U.S. Automated Fuel Dispenser EMV Liability Shift Delayed

EMV Liability Shift:

The EMV liability shift is designed to better protect all parties. With the new rules, the party that is the cause of a chip transaction not occurring, either the issuer or acquirer, will be held financially responsible for any resulting card-present counterfeit fraud losses.

- ✔ Issuers assume counterfeit fraud-related liability if a non-chip card is presented at a chip-capable terminal.
- ✔ Acquirers assume counterfeit fraud-related liability if a counterfeit chip card is presented at a non-chip-capable terminal.

New Visa Fraud Monitoring Program for Automated Fuel Dispensers

Visa has been working with merchants, acquirers, and fuel-industry providers to support migration to the more secure EMV technology. However, due to challenges with EMV Automated Fuel Dispensers (AFD) solution readiness, Visa is delaying the U.S. domestic AFD EMV liability shift date to **1 October 2020**.

To help mitigate any increases in counterfeit fraud at AFDs in the interim, Visa will expand its existing Visa Fraud Monitoring Program (VFMP) to include a new U.S. AFD-specific fraud-monitoring program. The expanded program will have unique thresholds based on U.S. AFD counterfeit fraud trends. For AFD locations that exceed the defined thresholds and reach enforcement status, issuers will receive chargeback recovery rights for reported counterfeit fraud. The new AFD fraud-monitoring program will begin in **July 2017**, identifying fraud in June 2017, the previous month.

VFMP-AFD Program

U.S. domestic transactions only

Program Basics

The VFMP-AFD program applies only to U.S. domestic transactions at AFDs (Merchant Category Code 5542). The VFMP will continue to operate as currently defined in the Visa Rules (ID#: 0029288).

Visa will notify U.S. acquirers of all the AFD merchant outlets in their portfolios, which are identified in the VFMP-AFD through the Visa Risk Performance Tracking (VRPT) tool available on Visa Online.

Just as with the existing VFMP, the VFMP-AFD will review the previous calendar month's domestic counterfeit fraud dollar totals and the domestic counterfeit fraud-to-sales ratio. However, the thresholds for VFMP-AFD are specific for and apply only to U.S. domestic AFD transactions.

Standard Program

U.S. AFD merchant outlets will be identified on a monthly basis if they meet or exceed the program's "standard" thresholds for counterfeit fraud activity in the previous calendar month, as follows:

- $10,000 in U.S. domestic counterfeit fraud AND
- 0.20 percent U.S. domestic counterfeit fraud amount to domestic sales amount ratio

Excessive Fraud Program

U.S. AFD merchant outlets will be identified on a monthly basis if they meet or exceed the program's "excessive" thresholds for counterfeit fraud activity in the previous calendar month, as follows:

- $10,000 in domestic counterfeit fraud AND
- 2.00 percent domestic counterfeit fraud amount to domestic sales amount ratio

VFMP-AFD Program Timelines

VFMP-AFD Standard Program Timeline

The VFMP-AFD program timelines mirror the existing VFMP program timelines. The following table summarizes the VFMP-AFD **Standard Program timeline**, with more detail available in the Visa Rules. The Standard Program will begin in **July 2017** (identifying fraud in June 2017, the previous month).

ACQUIRER ACTIONS / PROVISIONS BY PROGRAM MONTH	
Program Month 1: Notification *(e.g., July 2017)*	• Visa identifies merchant locations that exceed the program thresholds for fraud in the previous month (e.g., June 2017). • Visa notifies the acquirer that it has a merchant location in the program. The acquirer must notifiy the merchant, review the merchant's activity, and take appropriate mitigating steps.
Program Months 2-4: Workout Period *(e.g., August through October 2017)*	• Acquirers work with merchant locations to take action to reduce fraud levels below at least one of the listed thresholds.
Enforcement Period: Months 5+ *(e.g., November 2017 onward)*	• If the merchant location reduces fraud levels for the previous month (e.g. October 2017) below at least one of the listed thresholds, they will not be subject to Reason Code 93 chargebacks for counterfeit fraud. • If the merchant location is not able to reduce fraud levels below at least one of the listed thresholds, they will be subject to Reason Code 93 chargebacks for counterfeit fraud.

Note: Member Appeal Rights do not apply to the release of Reason Code 93 chargebacks.

VFMP-AFD Excessive Fraud Program Timeline

ACQUIRER ACTIONS / PROVISIONS BY PROGRAM MONTH	
Program Month 1: Counterfeit Liability *(e.g., July 2017)*	The VFMP-AFD **Excessive Fraud Program timeline** differs from the Standard Program Timeline in that merchant locations will be subject to Reason Code 93 chargebacks for counterfeit fraud immediately, in Month 1. The acquirer will not be subject to non-compliance assessments. The Excessive Fraud Program will begin in **November 2017** (identifying fraud in October 2017).
Program Workout Period *(through remediation)*	Once a U.S. AFD merchant outlet exceeds the Excessive Fraud Program threshold, that merchant will remain on the Excessive Fraud Program timeline until it remediates out of the program altogether. In addition: • Visa may escalate a U.S.-acquired AFD merchant outlet from the Standard to the Excessive Fraud Program timeline if it determines that the merchant poses a threat the Visa payments system. • Any U.S. AFD merchant outlet that re-enters the program within 12 months of completing remediation will automatically escalate to the Excessive Fraud Program timeline.

VFMP-AFD Program Duration

The VFMP-AFD program is scheduled to end in October 2020 for fraud identified in September 2020. After the VFMP-AFD terminates, AFDs will revert to monitoring under the terms of the existing VFMP as defined in the Visa Rules (ID#: 0029288). The existing VFMP remains unchanged and will continue to monitor fraud during the extension period.

Remediation for Identified Merchants

Working together to mitigate fraud.

As with the existing VFMP program, Visa will consider remediation successful if the merchant can remain below at least one of the listed standard thresholds for three consecutive months.

If the merchant is unable to reduce its counterfeit fraud levels below program thresholds 12 months after it has entered the program, it may lose Visa acceptance privileges. In cases of egregious counterfeit fraud activity, Visa may impose Member Risk reduction requirements on the acquirer, as outlined in the Visa Rules (ID#: 0005057), to expedite remediation efforts or require that Visa acceptance privileges be terminated immediately.

Merchants are encouraged to work with their acquirers; and acquirers are encouraged to work with high-fraud merchant outlets to identify and implement solutions to mitigate fraud. U.S. AFD merchants can implement a number of tools and services to help mitigate fraud, including Visa Transaction Advisor (VTA), Address Verification Service (AVS), and Transaction Velocity Controls. Visa has published guides, listed in the Additional Resources section below, with best practices on acceptance and minimizing fraud risks.

FAQs

Q.
How can AFD merchants attempt to mitigate fraud at the pump or in-store?

A.
Merchants are strongly encouraged to use available fraud-reduction tools, including VTA and AVS, to mitigate fraud in the interim period. Merchants can also run an active velocity strategy at the account level across the chain, if possible.

Q.
Since the liability shift delay is domestic only, is Visa doing anything to help protect merchants from cross-border fraud?

A.
Use of the AVS and VTA tools will help merchants identify and handle high-risk transactions. Because AVS has limited application for cross-border transactions except for cards issued in Canada, the net effect is that most cross-border customers at AFDs who use AVS will be directed in-store, where they will complete the transaction (preferably at an EMV terminal).

Q.
What will Visa do to manage potential issuer abuse of chargeback rights on lost and stolen fraud?

A.
Visa monitors issuer fraud reporting and related chargeback activity and will take appropriate action if anomalies are detected.

Q.
What are the compliance assessments associated with each level (standard vs. excessive) under Visa's fraud monitoring program?

A.
There are no monetary compliance assessments but Issuers will have chargeback rights. Issuers will be notified to submit RC93 chargebacks to the merchant's acquirer.

Q.
Does the fraud monitoring include fraud from both inside and outside, or is it only including fraud at the fuel pump outside?

A.
The monitoring is only for AFD transactions.

Q.
What is the cure period for the Visa fraud-monitoring program, and is there a consequence if a location is identified under the Excessive Fraud Program multiple times in a year?

A.
A merchant location is considered successfully remediated if it is below at least one threshold for three consecutive months. Any location that re-enters the program within 12 months of completing remediation will automatically escalate to the Excessive Fraud Program timeline.

Q.
What type of notification will be provided before chargebacks can be initiated to merchants—for example, 30 days past exceeding the threshold? Or will chargebacks be immediate?

A.
There is a warning and remediation period for the Standard Program before chargebacks can be initiated. For the Excessive Fraud Program, there is no warning and remediation period.

FAQs (continued)

Q. **Will the VFMP provide fraud detail for both VFMP and non-VFMP locations?**	**A.** No, only identified locations.
Q. **What type of fraud reporting is available for monitoring and analysis?**	**A.** Not available.
Q. **Are there specific requirements or preventive measures to be removed from the VFMP?**	**A.** A location is considered successfully remediated if it is below at least one threshold for three consecutive months.
Q. **Are there any exceptions to the VFMP threshold? For example, would use of AVS or VTA allow for a relaxed threshold?**	**A.** No. The use of Visa Fraud mitigation tools will not provide any VFMP exceptions.
Q. **How is the payment process going to be handled for merchant locations in New Jersey and Oregon, which do not allow drivers to pump their own gas?**	**A.** The program looks at AFD MCC 5542 transactions regardless of whether the cardholder pumps their own fuel.
Q. **Which fraud reason codes will be included in EMV Liability Shift? How are Lost/Stolen transactions affected?**	**A.** Chargeback Reason Code 62—Counterfeit fraud pertains to the EMV liability shift. Issuers will not have the ability to submit lost/stolen fraud chargebacks for chip-on-chip (contact or contactless) AFD transactions.
Q. **Are there any incentives under consideration to assist in offsetting the significant investment required for EMV support—for example, higher transaction limits at the pump, fee or interchange reduction?**	**A.** There are no incentives other than that merchants will not have lost/stolen fraud liability for chip-on-chip (contact or contactless) on AFD transactions.
Q. **Will EMV support be managed as a liability shift or a mandate in 2020?**	**A.** The U.S. AFD EMV deployment is only being managed as a counterfeit fraud liability shift, not a mandate.
Q. **How does the VFMP affect the EMV Liability Shift Delay for locations that have greater than 20bps of counterfeit fraud?**	**A.** Identification by the VFMP does not impact the Oct 2020 EMV liability shift date.

Next Steps & Questions

For further details, please contact your acquiring back, processor, or Visa representative today.

Additional Resources:

- *Counterfeit Fraud Mitigation Tools for AFD Transactions—Fuel Merchants Who Are Not EMV Chip Enabled*
- *Visa Payment Acceptance Best Practices for U.S. Retail Petroleum Merchants*