



SECURITY SUMMIT RECAP

What would bring together three of the Card Associations, four of the leading security assessment firms, four processors, twenty POS and PMS application developers, and 100 merchants from all industries and of all sizes? In a word: security.

Over 150 people attended the inaugural S.A.F.E. Transaction Security Summit, including Visa, MasterCard, American Express, Hilton Hotels, Swarovski, Heartland Payment Systems, InfoGenesis and INNfinity Hospitality.

The Transaction Security Summit brought together leading experts from across the credit card security industry. From the very first session by MasterCard, which introduced the regulations and explained their evolutions, to the very last session, a round table discussion featuring American Express, Visa, processors and security firms, the entire two-day seminar was focused on providing merchants and payment applications the detailed information they need about the latest security requirements.

"The difference between this event and others I have attended was foremost the level of detail available to attendees. They weren't just given the high level picture; they were able to delve into the details of security, to ask questions that related directly to their individual organization and certification process. It was like hours of free consulting from some of the most experienced names in credit card security, including several of us who were directly involved in the creation of these processes and procedures," stated D.J. Vogel, Managing Partner, 403 Labs, LLC.

The payment application track provided an overview of what your customers are facing in terms of the Payment Card Industry Data Security Standards (PCI DSS) and how that affects what

these customers are asking of you and your systems. More importantly, the summit provided a detailed look at the new Payment Application Best Practices (PABP) security guidelines, with which many processors are requiring validation, and how payment applications can design and upgrade their systems to address these regulations.

Overall, the event was a great success, receiving rave reviews from attendees and speakers alike. We look forward to an even more successful event next year and encourage all of you to attend. Look for the dates for the 2006 summit after the first of the year.

For those of you who would like to view the presentations and handouts from the events, they can be accessed on our website at www.shift4.com/summit_presentations.cfm

TOKENIZATION

To abide by the Card Associations' current requirement of not storing credit card data after the initial authorization (www.visa.com/cisp), Shift4 has developed a new Tokenization technology which enables merchants and payment application vendors to enjoy the highest level of payment processing security possible without requiring a lot of time, money or resources and still supporting incremental authorizations and recurring billing environments.

With Tokenization the purchase starts off the same. The merchant swipes the card data and sends it over to Shift4 fully encrypted. Shift4 sends the card data on to the processor and



receives back from the processor an approval. All this is the same as it is today; it is after this point where the process differs. Instead of sending back the card data to the merchant and the POS system, Shift4 turns the data into a Token. A Token is a globally unique, randomized representation of credit card data that is 16 characters long. For payment applications and merchants who utilize Shift4, only the Token is stored in the system.

The Token spans the lifetime of the transaction, even into history, so it provides all the same support for tips, tabs and incremental authorizations. Basically, the Token is stored on the POS system and when an incremental authorization is required on the card the Token is sent to Shift4. The Token represents a specific credit card transaction and card data that is stored in Shift4's data center. When the Token is sent through, Shift4 translates that Token into the card data and sends it to the processor. The processor sends back the authorization code; Shift4 turns it back into a Token and sends that along with the approval code to the merchants. The authorization goes through and again no credit card data is stored on the system. That means that the merchant doesn't need the card number or data past the initial request, so there is absolutely no reason to store this potentially dangerous information. The entire liability to protect the card data is now on the gateway, where it should be.

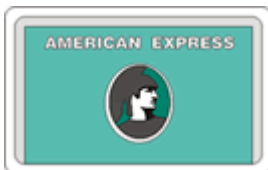
Implementing Tokenization is truly a small change with big results. Adding on Shift4 Tokenization requires a small change on the POS and PMS side. You need to add an addendum asking for this block and, of course, you need to store the Token. But even this part is easy. The Token can be stored in the now empty card number field, which is already setup to receive this type of data. Also, because the Token includes the last four digits of the credit card number, all of your system reports will still be fully functional. From a merchant's point of view, the implementation is seamless. In fact, it can be implemented even when there are pending sales or open tickets remaining. Best of all, the solution is available today and at no additional cost.

To find out more about Tokenization, please contact sales@shift4.com.

CREDIT CARD 101

American Express CAPN

Many of our merchants who accept American Express transactions have received a letter from American Express about their new Card Acceptance and Processing Network (CAPN) specifications. Basically, what the letter addresses is that American Express is



in the process of altering their authorization and settlement specifications. The letter states that if a system is not compliant with the CAPN specs by October 31, 2006 there will be an out-of-compliance fee of 25 cents added per transaction.

As a processor for American Express, Shift4 has already engaged American Express regarding the required changes and has a project plan in place. We should have the changes completed no later than 1st Quarter 2006. For your merchants who accept American Express and utilize \$ \$ \$ ON THE NET, no change is required by you or them. The update will be seamless and complete. For any customers you have going direct or through another gateway, you will want to contact American Express about the changes and new specifications so that you can reprogram your system directly.

NEW FEATURE

Stop Those Duplicates

We have added a new function to \$ \$ \$ ON THE NET to help merchants identify and resolve potential duplicate transactions before they are settled to the bank. There are a lot of reasons that a merchant may get duplicated transactions in a batch, everything from a clerk running a sale twice, to a POS sending the authorization request twice with different invoice numbers. When dealing with hundreds or even thousands of transactions in a batch, it isn't easy to sort through all of those transactions to identify potential duplicates. Thanks to customer input we have put together some new features that will help remedy this problem.

Now in the **View Options** menu merchants can turn on the **Duplicates Only** view. This will display all transactions in the batch containing the same card number (See Figure 1).

With this view, it is easy to identify a potential problem. We can see one instance, the \$200.34 transaction, which definitely appears to have been duplicated and needs to be corrected. The other case, however, could represent a consumer making two separate transactions on the same day for different product/services. Just because the card was used more than once doesn't mean it is a duplicate. The merchant will need to know whether these additional charges to that card are valid or not. When they are done reviewing their duplicate transactions, they simply go back to the **View Options** and turn off this selection so they can see the full batch again and submit it for settlement.

OVERCOMING COMMON NO'S

I want to Auto-Settle

\$\$\$ ON THE NET can be configured to enable merchants to auto-settle. However, this is NOT recommended. Shift4's \$\$\$ ON THE NET auditing functionality is the first line of defense against problem transactions. It empowers users to take control of their payment transactions by allowing a company wide audit to be conducted prior to deposit. Compared to traditional methods of transaction management, this proactive approach yields significant financial and operational benefits. However, merchants may be so accustomed to doing it "the old way" that they do not fully appreciate the value of the pre-settlement audit process.

Merchants employing the traditional reconciliation mode of transaction accounting (i.e. auto-settling), typically put off batch balancing and verification until their monthly bank statements arrive. This practice tends to put merchants in a reactive, defensive position, requiring them to correct errors that were made weeks or even months earlier. If errors are discovered after settlement, merchants may pay discount rates for a transaction for which they will ultimately not receive funding. Erroneous transactions also cause customer service issues and increase labor costs from retrieval requests.

Why let a monthly bank statement become an unwelcome surprise? \$\$\$ ON THE NET's allows merchants to correct errors before they become financial liabilities and/or customer service issues. Automatic settlement seems like it saves merchants a lot of time, but auditing before they settle can save them time and money.

If you are having trouble getting a merchant to understand the benefits of pre-settlement auditing or if you yourself would like more information, please contact the Shift4 sales team at (702) 597-2480, Option 3.

The Shift4Word is edited by Rebecca Kalogeris, Director of Marketing for the Shift4 Corporation. She can be reached by email at rkalogeris@shift4.com or by calling (702) 597-2480, ext. 3419.



Content is the opinion of Shift4 Corporation

© Copyright Shift4 Corporation, All Rights Reserved



Shift4 Corporation

1491 Center Crossing Road

Las Vegas, NV 89144-7047

(702) 597-2480

www.shift4.com

Current sale and credit transactions for ALL clerks. Only card types AX, DC, JC, MC, NS, VS and YC included. Only non-problem transactions are included. The transactions are ordered by card type, card number then invoice number. Only possible duplicate transactions are being displayed (multiple transactions with the same card number).

Printer Friendly

Export

Business Date: Fri Nov 4, 2005
(all transaction through)

Invoice	Clerk	Bus Date	Type*	Card Number	Amount	Tran	Customer Name	Terminal ID
0000104129	00001	Fri 11/04/2005	MC	5410xxxxxxxx1341	\$22.85	S	Stephanie Mancini	
0000114129	00001	Fri 11/04/2005	MC	5410xxxxxxxx1341	\$228.50	S	JP Prince	
0000064129	00001	Fri 11/04/2005	NS	6011xxxxxxxx3743	\$200.34	S	Katherine Bush	
0000074129	00001	Fri 11/04/2005	NS	6011xxxxxxxx3743	\$200.34	S	Katherine Bush	

Shift4 Sales Retail -- USD						
Card Type	Sales		Credits		Net	
	Count	Amount	Count	Amount	Count	Amount
MC	2	\$251.35	0	\$0.00	2	\$251.35
NS	2	\$400.68	0	\$0.00	2	\$400.68
	4	\$652.03	0	\$0.00	4	\$652.03

Figure 1 - *Potential Duplicates Screen*