openedge
A division of globalpayments

EMV® What OpenEdge Merchants Need to Know

With the liability shift date of October 1, 2015 quickly approaching, many businesses that accept card payments still have questions about what exactly happens on that date, what is changing based on EMV, and what it really means for them and their business.

EMV will impact different merchants in different ways. It will have virtually no impact on many businesses other than the way you physically process cards. The key is to understand what happens on October 1, 2015, how it is likely to impact your business, and your true level of risk relative to fraudulent card use.

We want to make sure you have the answers you need. We're here to support you as this technology is introduced to the US. We worked with OpenEdge to design this document to better enable you to understand how EMV will impact you and your business.

What Does the Liability Shift Really Mean for Merchants?

- Today, merchants do not carry any counterfeit fraud liability, it is all borne by the card issuers. Starting October 1, 2015 - the counterfeit liability shift is transferred to the merchant **only if a counterfeit of a chip card is used as a magstripe card at a non-EMV terminal**.

- After October 1, 2015, even if you are **not** EMV enabled, you are still not liable for ALL counterfeit fraud. **The counterfeiting of a magstripe card will remain the responsibility of the issuer**.

EMV Liability Shift – FAST FACTS

On/after October 1, 2015:

- **You will still be able to accept all cards whether they use an EMV chip or not**
- **EMV acceptance is not a mandate nor is it a law**
- **All cards – including EMV chip cards – will continue to process normally as magstripe transactions**

Understanding the TRUE cost of liability:

- **Merchants need to understand their fraud risk before making the decision to buy EMV-capable devices**
- **Although it varies by industry, the actual additional fraud liability for a merchant is likely to be very low – on average as little as $4 a month***

You are still in control:

- **EMV support is not a requirement to keep your business running, it is your choice to implement**
- **There is no need to panic over the October 1 deadline. This date does not represent the end, it is just the beginning.**

* Source: Internal data based on portfolio averages. Your liability level can vary based on a number of factors.

What Does Liability Cost You as a Merchant?

- Based on industry information, the liability shift will result in a typical merchant assuming an average of **0.02 bps** of additional fraud liability. **This is equivalent to $4 per month for a business processing $250,000 in annual credit card sales**[1].

- **While the actual dollar impact may be insignificant** (and varies by vertical market), OpenEdge still encourages most card-present merchants to eventually transition to EMV. The good news is that OpenEdge offers a multi-pronged security approach that goes beyond EMV to include additional security features such as point-to-point encryption, tokenization and NFC/Apple Pay™/Android Pay™ all within our security offering, EdgeShield. This provides one of the most secure and versatile processing solutions available today in addition to the fraud-reducing EMV chip technology. For more information on EdgeShield and the OpenEdge EMV solution, click here.

Is the Market Ready for EMV?

- **Not really. As of September, 2015, the overall payments market is falling behind the initial EMV chip penetration projections**. Only **4%** of the point of sale systems have been EMV-enabled so far. Approximately **7%** of the nation's ATMs can read EMV chip cards. As of July, only **18%** of all Visa-branded credit, debit and prepaid cards in the US contained an EMV chip[2]. This means that **currently, for the vast majority of credit and debit cards, you have no counterfeit liability whether you are EMV-enabled or not.**

How Does this Affect OpenEdge Merchants Still Processing on Legacy Platforms, such as the former PayPros Innovo Platform?

- Having been at the forefront of EMV innovation, OpenEdge acknowledges that enabling a large base of merchants for this technology is a significant challenge we all face. **OpenEdge's priority will remain getting merchants upgraded, and assisting with new device sales, deployment and configuration.** Accordingly, we are actively working with OpenEdge to migrate merchants from legacy platforms to the new OpenEdge platform. We are also deploying more migration-related resources to assist you when it comes time to upgrade, including EMV hardware ordering websites with FAQ content, automated utilities and communications, and streamlined fulfillment and Customer Care processes. OpenEdge is adding resources where appropriate, and doing all they can to accelerate adoption and activation of EMV equipment for those merchants desiring it.

What Does OpenEdge Recommend We Do Now?

- Please remember that OpenEdge's singular focus is to assist you in making this EMV transition seamlessly. However, it is clear that a transition of this magnitude will not be immediate. This migration was not designed to be completed prior to October 1, 2015, although OpenEdge will continue to move as many merchants to the new platform as quickly as possible.

- OpenEdge's recommendation for you is to **maintain your existing processing environment and allow the re-integration and migration process (underway between your software provider and OpenEdge) to complete the current beta phase**. OpenEdge will continue to provide more updates and timelines as soon as they are available relative to when you will be migrated to the new platform.

How Does This Affect Us Relative to the Liability Shift?

- The liability shift is only applicable in **card-present transactions when a new EMV chip card is being used, and only if that specific transaction is found to be fraudulent**. If you are not EMV-ready and a customer presents an EMV chip credit card, you should ask for a **second form of verification** before running the transaction.

- Even if you are not EMV-ready, **all EMV chip cards will still have a magnetic stripe** and can be swiped or keyed in manually.

- It is important that you should also evaluate your current chargeback liability and consider your typical customers to determine a temporary strategy for your business prior to EMV readiness. This strategy should take into account your expected EMV card fraud liability, which – as previously noted – averages around **$4 per month for a customer processing $250,000 in annual credit card sales**[1]. If you are not ready for EMV cards on October 1, you won't be alone - it is expected that the US EMV rollout will be gradual and continual with the majority of merchants not ready for EMV on October 1st.

[1] Source: Comparison of internal counterfeit fraud data and counterfeit fraud data provided by Visa across all vertical markets served by First Data/Innovo, 2015. This is a portfolio average – your actual risk could vary significantly based on multiple factors.
[2] Source: Data provided by Visa to *Digital Transaction News*, September, 2015.