

DAYTON BUSINESS JOURNAL

Guest Column: EMV Chip Credit Cards: Are businesses or banks liable for credit-card fraud?

ANA CRAWFORD
Porter Wright Morris & Arthur LLP

There is a new and potentially costly liability issue for retailers. As of Oct. 1, 2015, there was a shift in liability from credit card issuers being responsible for fraud, to merchants, such as your favorite neighborhood coffee shop, being responsible for fraudulent transactions when magnetic credit card strips are swiped at a reader that is not EMV chip-enabled. The EMV chip is widely used in other countries, and its recent implementation in the United States is expected to prevent fraud by creating a singular authorization code each time the card is used rather than a card using the same code with each transaction. This would prevent the reuse of account information in a subsequent data breach and increase protection for consumers.

This liability shift applies to the vast majority of credit card issuers, including Accel, American Express, China UnionPay, Discover, MasterCard, NYCE Payments Network, SHAZAM Network, STAR Network, and Visa.

Because the majority of credit card issuers are changing their policies with regard to liability, almost all businesses selling directly to consumers will be affected, with a few important exceptions. EMV chip card technology only applies at physically read terminals, so online businesses would not be affected by the liability shift. Any fraud associated with online or payments by phone would still be the responsibility of the credit card issuer. Additionally, major credit card companies have specifically granted an exemption to gas stations and ATMs until Oct. 1, 2017, to make the switch.

Another important nuance of this new rule is already causing confusion among small retailers and consumers. Businesses that do not use traditional cash registers or payment terminals and do not have an EMV reader are still affected by the liability shift. Since any merchant that accepts a physical credit card is responsible, so too is that cof-

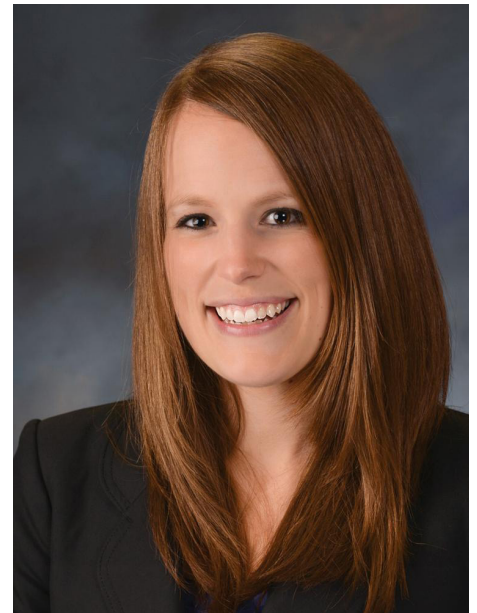
fee shop you like to frequent, even though they use Square or other mobile technology.

Now that the shift has occurred, businesses that previously were not liable for fraudulent transactions will be liable for fraudulent transactions if they do not use EMV chip-enabled readers. Liability hinges on whether or not a store is EMV-ready. So, generally, if a chip-card is used fraudulently and the merchant has EMV capability, then the card issuer will be liable for the fraudulent purchase, no matter if the EMV reader was actually used. If a merchant does not have EMV readers, then the merchant is responsible for any fraudulent transactions occurring during in-person transactions.

However, liability for lost or stolen cards likely depends on the type of credit card used. Visa's policy, for example, is that for lost and stolen cards, there is no change in liability, and the issuer is still responsible. One exception, for MasterCard, American Express or Discover cards, is if a fraudster uses a PIN credit or debit card and the business did not have the capacity to process the card as an EMV chip card rather than the magnetic chip. In this case, the merchant would be liable because the PIN and EMV chip reader may have prevented the fraud.

In order to become EMV capable, that favorite coffee shop or any other business must purchase EMV-enabled terminals, and then must undergo a certification process for each credit card network. Card readers with the capacity to read both magnetic strips and EMV cards are available for purchase, with some selling for under \$50. Even mobile technology companies are in the process of developing EMV readers for their users.

It is important to note that while there is no actual requirement for businesses to switch to EMV chip readers, the potential for liability certainly increases for those businesses that fail to update their readers. It is likely that retailers with higher-value items that are easy to pawn or resell, like electronics or jewelry, will be most affected and are



Ana Crawford is an associate at Porter Wright Morris & Arthur LLP

at the highest risk for financial liability associated with this change. Businesses in these industries should consider the potentially costly ramifications of not making the switch quickly.

Ultimately, it is up to each individual business to perform a cost-benefit analysis to see whether the potential for liability is greater than the cost to implement the new readers, but businesses should be sure to investigate the option in order to protect themselves as well as consumers. If the research is not done and the right precautions are not taken, both consumers and merchants could find everyday purchases, such as a simple cup of coffee, costing them much more than they had bargained for.

porterwright
PORTER WRIGHT MORRIS & ARTHUR LLP