Volume 26 Fall 2015

Posi's Plate

Seasonal Tips and Information from Your Point of Sale Specialists

Notes from the Chef

Fall is here! We all look forward to the ramp up of business where we can start getting ready for the busy holiday season. This fall once again brings lots of changes to our restaurants. The ever evolving world of security and credit cards are changing the way we get and save data. One of the big changes that you will experience this fall is the shift in liability for EMV credit cards from the card issuers to the merchants. Make sure to look at our Appetizer section to learn more on the benefits of getting P2P/EMV and how our Ingenico P2P device allows you to be on the cutting edge with NFC payments. As always we truly appreciate your business and we love to help you succeed! We hope you enjoy reading about the options that we have to assist you in navigating the changing road map of data security.

Joel Smith

Director of Support Services

Specials

CHANGING CREDIT CARD PROCESSORS

There are many reasons for deciding to change processors such as a better rate, changing banks, quicker access to your money, etc. Do your research, ask questions, and read the fine print on the contract to make sure you know the terms and fees. Be aware that Gift Cards are sometimes linked to your credit cards so you may also need to decide how to handle them.

After you decide on a processor call Data Business Systems so that we have permission to work with the new processor. The first step will be to check your current configuration since a new processor will require you to be PCI Compliant for them to accept your business. We use that information to send you a contract for the cost of the processor change and any necessary upgrades to be PCI Compliant. The contract is then signed and paid; you or the processor would forward to us the new setup information, commonly referred to as a VAR sheet. We work directly with the processor and do in -house testing so that there is a smooth and seamless transition. Once we ensure the setup is working a new build goes to our software team for install.

Processor changes are done remotely and scheduled on Tuesdays, Wednesdays or Thursdays before the site opens. All prior credit card batches need to be closed before the new processor is installed. Once the processor change is complete, which takes approximately half an hour, the software rep will work with the manager to test a credit card to confirm credit is running before open.

By Mary Blanchard

Appetizers

More on EMV and P2PE

You may have noticed a few articles in our newsletters informing you of our P2PE (point to point encryption) solution and the liability shift occurring in October with the implementation of EMV in the United States. We have repeatedly included this information so that you, our partners, remain informed of the changes in the credit card industry.

We have always been firm believers in implementing a P2PE solution as a way to avoid being the next breach headline. With P2PE installed the system utilizes tokenization and removes the credit card data from your system. We are attaching a recently published article on this subject from the National Restaurant Association where they too believe the current focus of restaurateurs should be on protecting the credit card data while it is in transit. Without implementing a true P2PE solution, you are still exposing your business to a breach.

Contact your sales rep for more information on getting these devices installed.

By Tim Fogarty

Entrees

Entrees: Ingenico capabilities:

In this newsletter we are focusing on changing items. One item that is definitely changing, besides the weather, are the ways in which you can accept payments from your customers. The Ingenico unit that we have been deploying will not only outfit your establishment with the strongest level of credit card processing available by enabling P2PE (point to point encryption), it will also allow you to take NFC (near field communication) payments.

These can include Apple Pay, Google Wallet and any additional NFC payment types. In addition to this, the Ingenico unit is manufactured with the necessary slot to accept EMV cards. As of this publishing, the certifications are still in process with various processors so while they are capable, they are not yet ready. The immediate benefit is the activation of P2PE which utilizes tokenization to secure your credit card processing. The units are also able to address the times when manually entering a card number is needed as they are outfitted with a numeric keypad.

The implementation of these units does not affect your ability to adjust credit card mistakes, tip adjustments and all the other issues that arise. Not only are you securing your environment but you are also able to operate as usual. Contact your sales rep for more information!

By Tim Fogarty

Desserts

DBS Connect

If you've had to call the DBS helpdesk to troubleshoot any given issue, you may be familiar with DBS Help. It is a remote control utility tool that allows us to connect into your PC. Today around the globe, computer industries are working around the clock to make systems more secure, build walls against cyber-attack, and remedy known system vulnerabilities. Granting a third party PC access for remote connection imposes a serious security threat if the requester is not validated. It is comparable to letting thieves into your house who claim they are from the cable company in for repair. A question we should all ask, is the request to remote connect legit?

In response, we are soon retiring DBS Help. Instead of the faceless call requesting access to your computer, we at DBS have been using DBS Connect for remote connection. DBS Connect has a dual authentication remote connection utility tool that gives you increased security. We send a request which you must accept before we can access your system. DBS Connect users are controlled, maintained, and monitored by Data Business Systems. We can track who and when a DBS Connect user was connected into your system. Having a wall of security under your control brings confidence and peace of mind to you if there's a need for us to connect into your system. You can identify if you are currently using DBS Connect by looking for the above icon in your system tray. This change will be mandatory in order to receive remote support. If it is not maintained support will be available on site only. DBS Connect is a yearly subscription based service.

By Nirmal Amatya

Your Point of Sale Specialists since 1977.

Current Versions:

POSitouch: 6.40

TransAction Plus: 7.5.1

Please note, charges may apply for calls to our support center.

156 Business Park Dr.
Virginia Beach, VA 23462
(757) 490-1294

3040 Williams Drive, Ste 630
Fairfax, VA 22031
(703) 573-2292

Data Business Systems
(800)868-2323
WWW.1DBS.COM

To EMV or not to EMV?

June 30, 2015

To EMV or not to EMV? That's the question many restaurants are asking.

Deciding whether to invest in card-processing systems that accept credit and debit cards embedded with microchips – also known as EMV, or chip, cards -- is a hot topic in the restaurant world these days. Here's why: Starting Oct. 1, 2015, merchants who haven't invested in EMV-enabled equipment will be liable for fraudulent purchases made with a counterfeit credit or debit card.

If you're like many restaurateurs, you may be having a hard time building a business case to take action to meet the EMV "liability shift." Often, the numbers just can't justify the time and cost it takes to implement the technology. As restaurants consider purchasing and installing EMV-enabled terminals, here are a few tips and pointers.

What's EMV?

EMV or chip card technology, long used in Europe, makes it harder for criminals to produce counterfeit credit and debit cards.

Criminals known as "carders" take card numbers, often from hacked businesses, and make counterfeit cards using real account numbers. Counterfeiting remains easier in the United States because of outdated magnetic-stripe technology. EMV technology helps end this kind of fraud because retailers presented with an EMV card can run it through their readers to know it's genuine.

Banks and card companies have begun rolling out EMV cards in the United States. Estimates for how quickly they'll roll out vary widely. The Aite Group last year estimated that 70 percent of credit cards and 41 percent of debit cards in use in the United States will be EMV-enabled by the end of this year. Javelin predicts 29 percent of credit cards and 17 percent of debit and prepaid cards will be EMV-enabled by the end of 2015.

Unlike in Europe and Canada, the card brands in the United States are only issuing EMV cards that require "chip and signature" authorization. It's not clear when "chip and PIN" will arrive in the United States for EMV cards. Also, for the foreseeable future, the EMV cards that are being rolled out in the United States continue to carry the magnetic stripe. So even if you haven't installed an EMV reader, you can still continue to take and process card payments just as you always have.

Know the facts

It's important for restaurateurs to know the facts as the Oct. 1 liability-shift deadline approaches. Among the top things to remember:

- **This is a choice.** There's no legal or regulatory requirement for merchants to install EMV readers or take action by Oct. 1. The card brands have simply modified their contracts to penalize those merchants that chose not to implement the technology – and the penalties happen only if a merchant is defrauded through the use of counterfeit or stolen cards. It is a business decision that each company must make.

- **EMV may be a fix for a problem you don't have.** Counterfeit cards have primarily been a problem for high-end retailers, electronic stores and other retailers. Criminals use counterfeit cards to buy high-end goods and resell them on the black market for a quick and easy profit. Typically, carders and other criminals haven't targeted restaurants. If you haven't had a big problem, you may not need to make a change. If you see a growing problem after the October 2015 liability shift, you may want to reevaluate.

- **Weigh the costs.** To evaluate your potential liability, look at how many, if any, of your chargebacks are due to the use of counterfeit or stolen cards. If the numbers are low, it may be hard to justify the cost of EMV-enabled terminals. Even if you experience fraud, the cost of the chargeback may be far less than the cost of installing a new EMV reader, or fleet of readers. As you look at the expense of buying and installing EMV readers, consider whether you're better offer investing in new technology that offers stronger protections, such as encryption and tokenization.

- **Ask the right questions as you upgrade.** As you upgrade your POS system, make sure the new system incorporates not only EMV technology, but also encryption and tokenization technologies. The NRA considers these technologies far more important for restaurants than EMV. Encryption technology immediately encrypts card data as it's entered into the POS system, so it's unintelligible even if it get stolen. Tokenization replaces stored card data with "tokens." These tokens are unusable by hackers and have no value.

  A growing number of vendors -- including NRA partner Heartland Payment Systems, which offers its "Heartland Secure" solution – are offering end-to-end encryption and tokenization technologies to scramble customer card data and protect it from the moment the card is swiped.

In short, EMV helps you deal with counterfeit cards, but encryption and tokenization will protect a restaurant from hacking and data breaches – and that's a bigger threat to restaurants' bottom line because it could subject you to huge fines from card companies, customer lawsuits and damage to your restaurant brand.