© 2021 The Merchant Advisory Group

MERCHANT BEST PRACTICE GUIDE

PETROLEUM FRAUD PREVENTION BEST PRACTICES

Version 1.0
1/11/2021

QUICK OVERVIEW	
Also Known As	Petro AFD Fraud, Petro AFD Liability
Audience	Petroleum merchants looking for best and recommended practices to minimize the impact prior and subsequent to the EMV liability shift

This guide is made available for informational purposes only. Merchants should always make their own independent business decisions based on their best interests. This guide is not intended to be legal, financial, or risk management advice. The MAG has made efforts to ensure the accuracy of this information as of the date of publication, but is not responsible for any liability, loss or damage occurring as a result of following this guide or refraining to act based upon this guide. Specific legal, financial, risk management, or other technical advice should be sought with respect to any issue or information found in this guide prior to relying upon it in a way that may create risk of liability, loss or damage. The information in this guide does not create any contract, agreement, or legal relationship of any kind between you and the MAG.

© 2019 The Merchant Advisory Group

TABLE OF CONTENTS

^ Return to Table of Contents

FREQUENTLY USED TERMS & ACRONYMS

TERM / ACRONYM	WHAT IT MEANS
AFD	Automated Fuel Dispenser, or external fuel pumps that accept unattended payments
AVS	Address Verification Service, part of an authorization message where a merchant will validate part of the cardholder's address (with fuel merchants at AFDs, typically just the zip code) with the card issuer
CCTV	Closed Circuit Television
Chargebacks	A demand by a credit card provider for a merchant to make good the loss on a fraudulent or disputed transaction.
CRIND	Card Reader in Dispenser; the hardware within the fuel pump that accepts payment
CVV / CVC	Card Verification Value or Code – typically a 3- or 4-digit number printed on the back of a card, created with an algorithm. Generally used for eCommerce authentication
EMV	Europay, Mastercard, Visa. A technical standard for smart payment cards using a cryptogram inside of a chip embedded in a plastic card
Fallback	A fallback transaction normally occurs when a chip card, presented at a chip enabled terminal cannot be electronically read due to a technical issue with the chip that results in the technology "falling back" to a magnetic stripe transaction.
MCC	Merchant Category Code – a 4-digit code assigned by an acquirer to identify the merchant's business vertical
PCI/DSS	Payment Card Industry Data Security Standard – an information security standard that is mandated by the Card Brands
PIN	Personal Identification Number – typically a 4-digit number known only to the cardholder
PIN-less	PIN-less technology allows a payment card to be processed without entering a PIN
POS	Point-of-Sale system – the hardware used by the service station to process payment
RTC	Real Time Clearing – a Visa program
Skimmers	Skimming devices are used by criminals to obtain credit card numbers and cardholder information without the customer's knowledge. While skimming can occur at any point of sale (POS), it is more prevalent at Automated Fuel Dispensers (AFDs). Modern skimmers capture not only the card number but track data from the magnetic stripe, including the primary account number, customer name, expiration date, PIN, CVV & CVC. Capturing this additional data makes the stolen card easy to use or sell and makes detecting unauthorized use difficult.

^ Return to Table of Contents

TERM / ACRONYM	WHAT IT MEANS
System Offline	When your payment terminal or POS cannot connect to the authorization platform to receive a real-time response – possibly a result of several factors such as an internet outage in your location, disconnected wiring or cords, an outage at your acquirer or processor, a hardware malfunction, etc.
Velocity Checking	A fraud prevention measure that puts a limitation on the number of transactions that can be conducted within a given set of metrics – examples include limiting the number of times a particular card number can be used within a given time period, or the number of authorizations that can be attempted coming from a specific IP Address
VTA	Visa Transaction Advisor is an optional Visa service for fuel merchants that performs analytics on a cardholder's account to provide a risk score that merchants can leverage to identify transactions with a higher risk of fraud and optionally request additional authentication
ZIP	“Zone Improvement Plan”, or the 5-digit postal code used by the U.S. Postal Service that identifies the city or neighborhood of an address

^ Return to Table of Contents

OVERVIEW

This document provides best practices for petroleum merchants to minimize fraud at their Automated Fuel Dispensers (AFDs) prior to and subsequent to implementing EMV chip cards.

Today, petroleum merchants are liable for most fraud due to lost and stolen payment cards. Lost and stolen fraud accounts for about 10% of credit card fraud, whereas counterfeit fraud accounts for 90%.

- Effective April 2021*, petroleum merchants that have not installed EMV (chip card) technology at their AFDs will be liable for counterfeit fraud. Industry experts estimate that this will shift $451M in chargebacks from the banks to the merchants. It is estimated that potential chargebacks will exceed $201K per site in total over the next 7 years!
- While the number one best practice to prevent fraud at the AFD is to deploy EMV, we know that for various reasons - with many beyond the merchants' control, not all merchants will be EMV-capable by April 2021.
- It is important to note that even if you are not experiencing high volumes of counterfeit fraud today, as other petroleum merchants implement EMV, the fraudsters will seek out and move to locations that have not upgraded. Please contact your acquirer to see the estimated amount of counterfeit fraud that will shift to your location(s) in April 2021.

***The majority of networks will shift liability in April 2021, however other networks have remained at the October 2020 date. It is therefore best to validate with your acquirer in order to fully assess your specific implications.**

^ Return to Table of Contents

© 2019 The Merchant Advisory Group

OPERATIONAL BEST PRACTICES

1 Employee awareness is key! Make sure your employees know what to look for and are doing routine pump inspections (at every shift change). Require employees to complete regular training on fraud prevention and expectations.

2 Monitor suspicious activity at AFDs. Employees should be continually on the lookout for the warning signs of AFD fraud, which can include:

- A single customer activating multiple AFDs
- A vehicle parked at a pump for a long period of time (fraudsters usually target the pump furthest from the store)
- Cars blocking the view of a specific pump
- The same vehicle returning to the same pump repeatedly
- Filling multiple vehicles from one AFD transaction
- Filling large non-vehicle containers
- Fueling several times per day (systemwide and location specific)
- Card testing (swiping, inserting, or tapping payment card for authorization without pumping)
- Island surfing (individuals walking around offering to pump fuel with their payment card in exchange for cash)
- Customers using the “tag team” method—one customer will distract the employee while the other installs the skimmer or overlay

3 Routinely inspect the AFDs to ensure no skimming devices or foreign hardware/software are present.

- Keep your canopy lights well-maintained and bright and consider CCTV monitoring of all gas pumps
- Take a picture of the inside of the dispenser when no skimmer is present to use as a point of reference
- Look through both the front and back of the dispenser: some fraudsters are opening the dispenser on one side and installing the skimmer on the other, making them harder to detect
- Reader should be flush mounted; no external devices
- Use a flashlight to inspect card reader slot (shimmers)
- Listen to cues from customers, e.g. “it’s hard to get my card in/out of the slot”
- Use & monitor pump security seals:
    - Utilize the three-point method (placing the security seals in three distinct places on the dispenser door)
    - Compare the serial number on the current security seal to the last serial number recorded on the pump
    - Keep a log tracking their status (look for broken or missing security seals)
- Consider purchasing lock systems for dispensers and/or tamper alarms to render the pump disabled if tampered with

If a skimming device is found:

- Document and take pictures of the skimming device

^ Return to Table of Contents

© 2019 The Merchant Advisory Group

OPERATIONAL BEST PRACTICES	
	• Do not tamper with or remove the device • Try to minimize your contact with the dispenser door, lock etc. • Close the fueling position and don't let anyone near the dispenser • Contact the local authorities and U.S. Secret Service immediately • Do not approach or confront anyone who looks suspicious, or who is installing or removing a skimming device
4	Eliminate "church key" access to mitigate AFD tampering. Some older AFDs share common keys that allow service station employees and service technicians to easily gain access to the interior of the AFD. Unfortunately, fraudsters have exploited this ease-of-entry feature using copies of the keys to gain unauthorized access.
5	Minimize opportunities for full-service attendants to engage in fraudulent behavior: • Stay current on trends regarding attended fraud, such as pump attendants who accept cash while using fraudulent cards to activate the dispenser • Ensure the POS communicates authorized amounts directly to the pump for dispensing • Have all pump cashiers enter an identification code whenever using the POS • To avoid card compromise, consider wireless handheld card readers so that the cardholder never loses sight of the card (or preferably, retains possession of the card)

^ Return to Table of Contents

© 2019 The Merchant Advisory Group

PAYMENT ACCEPTANCE/PROCESSING BEST PRACTICES

1 Authorize all purchase transactions online.

2 Apply system offline (authorization not available) procedures as needed

- Alert owner/operator headquarters of all offline issues
- Verify transmission is not blocked or purposely interrupted
- Temporarily have dispensers direct cardholders to “see cashier” for all transactions
- Enable offline velocity checking rules/logic; e.g. only allow a card to be used X times in a 24-hour period while offline

3 Always prompt for PIN but allow for bypass in accordance with network rules.

4 If you require the ZIP in a full-service environment (attended terminal) and the cardholder refuses to verbally provide their ZIP, the transaction should not be processed.

5 In full-service environment where attendant is processing payment on the AFD, attendant should not prompt for PIN.

6 Consider PIN-less acceptance to eliminate PIN entry while retaining counterfeit fraud protection.

7 Set a delay time between authorization requests to help prevent counterfeit card testing (this can typically be done through your POS or Fuel System solution). Setting delays between authorization requests may make it less convenient for fraudsters to test stolen or re-encoded cards.

8 Velocity Checking is recommended to monitor card usage by each location as well as across all locations. The velocity checking database must be PCI DSS compliant. It is also a best practice to limit the velocity checking to only transactions above a certain dollar threshold (e.g., above $25, so that in-store small ticket transactions are not impacted).

9 Enter last four requires the cardholder enter the last four digits of the account number into the keypad. Note the last four do not get submitted in the authorization message. Instead, some POS systems can be configured to compare the last four entered against the last four read from the card and refer inside or decline if not a match.

10 Authorization options (Visa specific)

- Authorize for the exact amount (if cardholder is prompted for the amount prior to authorization)
- $1.00 status check procedure; Visa’s dispute protection is $100 for U.S. cards, $75 for non-U.S. issued card, $150 for fleet cards
    - Authorization reversals for transactions authorized via status check are required if the transaction is cancelled (no fuel dispensed) but should not be used if any fuel is dispensed
- Real-time processing estimated authorization amount (if processor participates in Visa’s Real-Time Clearing (RTC) program)

11 Authorization options (All networks)

- For AFD transactions when a $1.00 status check authorization is used, merchants must send an AFD confirmation advice message as soon as possible after the fuel has been pumped
- Submit clearing messages for the final amount as promptly as possible

12 Set your AFD gas pumps to shut off when they reach the initial authorization amount in accordance with the above option.

^ Return to Table of Contents

PAYMENT ACCEPTANCE/PROCESSING BEST PRACTICES	
13	If the cardholder cancels the transaction, or does not dispense any fuel, submit an authorization reversal for the full amount. It is recommended no cash refunds are ever given in this scenario. Reverse unused authorizations or reverse the portion of authorization that is not used for AFD transactions.
14	For prepaid transactions submit a pre-authorization for the requested amount. If the approved amount is not fully dispensed submit a completion for the final, actual amount.
15	Set estimated authorization amounts appropriately or through use of a status check authorization.
16	For commercial diesel transactions, adjust the initial authorization amount to accommodate the typically higher charge.
17	Merchants should ensure that limits are in place for the fuel dispensed, and that these limits do not exceed the authorized amount (typically set up in POS fuel system) to avoid automatic issuer disputes for the amount that exceeds the authorization amount.
18	Monitor authorization rates • AVS referrals – ensure negative AVS response codes are referred inside instead of being allowed to pump • VTA referrals – could indicate changing fraud patterns; adjust VTA scores accordingly • Transaction runs – could indicate sophisticated fraud at a location or area • Review of large sequential fuel (diesel) transactions. Fraud is typically related to large volumes of diesel fuel sales in very short timeframes.

^ Return to Table of Contents

© 2019 The Merchant Advisory Group

DISPUTE MITIGATION BEST PRACTICES	
1	Authorization Related Disputes (transactions not properly authorized due to being offline etc.) After coming back online, reauthorize all stored transactions versus forwarding directly into settlement to prevent: • No-Authorization Disputes • Zero-Floor Limit misuse fees • Transaction interchange downgrade • Debit Transaction Integrity Fees (TIF)
2	Fraud Disputes (Card Present): • Ensure all transactions are electronically authorized (do not key-enter if at all possible) • Use AVS or Velocity Checking together to avoid fraudulent transactions
3	Fraud Disputes (Card Not Present/Card-on-File - including mobile transactions) • Ensure all transactions are utilizing CVV2 and AVS tools at a minimum • Consider additional fraud tools to layer into fraud prevention strategy
4	Duplicate Processing Disputes • Ensure your POS systems are not submitting duplicate transactions to the acquirer by implementing velocity rules on same-value transactions from the same card # within a certain amount of time
5	Invalid Disputes • Be sure to review all dispute reason codes to ensure the dispute reason is relevant to your business (i.e., AFD merchants should push back on reason codes such as ‘Goods Not Received’ and ‘Product Not As Described’) • Send inappropriate reason code disputes back to your acquirer
6	Detailed Analysis / Reporting • Work with your acquirer to access raw data/BIN detail in order to monitor dispute volume by issuer on a regular basis to identify anomalies

^ Return to Table of Contents

© 2019 The Merchant Advisory Group

OUTDOOR EMV ENABLEMENT BEST PRACTICES

1	Implementing outdoor EMV requires multiple tasks being completed by multiple teams. Work with your vendors and internal stakeholders to develop a common understanding of the roles and responsibilities for all of the organizations that will be critical to enabling outdoor EMV including: • Vendors (POS & dispenser) • Secure firewall/network service providers • Acquirers/Payment processors • Service contractors • Site operators • Your fuel brand / Convenience store brand
2	Develop comprehensive playbooks for site operators to assist them in planning and executing their outdoor EMV upgrades. The playbook is a single document that helps the site operator understand the task sequence and dependencies for that store's particular combination of equipment. When correctly built and maintained, outdoor EMV playbooks pull together information on all of the tasks needed to deploy outdoor EMV for each specific combination of POS and dispenser type. Playbooks have proven to accelerate the pace of outdoor EMV upgrades while reducing the delays and post go-live problems that can adversely impact consumer experiences.
3	While every merchant location can be targeted by fraudsters, certain retail locations, metropolitan areas, and entire states are experiencing significantly higher fraud levels. Target these sites first, to reduce your exposure in the event you are not able to convert 100% of your sites by the liability shift deadline, and to avoid the immediate risk of chargebacks if these sites exceed the high fraud threshold established by the card brands.
4	The additional fraud reduction measures described in this white paper may take time to implement. Review them now with your POS vendors and payment processor, to determine which fraud reduction options make sense for your sites and understand the lead time required to test and deploy these measures to your sites.
5	If your sites are operated by independent retail channel partners that have to fund their own upgrades, develop a comprehensive communication strategy for these channel partners. Provide them with the information they need to make good decisions, e.g. current site-by-site fraud levels, help available from internal as well as vendor sources, availability of funding options, etc. Proactively communicate with these channel operators to understand their schedules, keep them updated with the latest information, help them resolve supplier or other roadblocks, and identify any common issues post-install.
6	Consider a phased approach to installation of the outdoor EMV components. Sites will need new dispenser hardware, upgraded communications, new software/firmware, and in many cases new MNSP services. By completing these upgrades in phases, a merchant may be able to complete each in a shorter, possibly off-hours time window, reducing the customer impact and avoiding prolonged outages on the day of final conversion.

^ Return to Table of Contents

CUSTOMER SATISFACTION BEST PRACTICES

1	Check automated fuel dispenser keypads to make sure they are functioning properly to expedite transactions.
2	Use intercom systems to offer customer assistance.
3	As locations are preparing for EMV installation, signage or integrated televisions should educate consumers on upcoming changes or alert them after the installation has taken place.
4	Signage should indicate when a transaction limit is in place and should instruct customers to swipe/insert their card again or pay inside but signage should not display the actual limit.
5	Ensure displays provide clear instructions to customer on how to complete a sale at an AFD (e.g. AVS or other prompts).
6	Test transaction flows to ensure you are providing the most intuitive customer experience while minimizing cost and fraud risk.

^ Return to Table of Contents

TOOLS TO REDUCE AFD FRAUD RISK

VISA TRANSACTION ADVISOR (VTA)	
What is it?	• Visa Transaction Advisor (VTA) is a Visa service that allows merchants to identify transactions with a higher risk of fraud and perform further cardholder authentication before gas is dispensed. • VTA works as follows: ○ After a cardholder inserts the card at the pump, Visa analyzes multiple data sets, such as past transactions, whether the account has been involved in a data compromise, and nearly 500 other pieces of data to create a risk score for each fuel pump transaction ○ If an AFD transaction exceeds a fraud score threshold set by the merchant, Visa sends the merchant a response code of '19' that the merchant can translate to "see cashier" or similar ○ This fraud management solution operates invisibly to the cardholder, helping to ensure a positive customer experience ○ VTA also leverages existing payment processes, thus requiring minimal or no new investments in infrastructure changes ○ It works for all types of non-PIN transactions including mobile app transactions ○ VTA does not score chip on chip transactions ○ There is a maximum number of rules allowed to be set by the merchant per Merchant Category Code (MCC), segregating locations by individual store, ZIP code and entry method
How do I subscribe to the service?	• You will need an agreement to participate; reach out to your Visa Account Executive for more information • This service requires a Visa specific merchant identifier so it's important to ensure your gateway / acquirer can support
What does it cost?	This is a paid service; reach out to your gateway / acquirer for pricing
VTA BEST PRACTICES	
1	Review your portfolio to identify the risk / threat and establish rules accordingly. Visa and/or your gateway/acquirer may be able to assist if needed. • High fraud states, zip codes or individual merchant locations • Outside v. inside transactions • EMV cards v. mag stripe cards
2	Submit the rules form to vta@visa.com

^ Return to Table of Contents

3	Review for response code “19” authorization activity for referral trends and adjust accordingly: ○ False positives ○ Evidence of activity suggesting a rules update is appropriate Access to authorization activity may be governed by your gateway / acquirer
4	Review lookback activity provided by Visa
5	Utilize chargeback data to gauge rules effectiveness
6	Combine fraud mitigation tools for the best results

^ Return to Table of Contents

© 2019 The Merchant Advisory Group

ADDRESS VERIFICATION SERVICE (AVS)

What is it?

- Address Verification Service (AVS) verifies the five-digit billing statement postal code of the customer who is paying with a card at an AFD
- The postal code is included in the authorization request message
- The response message back will contain an AVS result code (separate from the authorization response code) that indicates whether the postal code given by the customer matches the postal code, on file, with the card issuer

How do I subscribe to the service?

- There is no subscription per se, but there is an authorization field where merchants can populate the address information they are collecting from guests.
- Merchants should work with their acquirer on how the result of that field from the issuer specifically impacts transaction decisioning

What does it cost?

***Costs passed through acquirer*

- Visa: $0.025 per Zero Dollar Authorization Request (that includes AVS information)
- Mastercard: $0.01 per AVS request

AVS BEST PRACTICES

1

Provide signage to international cardholders that allows them to either:

- Bypass a ZIP or postal code entry (using the Clear/Cancel key) or
- Instructs the cardholder to “See Cashier” to complete the transaction

Canadian Postal Codes

Canadian customers who travel to the U.S. can participate in AVS when prompted for a 5-digit numeric ZIP code at the pump, by doing the following:

Take the three numbers from the Canadian postal code	Add two zeros to the end	This is the number a Canadian cardholder can use when asked for a U.S. ZIP Code
A2B 3C4	**+ 00**	**23400**

*Be sure to work with your acquirer on mapping to the correct response codes

2

In the event of a ZIP or postal code input error, provide a “Clear/Cancel” key

^ Return to Table of Contents

3	Provide signage to mitigate cardholder phishing fears. For example, stickers or video screen content, explaining the point-of-sale is requesting the cardholder's billing statement ZIP or postal code for security purposes only and will not be retained or used for marketing purposes
4	Use AVS at high fraud locations. It's recommended to take the following actions: • To prevent shoulder surfers, mask the ZIP or postal code digits as they are input by the cardholder (e.g. ****3) • If the cardholder does not correctly input their current billing statement ZIP code within two attempts, instruct the cardholder to "see cashier" to complete the transaction • "Approve" the following AVS results codes: Z, P, Y • "Decline" all other result codes and instruct the cardholder to "see cashier" for additional assistance If the transaction is approved by the issuer but the merchant chooses not to complete due to an AVS "no match" response, the authorization approval must be reversed
5	Visa requires zip prompting be enabled in the following geographies (required both pre and post EMV implementation) • Atlanta, GA • Brooklyn, NY • Detroit, MI • Fresno, CA • Greater Los Angeles, CA • Houston, TX • Kingman, AZ • Las Vegas, NV • Louisville, KY • Florida (all cities and counties)
6	Ensure configuration only authorizes valid AVS response codes. Each card network sends an alpha character response to each AVS request; some of which are negative responses – be sure to work with your acquirer to ensure you are interpreting the correct AVS response codes

^ Return to Table of Contents

FALLBACK

What is it?	A fallback transaction normally occurs when a chip card, presented at a chip enabled terminal, cannot be read due to either a malfunction of the chip itself or the chip reader. In these situations, the card information can usually be read via the magnetic stripe, and the transaction is subsequently labeled a “fallback transaction.”
What does it cost?	There are no additional costs related to Fallback; however, merchants will still bear lost/stolen liability on any mag stripe transactions, regardless if they occur at a Chip-enabled terminal or not.
Notes	• Bad actors know fallback can allow mag stripe transactions at an EMV enabled terminal, and therefore, approval rates on fallback transactions are often lower. • Issuer can still decline fallback transaction even if the merchant passes all the necessary data. • At AFD’s, the magnetic stripe reader and chip reader are typically combined in the same slot – which impacts the processing of technical fallback. Whether a chip was detected will determine if the transaction can process as a technical fallback: ○ **If a chip is not detected**, the track data is read as the card is extracted and therefore the payment application must determine how to handle the magnetic stripe read transaction – whether as a true magnetic stripe or as a fallback to a chip error transaction. In a traditional POS environment, the terminal would report back a chip error and instruct the cardholder to swipe the card ○ **If a chip is detected, but cannot be read,** the transaction is able to be processed as a technical fallback since the chip was detected and a ‘chip error’ was returned

FALLBACK BEST PRACTICES

1	Monitor quantity of fallback of chip card transactions for both magnetic-stripe read and key-entered transactions by location, POS terminal, and clerk ID. A high number of fallback transactions can be indicative of internal/external fraud or equipment maintenance issues.
2	Merchants should work with their acquirer to receive regular fallback reporting for continuous monitoring.
3	Liability rules differ by network for fallback transactions. Merchants may support fallback for certain networks and not others due to these liability concerns.
4	The U.S. Payments Forum has published a detailed whitepaper on Fallback Best Practices located here.

^ Return to Table of Contents

MASTERCARD CONSUMER PROTECTION PROGRAM

What is it?	A new Mastercard Program designed to address the fraud vulnerabilities that exist today at U.S. region automated fuel dispenser (AFD) merchants that have not completed migration to EMV technology. This new program has been put in place to support consumers and AFD merchants still completing migration to EMV. The program includes a Fraud Insights Dashboard for merchants to provide aggregate insights into auth, clearing, chargeback, digital and confirmed fraud.
How do I subscribe to the service?	Reach out to your Mastercard Account Executive or through your acquirer to express interest in the service. An agreement must be executed between merchant and Mastercard.
What does it cost?	The monthly fee for the Fraud Insights Dashboard is waived for merchants through April 16, 2021.

PERFORMANCE PROGRAM FOR HIGH-RISK AFD MERCHANTS

1	• Mastercard will review network data over a **three-month rolling** period to identify U.S. region fuel merchant locations that meet the following high-risk fraud criteria: ○ At least 300 cleared transactions **in total** over the three-month period ○ At least $1,000 USD in reported fraud over the three-month period • Notifications will be sent to the merchants' acquirers, who will be required to complete and submit a remediation plan providing key details about each merchant's fraud controls and actions being taken to mitigate fraud. • Merchant locations that have been identified as having met the high-risk fraud criteria will have their Mastercard IDs shared with issuers.
2	Compliance fees may be assessed for exceeding the above thresholds. Failure to provide a remediation plan may result in fines of up to $15,000.

^ Return to Table of Contents

© 2019 The Merchant Advisory Group

PINLESS LIABILITY ON AFD TRANSACTIONS

BEST PRACTICE: Discuss with your acquirer what PINless capabilities and options are available for AFD at your locations and what liability rules accompany them

*As of September 2020**

TERMINAL TYPE	CARD TYPE	NETWORK	TRANSACTION AMOUNT	CHARGEBACK LIABILITY
EMV Enabled	MSR	AFFN[2]	Any Amount	Issuer
		Culiance[2]		
		NYCE[2]		
		Pulse		
		SHAZAM	Over $100	Merchant**
			Under $100	Issuer
	Chip	AFFN	Any Amount	Issuer~
		Culiance		
		NYCE		
		Pulse	Over $50	Issuer[1]
			Under $50	Issuer
		SHAZAM	Over $100	Merchant**
			Under $100	Issuer
Not EMV Enabled	MSR	AFFN[2]	Any Amount	
		Culiance[2]		
		NYCE[2]		
		Pulse		
		SHAZAM	Over $100	Merchant**
			Under $100	Issuer
	Chip	AFFN	Any Amount	Merchant
		Culiance		
		NYCE		
		Pulse		
		SHAZAM		

* Note, the table above represents current program rules **AS OF SEPTEMBER 2020** and may change in the future. Always contact the network directly for their most current rules.

** Issuer may dispute amount of transaction over $100 with valid fraud reason (Example: $125 transaction with a valid dispute reason, issuer can dispute only $25).

~ For transactions less than $50, Issuer does not have any chargeback rights. If over $50, issuer may chargeback if they believe merchant intentionally processed a transaction that they knew to be fraudulent.

[1] Issuer may dispute transaction if card is PIN preferring, PIN was not entered, and card was reported lost/stolen at time of transaction.

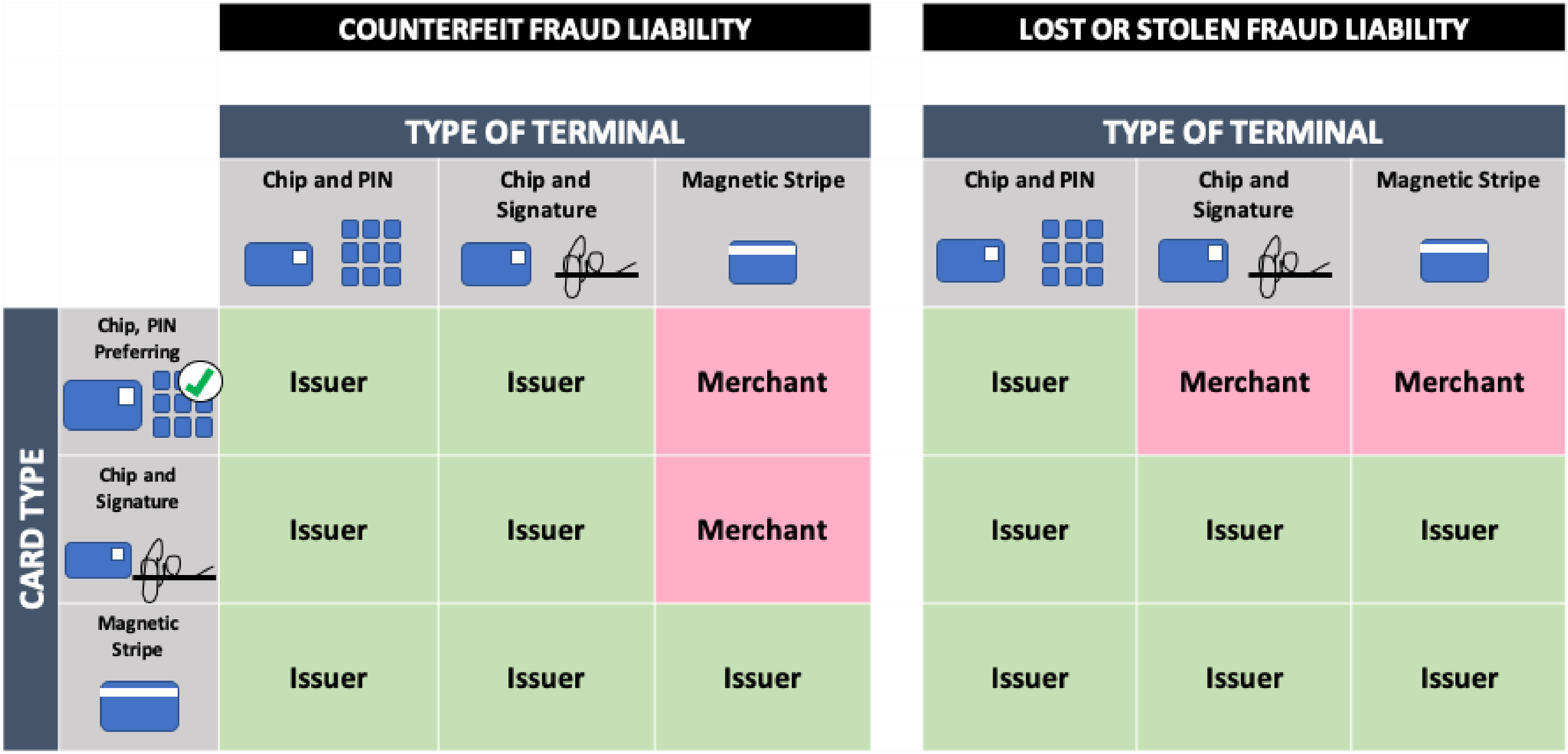
[2] Signature required if transaction greater than $50.

^ Return to Table of Contents

APPENDIX

FRAUD LIABILITY SHIFT MATRIX

- Liability shifts to the party in the payment chain with the least secure payment technology



		COUNTERFEIT FRAUD LIABILITY			LOST OR STOLEN FRAUD LIABILITY		
		TYPE OF TERMINAL			TYPE OF TERMINAL		
		Chip and PIN	Chip and Signature	Magnetic Stripe	Chip and PIN	Chip and Signature	Magnetic Stripe
CARD TYPE	Chip, PIN Preferring ✓	Issuer	Issuer	Merchant	Issuer	Merchant	Merchant
	Chip and Signature	Issuer	Issuer	Merchant	Issuer	Issuer	Issuer
	Magnetic Stripe	Issuer	Issuer	Issuer	Issuer	Issuer	Issuer

^ Return to Table of Contents

© 2019 The Merchant Advisory Group

NOTE: This chart indicates which party is generally liable at the time of this publication. These may change, and there may be exceptions in specific cases such as with technical fallback for example.

CARD NETWORKS FRAUD MONITORING PROGRAMS

- Refer to Fraud & Chargeback Risk Programs to see an overview of each network's program.

BEST PRACTICE

BEST PRACTICE:

- Leveraging the tools and services described in this guide could help merchants avoid being placed on the Networks' excessive fraud monitoring programs. Merchants should always work with their acquirer to get reporting on high risk locations (including fraud that is currently not passed to the merchant but will after the EMV liability shift) to prioritize mitigation efforts in those specific geographic areas. If your acquirer is unable to accommodate, you should work directly with the networks
- Each of the global card networks (Visa, Mastercard, Amex, Discover) as well as the fleet card networks (e.g. WEX, Voyager) have defined programs for monitoring merchant fraud and chargebacks. Merchants may be assessed fees/fines if they exceed the thresholds defined by each network.

^ Return to Table of Contents