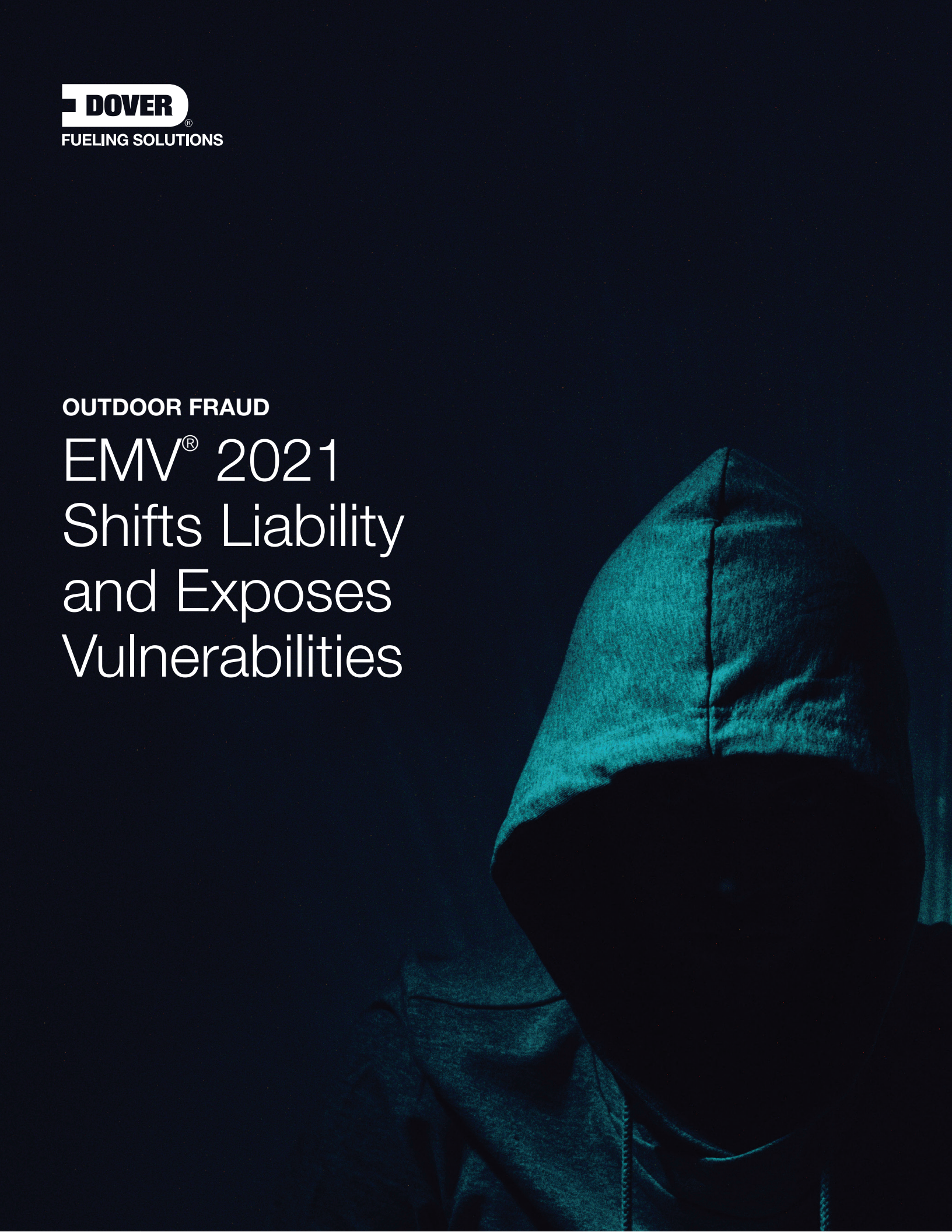
DOVER
FUELING SOLUTIONS

OUTDOOR FRAUD

# EMV® 2021 Shifts Liability and Exposes Vulnerabilities



Visit **www.doverfuelingsolutions.com/EMV** to learn more.

# What is your revenue and your reputation worth? How would you like to lose a big chunk of both?

Rampant card skimming steals customers' payment data and currently costs card issuers nearly $3 million a day. In addition to using stolen data to make fraudulent purchases, skimmers produce counterfeit cards for use at unsecure payment terminals. In April 2021, fuel retailers who haven't made the switch to EMV® compliant card readers will be on the hook for the entire cost of those charges – $400 million a year in the U.S. retail fueling market alone. Plus, organized crime will put a bullseye on unsecured automated fuel dispensers at retailers who miss or ignore the deadline.

Payment card fraud is pervasive across the United States, but the widespread adoption of EMV chip cards from mag-stripe cards has significantly reduced fraud for most merchants. Fuel retailers, however, are behind in adopting the new technology and are facing pressure on two fronts: increased vulnerability and the upcoming liability shift.

Fuel retailers are low-hanging fruit for criminals using skimmers to grab data off of mag-stripe cards. The thieves – who now include multiple organized crime rings based in Cuba along with Russian and Eastern European gangs – are coordinated and sophisticated, with state-of-the-art technology that's easy to install and hard to detect.

Having found an easy target, the bad guys won't stop skimming in April 2021. They will simply shift their focus to merchants who are still using non-EMV compliant dispensers. With an educated consumer base aware of the weaknesses of mag-stripe cards, those merchant locations will inevitably become suspect and lose customers.

This is on top of the fast-approaching deadline for the liability shift. All indications are that the 2021 date – which was delayed by Visa and Mastercard to accommodate challenges for fuel retailers – will not be moved again. There is simply too much at stake in the payments ecosystem, with card issuers having invested heavily in EMV technology to reduce counterfeit card fraud.

## FUEL DISPENSERS MAIN TARGET OF OUTDOOR FRAUD

Credit card fraud, including skimming, is a federal offense and carries stiff penalties including heavy fines and lengthy prison sentences. As a federal crime, it attracts the attention of the U.S. Secret Service, which estimates that criminals steal $1 billion every year using skimming devices.

The two main targets: ATMs and fuel dispensers. That's because other types of skimming fraud are harder to commit. Most retail point-of-sale terminals have converted to chip card readers and many that still take mag-stripe cards are in busy areas with security camera surveillance, making it difficult for criminals to install skimming devices.

Anti-skimming technology has been widely adapted in ATMs with only 9% of automated teller machines in the U.S. not yet EMV compliant, according to the ATM Industry Association. That leaves unattended fuel dispensers as the easiest available target. Matt Schulz, chief industry analyst at CompareCards, said, "Gas stations are the lowest-hanging fruit for bad guys when it comes to skimming."[1]

Secret Service special agent Matthew O'Neill said, "Gas pump skimmers are getting worse because there's more technology to look for skimmers in ATMs, so bad actors move towards gas pump skimmers." He estimates that the agency recovers 20 to 30 skimmers a week, each holding information for about 80 payment cards.[2]

As with other types of fraud technology, skimmers are becoming more sophisticated, adding Bluetooth and wireless network signals to transmit skimmer data to cell phones anywhere in the world, as well as shrinking to a size that can be nearly impossible to detect. "They're easy to create, easy to deploy and can get a lot of credit card data very quickly," O'Neill said.

Among the challenges to combating this crime is that the skimmers are placed inside of the fuel dispenser, making it virtually impossible to know there's a skimmer inside. The devices also are connected to the dispenser's electric power, so they don't need batteries and can operate indefinitely. It's also difficult to track the data transfer – all adding up to a crime that is hard to prosecute.

For their part, most consumers are on to the scam due to an increasing number of news reports. In a survey by CompareCards, 15% of Americans who purchased gas recently believe they've been a victim of skimming at the pump. Millennials are more likely to say they've been scammed, with just over 20% saying they've been victims of skimming at the pump in the last year. That's compared to about 15% of Gen-Xers and just 8% of Baby Boomers.[1]

68% of U.S. adults who experienced payment card fraud related to card skimming said they have changed the way they pay for gas, according to a 2018 survey by CompareCards. Almost half of card-skimming victims said they use a credit card to pay more often for gas, while 39% said they now pay for gas inside the station, and 16% said they use cash more often.

# Skimming Fraud at Fuel Dispensers is a Nationwide Issue

Fuel merchants across the country are regularly targeted. This is just the tip of the iceberg:

- A 12-person organization in Colorado racked up an average of $2.5 million per week in fraudulent charges to credit card numbers stolen from gas pumps.[3]
- Florida's Department of Agriculture and Consumer Services found 588 skimmers in gas pumps throughout the state just five months into 2019, adding to the total of 2,400 skimmers removed statewide since 2015.[5]
- Kentucky Department of Agriculture inspectors uncovered a skimming scheme in 2019 that compromised more than 7,000 unique card numbers at several Louisville-area retail locations, leading to the arrest of eight people.[6]
- In October 2017, authorities in Boulder, Colorado, busted a skimming ring that victimized people in Colorado, Illinois, Ohio and several other states.[7]

Hal Prince, chief of Florida's Bureau of Standards – which has its own enforcement personnel – said the state has pursued, arrested and convicted high-profile cases. However, time-consuming coordination between the bureau and federal and local law enforcement can mean lost revenue and paperwork for station owners and service technicians, as well as weights and measures officials.[8]

Making arrests in skimming cases is difficult, but not impossible. Efforts led by special agents and investigative analysts of the Secret Service are continuing to work closely with state and local law enforcement partners around the country to keep the public informed and apprehend those who are responsible for credit card skimming.[9]

Responsibility undoubtedly also falls on fuel merchants to secure their dispensers. At a recent petroleum industry seminar, Lt. Marcus Booth, Financial Crimes Unit Director of the San Antonio Police Department said they experienced a threefold increase in skimming crime from 2017 to 2018 and pointed to an industry-driven solution. "It's critical for merchants to secure their pumps from intrusion or upgrade pumps to eliminate the problem," he said. "We have yet to see a newer pump with encrypted electronics breached."

## A NATIONWIDE CRIME OF OPPORTUNITY

There is no honor among thieves. But there is competition. The National Association of Convenience Stores estimates that 37 million Americans refuel each day and over 29 million use a credit or debit card. Criminals look at those numbers and see dollar signs. Skimming fraud is moving to where the money is, and the ease of the crime is attracting coordinated, sophisticated criminals belonging to Cuban crime syndicates and the Russian mob.

Cuban crime rings have been uncovered from Wisconsin to Alabama and from Florida to Arizona, according to media reports. After apprehending criminals who stole hundreds of card numbers at gas stations across the Phoenix metro area in May 2019, Arizona Attorney General's Office spokesman Ryan Anderson said, "We believe these individuals are part of a larger criminal network associated with Florida-based Cuban organized crime. We know that these groups are now present in a majority of states, including Arizona."[3]

Also in May 2019, Texas Agriculture Commissioner Sid Miller said there is evidence of involvement by Russian organized crime in skimming. "We are finding a lot of them. We are cracking down on them. It's mainly mafia driven. Foreign mafia groups."[4]

## COMBATING OUTDOOR FRAUD WITH EMV TECHNOLOGY

EMV (Europay, Mastercard and Visa) technology can significantly curtail theft and protect fuel merchants from liability for losses. EMV cards feature a microprocessor chip that verifies the card, authenticates the cardholder and authorizes a transaction with a unique set of digital instructions – encrypting the confidential information and dramatically reducing the risk of card counterfeiting and fraud.

The U.S. payments industry began to shift to EMV chip cards in 2011. One of the primary selling points to get merchants to adopt their POS terminals to accept chip technology was its effectiveness in reducing counterfeit fraud, which was the primary type of fraud in the United States at the time.

Fraud losses due to counterfeit, stolen and lost cards hit an all-time peak of $5.4 billion in 2016, but plummeted to $3.9 billion in 2017 once merchants started to accept chip cards, according to data from Aite Group.

Criminals steal $1 billion every year using skimming devices.

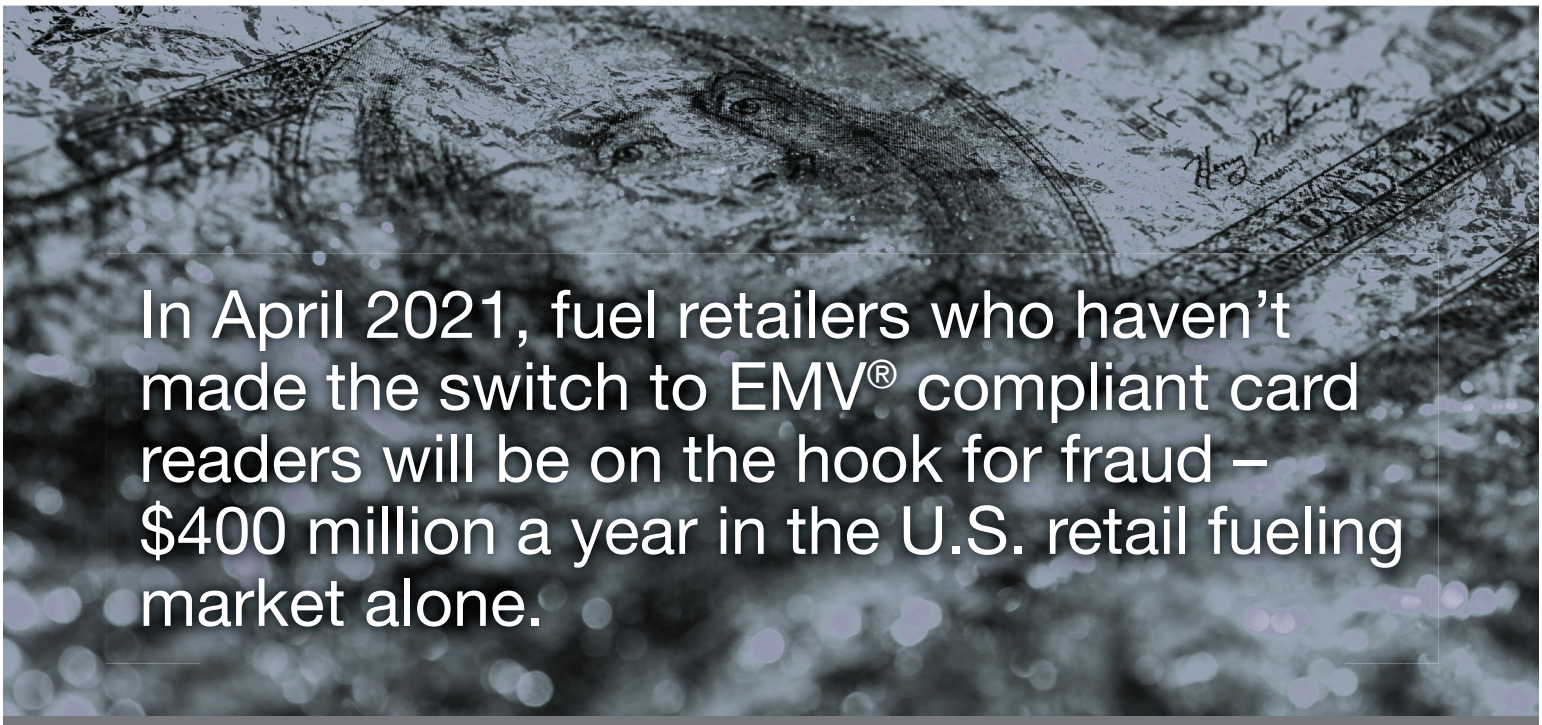
## EMV PUTS A SERIOUS DENT IN FRAUD

EMV chip cards and chip-activated merchants combat counterfeit fraud in the U.S.[10]

- For merchants who have completed the chip upgrade, counterfeit fraud dollars dropped 80% in September 2018 compared to September 2015.
- Over 3.1M merchant locations are now accepting chip cards. That's a 692% increase since the beginning of EMV migration in the U.S.
- Visa chip cards have increased by 221% since September 2015, from 159 million to 511.1 million cards.
- 98% of overall U.S. payment volume in December 2018 was on EMV cards.

While Visa has been working with merchants, acquirers and fuel industry providers to support migration to the more secure EMV technology, some of the same migration challenges the industry faced when the liability shift deadline was delayed still persist to varying degrees. Visa is monitoring industry progress and attempting to proactively address marketplace realities and known challenges wherever possible, noting unique challenges for the fuel industry, including:

- U.S. regulatory requirements that do not exist anywhere else
- The complicated infrastructure and specialized technology required for automated fuel dispensers
- A shortage of service technicians to install the equipment
- A backlog in getting equipment on time
- Communication integration with the POS system
- Cost to upgrade



The cost of conversion is perhaps the biggest hurdle for fuel merchants. There's no doubt that making a fueling facility EMV-compliant inside and out can be expensive. The number and age of a site's dispensers, network bandwidth, fuel volumes and average transaction size are all variables that can cause costs to vary from a few thousand dollars for a small site to tens of thousands of dollars for a larger one.

According to Fuels Market News, the wholesale replacement of the physical payments infrastructure for a typical gas pump forecourt with six dispensers could cost about $30,000 to become EMV-compliant. That can be further complicated by multiple types of outdoor terminals, fuel forecourt controllers and one or more electronic payment server applications.

"If the pump cannot accept an EMV upgrade kit, replacement — including new machines, infrastructure changes and labor – can cost more than the average profit an independent fuel merchant will see in a year," wrote Worldpay Enterprise Relationship Manager Glenda Preen.[11]

All of this has led some fuel retailers to take a wait-and-see approach. "However, fuel merchants need to understand that, in the end, there is more to gain than lose with the upgrade to EMV-enabled pumps," Preen said.

## REASONS TO CONVERT

In addition to EMV technology being proven to prevent counterfeit fraud, chip cards also lay the foundation for future payment systems, including mobile payments, biometrics and risk-based authentication.

### Combat Fraud Today

- More than 1.7 million merchants representing over a third of storefronts are now accepting chip cards, according to Visa
- 388 million Visa chip cards have been issued in the U.S.
- Chip-enabled merchants are seeing a 43% reduction of counterfeit fraud

### Reduce Liability Tomorrow

- Reduced fraud-to-sales ratios, amount and number of counterfeit fraud chargebacks, saving significant dollars
- Individual card brands – including Visa, Mastercard and American Express – could impose significant fines on any non-compliant merchants in the event of a breach

### Enjoy Future Advantages

- The benefits of a competitive advantage from offering safe and secure transactions
- New equipment is more advanced and feature-laden, yielding more for your investment
- Readiness for next generation payment systems like contactless cards and wearables

“I would recommend people start now and have a plan in place. Allow some time for bug resolution.”

Mark Gruggett,
Director of Construction
The Kroger Company

## THE IMPORTANCE OF STARTING NOW

The larger your operation, the more complicated it is to decide when and how to upgrade. Others who have been through it say the more complex the decision, the sooner the planning should start.

Mark Gruggett, Director of Construction at The Kroger Company said, "I would recommend people start now and have a plan in place. Allow some time for bug resolution." He added Kroger started the conversion to EMV before the initial deadline for compliance was moved.

"We did it for the mitigation of fraud and anticipated effect of liability. We knew it would be a long trek, because we had 8,000 to 9,000 dispensers. And you know how IT functions work – things got bogged down."

Gruggett's advice is to look at your options, set priorities, create budgets, and get started now. The longer you wait, especially during a technician shortage, the more likely you'll be at the back of a very long line.

The incentives for upgrading ahead of the April 2021 deadline go beyond avoiding responsibility for counterfeit fraud chargebacks, according to Chelsea Regan, Assistant Editor of Convenience Store News. "Doing so will allow companies to get up-to-date on next-generation hardware and software, get better access to equipment and technicians, refresh their image and, of course, protect customers."[12]

## TURN TO SOMEONE YOU TRUST

The long-term cost of not being capable of chip card acceptance has the potential to be significantly higher than the cost of the upgrade itself. Partnering with a fuel equipment manufacturer whose product portfolio supports an upgrade path gives retail fuel operators a measure of flexibility.

Since EMV payments are the foundation and the future of payment acceptance, and the liability shift deadline will not move again, choose to work with a reliable expert on all things EMV who can help you with everything you need to know for a smooth upgrade. Dover Fueling Solutions (DFS), a global leader in fuel dispenser products and software, offers a range of hardware and software solutions for making the transition to EMV as easy and cost-effective as possible—no matter your particular road to compliance.

To avoid the backlog caused by the last-minute conversion rush, get started early by contacting your local DFS distributor. A representative will visit your site and gather the necessary information to develop a custom EMV conversion plan. It will be based on your current hardware and software needs and will help you coordinate logistics for a seamless transition.

Visit **www.doverfuelingsolutions.com/EMV** for more information and to find your local distributor.

**SOURCES**


[1] CBNC.com, August 23, 2018. “1 in 5 millennials say they’ve been scammed at the pump in the past year.” By Megan Leonhardt, CNBC Make It.

[2] NBCNews.com, Nov. 23, 2018. “Secret Service cracks down on credit card skimming at gas pumps nationwide.” By Didi Martinez, Amy Calvin and Cydney Weiner.

[3] AZCentral.com, May 10, 2019. “Cuban crime ring may have stolen your credit card number from an Arizona gas station.” Rebekah Sanders, Arizona Republic.

[4] EastTexasMatters.com, May 14, 2019. “State investigators say foreign mafias are skimming at Texas gas stations.” By Alex Caprariello.

[5] Spacecoastdaily.com, May 12, 2019. “Florida Leaders Target Gas Pump Skimmer Fraud, Need for Stronger Consumer Protections.” By Space Coast Daily.

[6] Wtvq.com, May 13, 2019. “State on the Lookout for Credit Card Skimmers at Gas Pumps.” By Tom Kenny, ABC26, WTVQ, Lexington, KY.

[7] CBS 4 Denver, October 19, 2017. “Cuban Nationals Arrested In Bust of Gas Station Skimming Ring.” By Jamie Leary.

[8] PEI Journal, Second Quarter 2018. “Skimmers Dominate 2018 NCWM Interim Meeting.” By J. Rex Brown.

[9] Secretservice.gov, November 22, 2018. “U.S. Secret Service Serves up Cold Dish of Justice to Gas Pump Skimmers.” United Stated Secret Service press release.

[10] U.S. card figures are estimates based on the number of active cards per VisaNet data and operating certificates provided to Visa by client financial institutions as of the end of December 2018. Merchants that have completed an EMV transaction in the last 30 days considered chip-activated; Counterfeit fraud reduction at fully chip-enabled U.S. merchants for the quarter ended September 2018 compared to the quarter ended September 2015. Decline in counterfeit fraud dollars for all U.S. merchants in the quarter ended September 2018 compared to the quarter ended September 2015 includes chip-enabled and non-chip-enabled merchants. Fully chip-enabled merchants defined as locations where 75% of card present payment volume is chip-on-chip. Data includes both U.S.-issued credit and debit cards; Transaction number and volume based on VisaNet data for U.S. locations with chip transactions as of end December 2018. Overall U.S. payment volume on EMV cards includes transactions made on all terminals (chip-enabled and non-chip).

[11] Fuels Market News, “To EMV or Not to EMV: The Fuel Merchant’s Question,” November 1, 2018. By Worldpay Enterprise Relationship Manager Glenda Preen.

[12] Convenience Store News, October 11, 2017. “C-stores Must Ready Themselves for EMV 2020.” By Chelsea Regan.

# We’re in your corner.

Visit **www.doverfuelingsolutions.com/EMV** for resources to help plan and implement your transition to EMV.

DOVER®
FUELING SOLUTIONS