Are you prepared for the EMV liability shift in October 2015?

As the liability shift draws closer, some merchants are asking what the consequences are of not meeting the deadline while others are weighing the impact, scale and cost of the effort necessary

Retail & Consumer
Payments Consulting
May 2015

On October 1, merchants will assume liability for counterfeit card fraud if they are not able to process chip card transactions at their POS locations

A Historic Liability Shift

Short for Europay MasterCard Visa, EMV is the name for the global specifications that govern issuance and acceptance of payment cards with embedded microchip technology. While most of the world converted from magnetic stripe-based plastic to "chips cards" years ago, the U.S. was a lone holdout . . . until now.

Effective October 1, the payments value chain entity that does not support EMV in the U.S. will assume liability for counterfeit card transactions**.** For the first time, merchants that process card-present transactions at point of sale (POS) locations can be liable for losses that are currently borne by card issuers.

The magnitude of the liability exposure depends on many factors such as the number of EMV cards issued in the market, historical counterfeit card fraud rates and chargeback ratios seen by merchants.

Tools to Define Impact

Based on our work with clients, PwC has developed tools and accelerators that can help merchants assess their liability exposure and understand the scope, cost and critical pathways to achieving EMV compliance.

Determining a Path Forward

By understanding both sides of the coin, liability risk vs. the cost and impact of implementation, merchants can document the business case for EMV and make informed decisions about the future.

pwc

What is Your Liability Exposure?

As the percentage of cards issued with an EMV chip rises, so too does a merchant's exposure to counterfeit fraud if it is not EMV ready. Liability exposure is driven by a merchant's card-present sales, the percentage of EMV ready cards used at its locations and the amount of chargebacks related to counterfeit card fraud. An estimated 70% of issued credit cards in the U.S. are expected to be EMV ready by the fourth quarter (Q4) of 2015 and 90% by Q4 of 2016, according to Aite Group.

To give a hypothetical risk scenario: if a merchant has total annual POS credit card sales of $2 billion, its annual liability exposure beginning in Q4 2015 could be $700,000 and that liability could rise to $900,000 annually by Q4 2016.

These estimates represent counterfeit credit card fraud liability only and do not include resource costs, fees and expenses for processing chargebacks. Also not included is liability associated with EMV debit cards or any of the consequences that may result from the expected shift in focus by malicious parties on to merchants that are not EMV compliant.

Scoping out the EMV implementation effort

To move to an EMV ready environment, most components in a merchant's payments operation have to be updated or replaced and then certified to accept chip cards and pass EMV messages. Components impacted include PIN Entry Devices (PEDs), POS software, in-store processors, gateways and switches.

There are 10 key questions merchants should ask themselves when evaluating their EMV readiness.

Ten Questions that Will Help You Size the EMV effort

1. Are PIN Entry Devices (PEDs) in card-present locations EMV capable and do you accept PIN debit today?
2. Do you have registers or POS devices away from customer view?
3. Do you require or desire mobile PEDs in your card-present locations?
4. How many different types of POS software do you use across locations?
5. Is your POS software EMV ready or has the vendor committed to a delivery date and cost?
6. Do you have In Store Processors (ISPs) or other middleware? If so, are they EMV ready?
7. Do you utilize any homegrown systems to route transactions to your acquirer/processor? Are those EMV ready and certified?
8. Do you leverage any 3rd party components such as a commercial switch or gateway? Are those components EMV ready and certified?
9. How many acquirers, processors and other authorizers do you have?
10. Are you currently authorizing on the platform your processor has designated and certified for EMV?

What Are The Other Risks to Waiting?

Although there are currently no card network brand requirements that demand that merchants be EMV compliant, there are additional risks beyond the liability shift to consider:

- Merchants that employ the traditional retail systems "freeze" period, limiting changes to critical systems during the holiday season, will have prolonged liability exposure potentially well into 2016.
- Merchants that are not EMV compliant will likely be targeted by criminals who are passing cards with counterfeit magnetic stripes, increasing fraud liability.
- Merchants may face resource unavailability and supply crunches for hardware and other solutions.
- Unavailability of key resources at partners and vendors can delay EMV certification timelines.
- Higher costs may be imposed on non-EMV ready merchants if there is a shift in regulation that favors EMV ready merchants.
- As EMV technology becomes more widespread, issuers may retire magnetic stripe cards and only issue EMV enabled chip cards.
- The ability to accept NFC based mobile payments may be delayed as EMV and mobile transactions require similar payments infrastructure and standards.

These considerations are important to evaluate when assessing the risks of delaying or foregoing EMV implementation.

For more information, please contact

Steve Barr
(415) 498 5190
steven.j.barr@us.pwc.com

Kevin Grieve
(303) 601 4805
kevin.c.grieve@strategyand.pwc.com

Gregory Holmes
(415) 498 7435
gregory.holmes@us.pwc.com

Ron Kinghorn
(617) 530 5938
ron.kinghorn@us.pwc.com

Andrew Luca
(646) 335 4649
andrew.j.luca@us.pwc.com

Bryan Oberlander
(617) 530 4125
bryan.s.oberlander@us.pwc.com

PJ Ritters
(612) 596 6356
paul.j.ritters@us.pwc.com

© 2015 PricewaterhouseCoopers LLP. All rights reserved. PwC refers to the United States member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.