Alert: Payments Security and Compliance for Dealers

When it comes to payments security, Dealer Pay has you covered.

There are 3 major components to security that we want to review: EMV, Hardware, Network & Connectivity, and PCI Compliance & Best Practices.

EMV CARDS

EMV cards are equipped with consumer chips for transaction authentication. When a chip card is inserted into a terminal, a unique code is created that can only be used one time. The code is sent to the cardholder's bank, which authenticates the transaction. In contrast, using magnetic stripes, the same data is used each time, opening options for duplicate and fraudulent transactions.

All merchants are required to have EMV ready terminals, that accept chip cards. But what happens if you don't? You are susceptible to fraud and even a bank chargeback. If you don't handle EMV transactions correctly, your funds for a legitimate transaction will be withdrawn, letting your customers get your products and services for free!

But that is not all! There are many payments providers, now implementing additional fees for EMV Non-Compliance, up to 1% and $25 per month!

HARDWARE

Not all payments hardware or terminals are the same. Again, they need to be equipped to accept EMV chip cards, but they also need to be connected to your secure network. Please note, if you are still using a phone line to process transactions, please act now to upgrade, for this could be a major security risk. Hardware devices should be deployed with PCI SSC encryptions directly from your provider, using rigorous standards for encryption, decryption, key management, and chain of custody. Point-to-point encryption is applied immediately to the payment data upon tap, dip, swipe, or key-entry. Not only does this both protect your dealership and reduce your PCI scope, but it also protects your customer's sensitive data.

PCI COMPLIANCE AND DEALERSHIP BEST PRACTICES

There are three main components; 1. how you protect stored cardholder data, 2. how you restrict physical access to cardholder data, and 3. maintaining policies that address information security for all personnel.

Dealer Pay's Point-of-Sale solution does much of this for you. We use secure gateways, tokens and other forms of security, such as IP filtering, multi-factor authentication and 3-D Secure, with all aspects of our solutions.

Annual PCI Self-Assessment Questionnaires are mandatory and there are various forms. The SAQ P2PE has been developed to address requirements applicable to merchants who process cardholder data via hardware payment terminals, included in a validated and PCI-listed Point-to-point encryption solution, such as Dealer Pay. Please also note, that your network security plays a large role in registering PCI compliance (with or without hardware). You must have the necessary firewalls and password protection on all servers interacting with any payment acceptance.

Lastly, just to make sure we covered all the bases, it is recommended to use best practices in each department, to both avoid loss and breech, which could result in large fines. Pay attention to The Gramm-Leach-Bliley Act, Truth in Lending Act, Red Flag Rule and Form 8300.

At any time you have questions about your existing configuration, exposure or compliance, you can always reach out to our team.