

Shift4® word

The Voice of Shift4 Corporation and \$\$\$ ON THE NET®

Volume 1, Issue 2

Payment Processing News from Shift4 Corporation

October 2004

Welcome to the second edition of **Shift4Word**.

NEW INTERFACES

One of the most unique and powerful advantages of \$\$\$ ON THE NET is its ability to integrate transactions from all your locations, all your profit centers into one single online solution. That's why we are constantly working to create additional interfaces to POS/PMS systems and why we are continually expanding on the capabilities of the interfaces we already offer. Some of the new and/or expanded interfaces now available include:

- HiRez Network by Digital Mediums
- Micros 3700 (now with full gift card, signature capture and dynamic currency conversion capabilities)
- Omni Tickets
- One Pointe by Island Pacific
- PC/Register™ by AIM Systems, Inc.
- Pro-Sheep Keeper
- RentWorks by BlueBird Auto Rental Systems

A full list of the nearly 100 POS & PMS interfaces available can be found at www.shift4.com/pos_pms.cfm.

If you have profit centers not currently on \$\$\$ ON THE NET, I encourage you to call your account representative at (702) 597-2480, ext. 3430. The benefits of using \$\$\$ ON THE NET across your whole enterprise are numerous - centralized reporting, elimination of duplicate data entry, real-time financial views, the potential to lower your per transaction fee and much more. And don't worry; if you happen to use a system that we don't currently interface with, we are happy to work with you and your POS/PMS provider to build the interface.

CREDIT CARD 101

Fraud

- 75% of business executives and government officials surveyed reported at least one instance of fraud in the 12 months prior
- 60% of all fraud originates with employees, costing organizations an average of \$464,000 annually

External Fraud

External or customer fraud generally refers to a situation where a customer uses a stolen credit card to purchase goods or services. Most credit cards offer fraud protection to their cardholders, meaning that the cardholder won't be held liable for any charges that occur if their card is lost or stolen. That means that the credit card companies are going to look for someone else to foot the bill for these charges. One way for you, as a merchant, to limit your liability for these fraudulent transactions is to show the banks and card associations that you did everything you could to ensure that the card was valid, including:



Signature Capture – Every merchant who deals with card present transactions (i.e. everyone except online and mail order/telephone order merchants) should be collecting a signature from a customer. It is the simplest and most effective defense. Remember, if you collect the signature on a paper receipt, be sure that your copy of the receipt has masked or truncated account

numbers. If the merchant copy of the receipt displays the full account number, you must destroy the receipt after settlement thus negating the advantage of collecting the signature. Ideally, you should employ a signature capture device that allows you to collect an electronic copy of the customer's signature. That electronic signature will be stored in \$\$\$ ON THE NET and linked to the appropriate transaction. Instead of searching through paper receipts, you will be able to easily search through your \$\$\$ ON THE NET transaction database and bring up the signature.

AVS & CVV2 Codes - Shift4 offers Address Verification Services (AVS) and full support of CVV2, CVC2 and CID codes (the three or four digit numbers located on the physical credit card). Historically, AVS and CVV2 were used only for 'card not present' transactions, such as those on e-commerce sites or through mail order. Visa's VIP program, however, has extended the advantages of these tools to merchants of all types. Running these verifications can help guard against the use of stolen cards and can be particularly beneficial for establishments with larger ticket averages and for any company running a tab or open authorization (hotels, auto rental, etc.)

While the above steps will not totally eliminate external fraud, they will greatly minimize your liability if fraud should occur.

Internal Fraud

There are many types of internal credit card fraud, the most common of which involves the practice of corrupt employees issuing false or over-stated credits to their own card(s) or to those of their cohorts. This type of fraud is generally the most expensive to merchants and the most difficult to detect.

To combat internal fraud, \$\$\$ ON THE NET includes the powerful 'trusted' employee fraud detection and prevention tool, Fraud Sentry®.



Prior to settlement, Fraud Sentry scans through a company's transaction

archive, searching for a matching charge or series of charges that

correspond to each credit transaction. If a valid match is not found or if the credit exceeds the charge(s), the suspect credit transaction is flagged and reported to you via email. In addition, Fraud Sentry offers a variety of ways to analyze trends that may signal there are fraudulent activities.

Within the Fraud Sentry settings screen on \$\$\$ ON THE NET, you have the ability to control the 'velocity' settings. Basically, you are able to request that Fraud Sentry track and report a variety of different trends by setting your own threshold tolerances. For example, you may want to know if a card was used over a certain number of times in a day, week or month; whether the total purchases for a card exceeded a certain amount in any given timeframe; or even whether the total number or price of credits for a single card exceed the threshold. This type of trend analysis capabilities, allow you to uncover even the most advanced fraud and should be an integral part of your fraud fighting efforts. In order to take full advantage of these features, you must be sure to have accurate and current emails entered in the **Account Setting** section of \$\$\$ ON THE NET (see Tech Tips).

TECH TIPS

How do I update who receives Fraud Sentry emails?

You can change who receives the Fraud Sentry email notifications directly in the \$\$\$ ON THE NET system. Log on to the Root Administrator Account and navigate to Account Settings (under **Home - Administration Home - Account Settings**) . Once in Account Settings, make the necessary e-mail address changes in the Fraud Sentry Notifications section and click Apply at the bottom of the screen.

If the e-mail address you wish to change does not appear in the Fraud Sentry Notifications section, Shift4 has configured your settings and you must contact us to make any changes. Please fax a signed change request on company letterhead to (702) 597-2499. Include the reason for the change (e.g. old contact no longer with property, etc.), a business card, and copy of your picture ID.

What do I do if one of my employees forgets their password?

During installation, all \$ \$ \$ ON THE NET customers are provided with a root administrator account which has the capability to change or reset passwords for other accounts. All other users who were given administrative rights have similar capabilities. To reset the password, simply logon as a user with administrative rights and make changes in **User Maintenance** .

If the password to a supervisor or administrative account is forgotten, Shift4 Customer Support can intervene. We can change the password for the root account administrator user to its default upon receipt of a faxed request on company letterhead from a property controller, general manager or other senior official. This request must include a copy of a picture ID and a business card. If the person wants us to speak to someone else about the password reset they must specifically say so in the letter. Because of security concerns and the way account information is encrypted in the Shift4 database, it is not possible for us to change any other \$ \$ \$ ON THE NET account information or to accept reset requests from resellers or other third parties.

Fax all password reset requests to the Support Manager at (702) 597-2499. \$ \$ \$ ON THE NET Administrator password resets can only be performed during standard business hours, 9-6 PST.



WARM WELCOME

We would like to extend a warm welcome to the following companies who have recently signed with Shift4. We appreciate their business and are excited to be putting our solution to work for their organization.

*All Seasons Resorts
American Apparel
Blue Water Resort and Casino
Conrad Miami
Consolidated Resorts
Corazon Retail Group
Four Seasons Resort Maui
Gold Rush Casino
Indianapolis Hilton
Magic Star Casino
Marco Destin - Marco Island Store*

PRESS BOX

Here are the latest Shift4 headlines. To access the full stories, visit www.shift4.com/pr.cfm

[Shift4 Selects Ambiron as Its Card Association Compliance Partner – September 2004](#)

[N9NE Group Installs Shift4's Payment Processing Solution \\$\\$\\$ ON THE NET® - August 2004](#)

[Shift4 Corporation Leads Payment Gateway Industry in Reliability - Las Vegas, NV, July 27, 2004](#)

The Shift4Word is edited by Rebecca Kalogeris, Marketing Manager 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