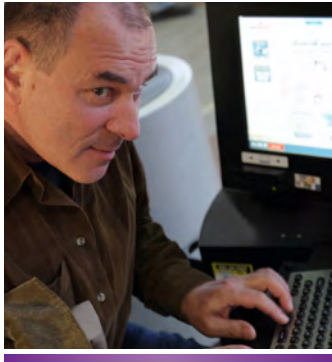


Welcome to the March edition of 4Sight. First, we'd like to thank all of you who answered the questions in last month's survey. We have worked to cater this issue to you, focusing first on fraud, which you listed as your top concern. We hope our Fraud Sentry[®] article will help you understand how Shift4 can help you monitor for and avoid "trusted-employee" fraud. As always, we welcome your questions and comments. You can submit them either on our blog or via OTNfeedback@shift4.com



Fraud Sentry

If you read our January newsletter, you already know that Shift4 was founded in response to a customer service inquiry. A client was looking for a unique solution, we were able to deliver that solution, and in the process come up with what we now call DOLLARS ON THE NET[®].

Another customer request came in a few years later and, as a result, we created Fraud Sentry[®], our powerful "trusted-employee" fraud detection and prevention tool. The following story is true; however, names have been changed to protect the privacy of those involved.

More than a decade ago, John, then CFO of a well-known hotel chain, came to us with a concern. He was seeing a disturbing trend: revenue was down but room occupancy and all other indicators were holding steady. John knew something was going on, but was struggling to figure out exactly what it was. He asked if there was anything we could do to help him sort through the mass of data and figure out where money was going missing. Of course, we agreed to help.

It took a few weeks of brainstorming to come up with a workable solution, but our team worked alongside John and eventually we found the cause. A few of John's controllers and at least one auditor were issuing credits on accounts with no corresponding charges.

The solution we developed was to imbed monitoring functionality into DOLLARS ON THE NET[®] that would watch for suspicious credits and automatically alert management to the questionable activity. We built the program so that clients could choose to block the transaction (preventing potential fraud) or to immediately receive alerts to suspicious activity (allowing them to catch dishonest employees in the act). John opted to configure the alerts to go directly to him – preferring to weed out these thieves rather than just stop their exploits.

Today, in addition to sending alerts to upper management confidentially, Fraud Sentry can also be set up to send alerts at the account level to managers/auditors at individual locations or at regional offices, thus giving a two-tier approach to fraud protection.

Within days, Fraud Sentry began to flag suspicious transactions and fraudulent activity at some of John's locations. His company had fallen victim to "trusted-employee" fraud. This internal fraud is rapidly becoming a major threat, with a recent study showing that nearly 50 percent of all fraud cases last year were internally generated. An enormous amount of money is lost each year when greedy and/or disgruntled employees who have been trusted with keys, passwords, and everything else they need to perform their daily operations turn against an organization and become thieves.

In addition to monitoring for suspicious credits, the current version of Fraud Sentry also offers a number of other ways to analyze trends that can point to fraudulent activities: users may set thresholds to know if a card was used multiple times during 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 dollar amount) of credits for a single card exceed the stated amount. These trend analysis capabilities allow merchants to uncover even the most creative fraud schemes.

If you are not familiar with Fraud Sentry, or need help setting up your automatic alerts, or need assistance validating who may be receiving these alerts currently, please send an e-mail to support@shift4.com, or give us a call at (702) 597-2480, option 2.



BIN Management

Debit or Credit? This is the age old question.

Do you currently accept Debit? If so, have you set your BIN management floor limits yet? If not, you could be losing money on unnecessary transaction fees.

BIN management sometimes known as “BIN spinning,” is a feature of Shift4’s Universal Transaction Gateway® (UTG®) that identifies card type as debit or credit. Validating that the card is debit-ready allows merchants to specify a dollar value above which all possible transactions will be processed as debit, thus saving money you would normally pay to your merchant service provider. You, as the merchant, have the flexibility to set this value at the point where the flat rate for accepting debit transactions and your negotiated discount rate for accepting credit transactions intersect.

What does that mean in plain English?

The vast majority of bank cards issued in the past few years have been debit cards that are backed by the card associations as well as issuers. These cards provide the cardholder the flexibility to pay using either debit or credit. This also provides flexibility to savvy merchants in that they can choose the most cost-effective method to process each transaction.

On credit transactions, merchants are charged a percentage of the total transaction amount (the exact percentage is determined by their discount rate); on debit transactions, merchants are charged a flat fee.

For example, if a merchant service agreement is negotiated for a \$0.50 per transaction flat fee for debit and a 3% charge on each credit transaction, at what point does it become more cost effective for the merchant to process as debit? While you’re opening your calculator app, we’ll save you some time. In this case, the threshold should be set to \$16.67.

This hypothetical merchant ought to set the floor limit at \$16.67, meaning all charges greater than that amount will be automatically processed as debit. The PIN Pad can be configured to not even display the option for credit and instead immediately present this transaction as debit (of course, for customer service, the customer can opt out and request credit).

Exactly how much money a merchant can save by using BIN spinning depends on the average ticket price and transaction volume. Given the figures above, BIN spinning would save the merchant \$2.50 on every \$100 transaction. It’s no wonder banks are implementing promotions offering cash-back or other rewards to customers who use their check cards as credit instead of debit – their profit on credit transactions adds up quickly!

As always, if you need help setting your BIN management thresholds, please send an e-mail to support@shift4.com, or give us a call at (702) 597-2480, option 2.



What You Had to Say: Results of the Customer Survey

We genuinely appreciate the time you took to respond to the survey we included with our last newsletter. The results confirmed some things that we were glad to hear and gave us the opportunity to cater our messaging to you, our clients.

Our commitment to merchant advocacy requires that we keep in touch with you. We need to be on the same page as our clients if we are to fulfill our goal of providing world-class service. Thankfully, it looks like we're doing well there, as 94 percent of respondents ranked our customer service as good or excellent (with more than 50 percent choosing "excellent").

For us, this level of customer satisfaction is the ultimate reward for our efforts. In nearly every meeting with Kathy Oder, our COO, she reiterates our need to fight for our clients and to remain committed to providing them with world-class support. "What does it mean to be committed?" she'll ask rhetorically. "Well, look at it this way: in a ham and egg breakfast, the chicken was involved – but the pig is committed. That's the kind of commitment we have to our customers!"

Part of our role as a merchant advocate is to educate our clients. Our survey showed that you are most interested in learning about fraud prevention, so we hope you'll take the opportunity to read the Fraud Sentry® article we included in this newsletter. Security and PCI-compliance rounded out the top three areas of interest, so we will be sure to work those into upcoming editions.

Ultimately, the message is this: we want to – we need to – hear what you have to say. We've been working to make it easier for you to provide feedback. We've added social media channels, a blog, and additional staff. If you didn't have the chance to fill out our survey, but have something you'd like to say, feel free to engage with us through any of these methods. And, of course, if you prefer your comments not be public, you can always send an e-mail to OTNFeedback@shift4.com

Upgrade Required for MICROS® 3700 Users

We recently sent an alert to all of our MICROS® users announcing a required upgrade for Secure Suite 4 MICROS 3700 – DOLLARS ON THE NET®.

As Shift4 makes every effort to install and upgrade our customers with the most up-to-date and secure versions of our systems and drivers. We again are taking our role as merchant advocates one step further with this upgrade; as this will secure the transactions at the terminal level to the Universal Transaction Gateway® (UTG®) and then from the UTG on to the Shift4 data center – thus getting the transactions out of the terminal, replacing them with a faux card and giving the properties an additional layer of security. A member of the Shift4 Technical Services team will be calling you (or perhaps already has called) to perform a survey and answer any questions. This call will be followed by a scheduling call with one of our Project Managers. You will need to schedule a 30-minute window for upgrade. (If you do not have a Remote Access Authorization Agreement on file with us, you will need to plan for a 90-minute upgrade process.) We will do our best to coordinate a time that best meets your needs.

For more information on this upgrade, please see the [original alert e-mail](#).

If you have an interest in starting this upgrade immediately, please contact our Account Maintenance Team at myaccount@shift4.com or contact our 24/7/365 Customer Support department at 702.597.2480, option 2.