

Fall is in full swing. We hope you all are enjoying the calm before the holiday rush and taking this time to make sure your operation is in tip-top shape. To help you, we've loaded this edition with technical tidbits to ensure you're at the top of your game. We've got articles on simplifying AVS, speeding up your connections, and another way to avoid suspended batches.

What to do if You Think You May Have Been Breached



Imagine you have just discovered something amiss in your system and signs point toward a potential data breach. Do you have a plan of action in place? Do you have people on hand who know how to deal with such a problem? If not, have you found an expert you can contact?

"When the time for action comes, the time for preparation has passed." An oft-repeated quote in emergency preparedness circles holds true in the world of payment card security as well.

This is why all of the questions we just posed (and many more) should be addressed in your Incident Response Plan (mandated by PCI DSS Requirement 12.9). When developing or updating this plan, we recommend you make sure the following elements are included:

1. Disconnect (but do not power down)
 - a. Disconnect from the network and from the Internet any devices you suspect have been compromised. (Literally unplug the network cables from the devices.)
 - b. Be sure you do not power down these devices until they have been fully investigated. (Malware could be removed from memory, making it more difficult for investigators to track down the bad guys.)
2. Notify
 - a. Do not attempt to hide the fact that you have been breached. The problem may spread with time, and you may be liable for trying to cover it up.
 - b. By card brand regulations, your merchant bank owns the ultimate risk for the breach, so their security and/or compliance officer should be ready and willing to provide you with guidance and expertise.
 - c. If your bank is unwilling to assist, contact Shift4 and we'll help you explain to the bank their responsibility to assist you (and liability if they refuse to do so).
 - d. You may need to contact local (or federal) law enforcement agencies to conduct an investigation.
 - e. Also, in many states you are required to notify any potential breach victims and/or constituents of your state. Consult with your legal counsel to determine your responsibilities and set an appropriate course of action.
3. Investigate
 - a. Depending on the severity of the breach, your bank or a card brand may require a PFI (PCI Forensics Investigator) to complete a forensic investigation of your organization. You should know that PFIs are not permitted to fix any problems

they find during the investigation, but should provide you with a list of items to be addressed by your staff or your IT contractor.

- b. If a forensic audit by a PFI is not deemed necessary, your bank may require you to complete some sort of investigation and report. If you have qualified staff on hand, you should complete a full investigation to determine what happened.
- c. Retention of a third party to perform a forensic investigation presents another set of risks on its own and is not recommended. If you have no other choice, you should seek guidance from your bank.

4. Remediate (Fix)

- a. If your internal IT staff is performing the investigation, they should fix problems as they find them.
- b. If the problem has been identified by a PFI or other external source, you should immediately begin fixing the issue(s).
- c. It's not enough to just fix the problem; you should also look at the underlying risks and threat agents that exploited the vulnerability(ies) in the first place, and ensure that vulnerabilities have been remedied to prevent their recurrence.

For reasons of liability, Shift4's support representatives are not permitted to provide additional advice concerning a suspected breach.

If you haven't reviewed your incident response plan recently, now may be a good time to do so. Ensure your policies are up-to-date and that you have contact information for any external sources of assistance you may need. [Visa's "What to do if Compromised"](#) document contains a number of useful hints that we recommend you incorporate into your plan.

Remember, "when the time for action comes, the time for preparation has passed."

More Suspended Batches? Discover the Solution



Back in July, we discussed [suspended batches](#) and gave you the two most common reasons batches suspend: 1) missing or invalid data included in the batch or 2) a communication failure somewhere between you and your processor.

Today, we'd like to add a third reason that has become common enough that we feel it deserves your attention. That reason stems from Discover's buyouts of Diner's, Carte Blanche, and JCB. (A move many of you may be unaware of because Discover has yet to rebrand the cards with their own name and logos.)

Basically, what happens is you accept a card number that references what was once a Diners, Carte Blanche, or JCB card. It's a valid card and the card number is within Discover's acceptable range, so the authorization comes back fine. However, upon settlement, when this card is to be sent to the processor, there is no indication as to which processor should handle it.

This is due to an oversight on the part of MSPs (your bank). To properly deal with this re-branded cards, MSPs need to bridge the old Diners/Carte Blanche/ JCB card ranges to their Discover setup.

If you're seeing lots of suspended batches, and especially if there are Discover cards in the mix, take the time to call your MSP and make sure you are properly set up to handle all Discover cards (even the ones that used to be something else). If you don't, you may end up having to void these transactions – which will cost you hard-earned revenue.

As always, if you need more information, feel free to contact us at support@shift4.com.

Shift4 Makes AVS Better



In our last newsletter, we discussed [several mistakes merchants make](#) that can result in costly Visa downgrades. One of these mistakes was not getting all the necessary AVS information. In an effort to demystify AVS for our merchants and advise of Shift4 features and benefits you may not currently be taking advantage of, we would like to offer the following “encore edition” of AVS education.

The Facts

AVS (Address Verification Service) is a functionality provided by issuing banks by which address and ZIP/Postal code information provided on a transaction can be verified against the billing information provided by the cardholder when they registered the card. The idea behind AVS is to prevent credit card fraud by validating that the customer is able to provide

not only the card number (which is printed on the card) but also the address information (which, theoretically, only the real owner should know) before allowing a transaction to process.

What AVS checks:

- Street number
- ZIP code, ZIP+4 code, or postal code

What AVS does not check:

- Cardholder name
- Street name
- Secondary address information (apartment number, etc.)

Interestingly, half of US and Canadian issuing banks are not ready to handle AVS. Those that are ready may only have accurate ZIP codes in their systems. There is also some industry confusion as to which numbers in the street address should be included with AVS (e.g., should 1123 32nd St. be 1123 or 112332, or should 12591 Main St. Apt. 12 be 12591 or 1259112). With this still up in the air, many issuing banks are sticking with only ZIP and/or ZIP+4. The merchant is given the option of what they want to accept as a valid address: ZIP, ZIP+4, address plus ZIP, or address plus ZIP+4.

Checking for AVS optimizes discount and exchange rates for card-not-present or manually entered transactions (especially MO/TO and e-Commerce). Strangely, merchants qualify for these optimal rates just by asking for AVS verification – the AVS information provided doesn't even have to match. We'll explain this next.

How it Works

What many merchants don't know is that AVS verification is not part of the authorization – it's an entirely separate request. So, if a merchant manually keys a transaction, he or she will actually get two responses from the issuing bank. One will approve/decline the amount and the other provide a single-digit code that tells the merchant if the AVS information provided was a whole, partial, or non-match. (A detailed list of these codes and what they mean will be provided at the end of this article.)

You should know that a failed or partial AVS verification does not always stop the issuing bank from authorizing the transaction. You, as the merchant, must decide which AVS responses you are willing to accept. Restricting the number of allowed AVS responses can create customer service issues and lost revenue, especially if you do not accept codes that indicate a partial AVS match (such as ZIP verified, but not street number). The catch-22 is that accepting certain AVS responses can also increase your liability when it comes to chargeback defense. If you're not sure which codes to handle, we recommend talking to your MSP.

Once you have determined which codes you are willing to accept, these codes are typically configured in your POS/PMS system, which will then allow or reject card-not-present/manually keyed transactions according to your specifications.

Shift4 and AVS

Shift4 makes this process easier for you by managing your AVS responses on a centralized basis. This means we take on the responsibility of approving or failing transactions based on your configured list. If a transaction you process receives an AVS response code that you indicated you don't want to accept, we send a failure response to your POS/PMS. (If you are unsure of which AVS codes are currently configured for your account, please contact our Support department at 702-597-2480, option 2.)

Shift4's Two-Pass AVS Feature

Shift4 provides another advantage for AVS verification. Because we manage AVS responses centrally, we can also offer merchants our Two-Pass AVS functionality. This is particularly helpful for MO/TO and e-Commerce merchants who want to validate AVS information on a transaction before authorizing the card for the full purchase amount. Rather than processing a \$1,000 charge only to find out the transaction failed AVS, Two-Pass allows merchants to submit an "AVS Only" transaction to verify AVS-validation status before submitting the full amount. If the first pass fails AVS per the codes you configure, Shift4 will send a failed response to the POS/PMS thus not tying up a cardholder's available balance (often referred to as their "open-to-buy" limit).

While using Two-Pass will increase the number of authorization requests sent via our system to the processor and therefore may involve some additional fees, the benefits far outweigh the costs when it comes to merchant protection and customer satisfaction. And, because we want to help you save as much money as possible, Two-Pass allows merchants the freedom to set a dollar-amount threshold below which "AVS only" validation request is not required. (In other words, you will only see these small additional fees on transactions that you deem large enough to warrant the additional security). For more information on Two-Pass AVS, please [contact us](#).

Are You Slowing Your Own Connection?



To facilitate the hundreds of millions of transactions we process each year, Shift4 maintains multiple data centers, a host of Web servers, and numerous Internet connections. The duplication of components provides redundancy and increases uptime, but thanks to a little bit of technical magic, it also enhances our speed.

Just as Shift4's Universal Transaction Gateway® supports adaptive routing to score all potential routes to and from your processor and provide you with the fastest transaction times, merchants logging into DOLLARS ON THE NET® can be automatically routed to our least busy server. More server bandwidth means faster responses to your queries and a smoother overall experience.

Sounds great, right? So why are we telling you this? Well, we're telling you this because many of you make a simple mistake that could be keeping this process from working correctly.

When you type in "www.dollaronthenet.net," you don't actually connect to that page. Rather you are routed to a server (whichever one has the least traffic at that moment) so by the time the page loads you'll see a URL of "serverX.dollaronthenet.net." If you then bookmark that page you will forever be routed to that specific server (whether it's busy, empty, or even offline for maintenance at the moment you try to log on).

The easiest way to fix this is to edit your bookmark and be sure that it points to www.dollaronthenet.net and not to any specific server or sub domain. If you're not sure how to edit bookmarks, open your browser's help function (usually by pressing F1 while the browser is active) and search for bookmarks.

If you need additional assistance, contact Shift4 Support at 702.597.2480, option 2.

Micros 3700 “Special Swipe” Issues with Secure Suite for Micros



Shift4 has recently identified a glitch that can occur in certain scenarios with Micros 3700 systems that are running a piece of technology called “Special Swipe” interfacing with our Secure Suite for Micros. Since the issue only arises when the product is used in conjunction with Shift4’s driver, please contact us and not Micros support to resolve it.

“Special Swipe,” a technology provided by Micros, gathers partial card data from erratic (too fast, back-and-forth, or repeated) swipes and attempts to combine those partial reads into a single, intelligible swipe.

The problem surfaces when “Special Swipe” is installed on your Micros terminals along with Shift4’s Secure Suite for Micros and clerks swipe erratically. When “Special Swipe” kicks in, it has a tendency to send the complete card number saved from the previous transaction to 4Go and on to DOLLARS ON THE NET®. It is easy to imagine the confusion and frustration that might ensue if your last customer’s card was charged for the transaction immediately following their own.

With this in mind, we have added code to assist with this issue and to prevent these errors from happening to your customers. If you’re a Micros 3700 user, please take a moment to see if your system has “Special Swipe” and if it does, contact Shift4 so we can ensure your system receives this updated version of Secure Suite for Micros.

To determine if you have “Special Swipe” and if you need the Shift4 update, go to the 4Go screen. On the bottom right of the screen you should see a button. If that button says “display version,” you are up-to-date and do not need to update. If the button is blank, click it. Upon clicking, you should see a screen display. If you see (ss) in the line of information on the pop-up, you have Special Swipe on that terminal and need to contact our 24/7 Technical Support Help Desk to update to the new version of Secure Suite for Micros.

Support can be reached by calling 702.597.2480, option 2, or by e-mailing support@shift4.com. If you need additional assistance, contact Shift4 Support at 702.597.2480, option 2.



Will Your New POS/PMS Work with Shift4?

Implementing a new POS or PMS is often a major undertaking. Research, the purchase process, and planning for and then installing the new system can take months. How would you feel if you went through this whole process only to find that your new system does not work with Shift4?

This recently happened to a client of ours, and it took them weeks to remedy. Imagine weeks without [TrueTokenization®](#), without [DOLLARS ON THE NET®](#), and without all of the other Shift4 tools you rely on every day. Weeks of frustration could have been easily avoided with a two-minute phone call to Shift4 to verify the new system was integrated to and compatible with DOLLARS ON THE NET before buying.

If you’re planning to change your POS or PMS, please [check our list of compatible integrations](#). If you don’t see your desired choice, take a few minutes to call or e-mail us and find out if it’s going to work. If we don’t currently support it and you can convince us we should, we might even write a new integration for you.