CONNECTED PAYMENTS

Connected Payments EMV Capabilities Update and FAQ: October 21, 2015

Dear Valued Connected Payments Customer,

The NCR Connected Payments and EMV Liability Shift teams continue working to deliver a certified EMV acceptance solution for use in the field with the NCR Connected Payments solution.

As previously communicated, certifications by some processors and card brands are delayed due to the multi-party complexity and interdependencies of the payment solutions, not just for Connected Payments for EMV support, but industry-wide. NCR and our NCR Connected Payments partners continue to work with all necessary third parties to secure the EMV solution certifications.

Below please find the latest update and targeted approval dates for EMV-certified solutions:

NCR Connect Payments EMV Certifications	First Data Concord H&C	First Data Rapid Connect	Vantiv Tandem	Worldpay	Chase	Elavon
VeriFone Mx915, Mx925	**Certified**	**Certified**	**Certified**	Oct 30, 2015	Oct 23, 2015	Oct 30, 2015
VeriFone TAVE/VSP Mx915, Mx925	**Certified**	n/a	n/a	TBD	n/a	n/a
VeriFone Mx830,850,860,870,880	**Certified**	**Certified**	**Certified**	Oct 30, 2015	Oct 30, 2015	Oct 23, 2015
VeriFone TAVE/VSP x830,850,860,870,880	TBD	n/a	n/a	TBD	n/a	n/a
VeriFone e335 (for PVH Mobile)	TBD	TBD	n/a	n/a	n/a	n/a
Equinox L5200, L5300	TBD	Roadmap 2016	TBD	TBD	TBD	TBD
Ingenico iSC250, iSC350, iSC480	Nov 13, 2015	Roadmap 2016	Nov 13, 2015	TBD	TBD	TBD

There are a few important points to note regarding EMV liability shift:

- The shift is the result of contract requirements that major payment networks have put in place with their merchant customers, and is not based on statutory or regulatory requirements. We are aware of no regulations or penalties by financial or governing bodies regarding merchants' acceptance of EMV cards, before or after Oct 1st.

- The change in liability for a merchant after Oct 1st is only present in particular “card present” scenarios when the mag stripe is used on an EMV capable card and the card is fraudulent. We have detailed this scenario, along with ways to help mitigate potential liability, in the FAQs below.

Because the liability shift arises from your contract with your payment network, we strongly encourage you to consult with your network, payment processor, or other relevant subject matter experts regarding any questions or concerns. Statements in this update and the attached FAQs regarding liability are based on generally available information, and while we believe them to be correct, they are not warranted to be accurate, and are not intended to provide legal advice.

Your partnership and collaboration are extremely important to us and our teams are fully committed to supporting your success, and to providing superior service and reliable performance. Our goal remains to provide the solution you need to optimize your enterprise and best serve your shoppers while protecting your business. We thank you for your patience and support as we work towards our mutual goals and to uphold this commitment.

In the interim, we understand there will be many questions as we move through this process; therefore we have included a status chart along with FAQs to best answer the most common inquiries on status and potential impacts.

Kind regards,
NCR Connected Payments Team

Frequently Asked Questions (FAQs) about EMV

Q. If I don’t have an EMV ready payment solution in place by October 1, am I liable for chargebacks and penalty fees associated with the use of counterfeit or stolen cards used at my store?

A. According to generally available information, the liability shift means that a merchant, rather than the network or bank, will be liable for fraudulent transactions made under certain circumstances. One scenario in which the shift occurs is where an EMV card is presented by a consumer, but cannot be accepted via chip reader, and is instead accepted via Mag Stripe Reader (MSR), or as a manually entered card number. If this transaction is subsequently flagged as fraudulent to the issuing bank, after Oct 1st, this transaction will result in a chargeback to the merchant for the amount associated with that fraudulent transaction.

The Oct 1st liability shift has no effect on liability associated with credit card breaches; it addresses only fraudulent or counterfeit cards physically presented at a merchant location. The PCI-DSS standards remain the generally accepted framework for protecting systems that store, process, or transmit cardholder data.

Merchants, acquirers, processors and others implementing EMV chip technology in the U.S. are strongly encouraged to consult with the respective payment card brands regarding applicable liability shifts and rules. Merchant liability is determined by the card issuer, and each has different rules for different scenarios.

Q. If I do not have an EMV ready solution by October 1, do I need to notify anyone?

A. We are not aware of any requirement for merchants to notify anyone of their EMV readiness or status.

Q. What should I tell customers when they ask me why they can’t use the EMV chip and PIN capabilities on their card? How can I assure them that their credit card data is safe?

A. You can assure your customers that while the store does not yet support EMV technology, you are currently in process of certification. However, reassure your customers that their credit card data is highly protected and the transaction is supported by a Connected Payments system that provides superior security. Even without EMV

technology in place, our Connected Payments system uses point-to-point encryption, which provides one of the most secure payment architectures outside of EMV. EMV is a complement to an already strong security posture.

Q. Why is it taking so long to get the payment solution EMV ready?

A. There are many components and dependencies of a retailer's payment solution with multiple providers involved in an EMV certification, including payment solutions, PIN pad, and host processors. Additionally, each of the card brands - Visa, MasterCard, AMEX, Discover, and others - require individual certification each with its own set of very specific tests. NCR's certification letters are achieved with each individual card brand and are sponsored by the processors and acquirers. This multi-layer process can sometimes cause unforeseen delays.

Q. How can I learn more about EMV in general, and how can I access additional technical details regarding EMV implementation as it specifically relates to NCR Connected Payments?

A. You can visit http://www.emv-connection.com/downloads/2015/05/EMF-Liability-Shift-Document-FINAL5-052715.pdf to download a general Industry White Paper published by the EMV Migration Forum titled, "Understanding the 2015 U.S. Fraud Liability Shifts." NCR is not affiliated with the EMV Migration Forum and this information is provided solely for informational purposes. In addition, please review our EMV webinar at https://ncr.webex.com/ncr/ldr.php?RCID=1c8dfd8beb61df45f2614a7c4d7fd1ee.

You can find a comprehensive White Paper in the Connected Payments web portal that explains EMV as it relates to Connected Payments.

- Login to your Connected Payments web portal
- In the top right corner under "Help click on the "Customer Service" link
- In the Customer Service page, the first link provided is "EMV White Paper"

Q. What are the software requirements for going live with EMV and my POS/PIN pad?

A. Software requirements for EMV:

POS/PIN Pads	EMV Software Requirements
Verifone PIN Pads	• The latest OpenEPS.dll installed and running on the POS • The latest Verifone PIN pad Operating System from Verifone • The latest XPI component (must be licensed from your Verifone Rep). You may request the NCR EMV builds via the NCR support desk, or from Verifone directly • The latest PIN pad screen files from Verifone (if your screen files were originally signed by Verifone, you will need to retrieve EMV specific signed screens from your Verifone rep)
Ingenico PIN Pads	• The latest OpenEPS.dll installed and running on the POS • The latest RBA application from Ingenico (OS and application version information still being finalized)
Equinox PIN Pads	• The latest OpenEPS. DLL installed and running on the POS • The latest version of FPE application from Equinox (OS and application version information still being finalized)