's not enough, Visa also offers guaranteed payment, including chargeback protection, on what it likes to call "attempts processing."

This means that if merchants have the Verified by Visa software on their sites, even if shoppers have not yet enrolled in the program (have not set up their passwords), Visa will still guarantee payment on those transactions and block any chargebacks from coming back to merchants on those transactions.

This represents an additional 60% - 65% of a merchant's overall Visa card volume. When you combine the protection outlined in the above two paragraphs, that equates to roughly 60% - 70% of a merchant's overall credit card volume that's covered by the two programs. That means 60% - 70% of a merchant's overall credit card volume will be guaranteed payment and will be protected from chargeback liability. Sounds crazy, right? See Misconception #3 above to see how crazy it really is.

Chargeback Blocking

What is chargeback blocking? Exactly what it sounds like. Visa and MasterCard step in between the issuing and acquiring banks and block the passing of chargebacks from the issuing bank (which issues credit cards to consumers), to the merchant acquiring bank, (which receives funds for settled purchases from issuing banks on behalf of the merchant).

What this means is that the software blocks a chargeback from ever reaching the merchant's acquiring bank. This also means that the number of chargebacks that show up on merchants' monthly chargeback reports will drop dramatically, typically by 65% - 70%.

When the number of chargebacks drops, the fines for those chargebacks (usually $15 - $25 each) also go away. In addition, on a protected transaction that proves to be fraudulent, since there was no chargeback because the software blocked it, the merchant can keep the funds for that purchase.

The software again blocks the issuing bank from pulling the funds for that fraudulent purchase out of the merchant account. Why? Because in the eyes of Visa and MasterCard, merchants have done their part to protect the transaction: They have the payer authentication software on their sites. Merchants might be off the hook for those protected transactions, but somebody has to pay for the fraudulent transactions, right?

Transaction Liability Shift

Transaction liability is the end result of chargeback blocking. If fraud occurs on a transaction, and the merchant is no longer required to reimburse the consumer for that fraud because the merchant employed payer authentication on the site, then who will? The bank that issued the credit card. All banks that issue Visa or MasterCard credit cards are now liable for all e-commerce transactions protected with payer authentication by merchants. When did this happen?

Well, it's actually been a couple of years now, and has always been this way for Verified by Visa and MasterCard SecureCode. Now does it make sense why the biggest merchants in the world want these programs on their Web sites?

Why would issuing banks allow this to happen? Aren't they now exposed to a huge amount of fraud? That's partially true, but banks, as members of Visa and MasterCard, are bound by the rules of the card Associations of which they are members. Also, issuing banks realize that in the long run these programs will strengthen the brand of their cards and make consumers more willing to shop online.

The e-commerce channel today represents only 2% - 3% of the overall commerce in the United States; however, it's the fastest growing payment channel. Issuing banks realize that e-commerce is really still in its infancy. Or maybe now it's more like a toddler, like my one-year-old son learning to walk; sometimes he still stumbles around like a drunken sailor.

E-commerce might not be perfect, but it's getting better and becoming ubiquitous. However, in a few short years, e-commerce will be so big it will be too big to fix, so banks are willing to scrape their knees a little now and address any problems while they are still manageable.

When e-commerce is 5%, 10%, 20% or 50% of U.S. commerce, consumers should by then feel good about using their credit cards to shop online and not be afraid of identity theft and fraud.

Accept International Transactions

Do your merchants accept transactions today from Nigeria? No? Not surprising. Nobody does. However, what about Canada, Mexico, England, Germany, Australia or Japan?

Certainly customers exist in these and many other countries in which merchants would be happy to do business, if they only felt safe about accepting the transactions. But there's no Address Verification System (AVS) for these countries, so what can they do?

If merchants enable Verified by Visa and MasterCard SecureCode on their e-commerce sites, not only can they accept transactions from these countries and others all over the world, but they can do so with exactly the same benefits and protections that they receive on U.S.-issued credit cards.

A conservative approach for a merchant who is hesitant to test the international markets might be to simply offer to accept international orders only if consumers make them with a Verified by Visa or MasterCard SecureCode credit card. That seems fair enough. Talk about expanding your markets!

Reduce Overall Cost of Doing Business (Operational Overhead)

This benefit is probably the most difficult to put one's thumb on initially, but can be pretty substantial.

Ask merchants this question: How much manpower, resources and time does your business spend screening/filtering/manually reviewing transactions for fraud and then later dealing with chargebacks that slipped through these measures?

Whatever the answer is, cut that manpower, resource allocation and time by 60% - 70%, and that's what payer authentication has to offer merchants in terms of reducing their costs of doing business.

The bottom line is that Verified by Visa and MasterCard SecureCode make merchants' businesses more efficient. They reduce the time merchants spend trying to be security experts, and give them more time and resources to focus on selling their products, which is what they should be doing. It's a beautiful thing!

Which Merchants Will Benefit Most From These Programs?

If merchants accept credit cards as payment online for merchandise, then they can benefit. It doesn't matter if they are a small business or if they sell millions of dollars in merchandise every year.

More specifically, the types of merchants who will benefit most are those:

Who sell in high-risk categories for fraud such as jewelry, consumer electronics, software and DVDs

Whose items consumers can easily pawn or fence such as sporting goods, tools, tobacco and ticketing

Who sell 'soft' products such as games, music, content and airtime/phone minutes.

Where Can Merchants Get This Software?

Visa and MasterCard both have published vendor lists on their Web sites. Merchants should also talk to their merchant acquiring bank, payment gateway, and/or payment processor to find out if they already have a vendor that they recommend or have partnered with.

Oh, and Managed Prepaid also offers the service.

- Verified by Visa Merchant Information Site:
- http://usa.visa.com/business/accepting_visa/ops_risk_management/vbv_marketing_support.html
- Verified by Visa Consumer Information Site:
- https://usa.visa.com/personal/security/vbv/index.html
- MasterCard SecureCode Merchant Information Site:
- www.mastercardmerchant.com/securecode/index.html
- MasterCard SecureCode Consumer Information Site:
- www.mastercard.com/securecd/welcome.do

Verified by Visa Chargeback Reason Codes Covered:	
U.S. Visa Credit and Debit Cards - Full and Attempted Authentication	
23	Invalid Travel & Entertainment
61	Fraudulent Mail Order/Telephone Order/E-commerce
75	Cardholder Does Not Recognize Transactions
Visa International Credit and Debit Cards - Full and Attempted Authentication	
23	Invalid Travel & Entertainment
83	Fraudulent Mail Order/Telephone Order/E-commerce

MasterCard SecureCode Chargeback Reason Codes Covered:	
U.S. MasterCard and Maestro Cards Full Authentication	
4837	Cardholder Non-Authorization
4863	Cardholder Not Recognized