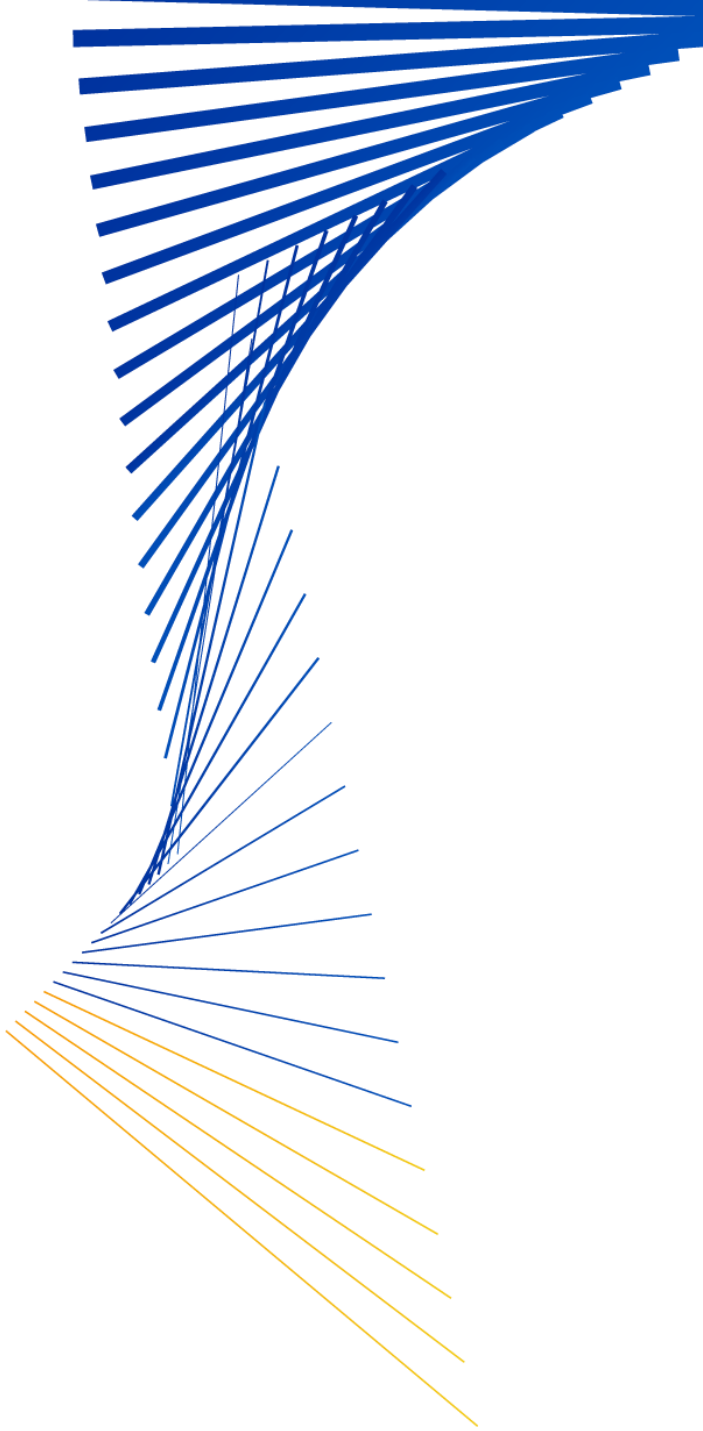
Visa U.S. Fuel Merchant Automated Fuel Dispenser Fraud Mitigation Best Practices

Webinar

November 27, 2018



Webinar Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

CONEXXUS
solve forward

Housekeeping

This webinar is being recorded and will be made available on:

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Available at conexxus.org

Survey

- Please complete the short survey sent out an hour after the live webinar

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions

Email: **info@conexxus.org**

Presenters

Conexxus Host

Allie Russell
Conexxus
arussell@conexxus.org

Jenny Bullard
Conexxus
jbullard@conexxus.org

Moderator

Jenny Bullard
Manager Membership Engagement
Conexxus
jbullard@conexxus.org

Speakers

Robert Alandt, Visa Senior Director Merchant Solutions

Sydney Green, Visa Senior Director Risk and Authentication

Andrew McGloin, Visa Senior Director of NA Risk

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy

CONEXXUS
solve forward

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Profile: Conexxus.org
- Follow us on Twitter: @Conexxusonline

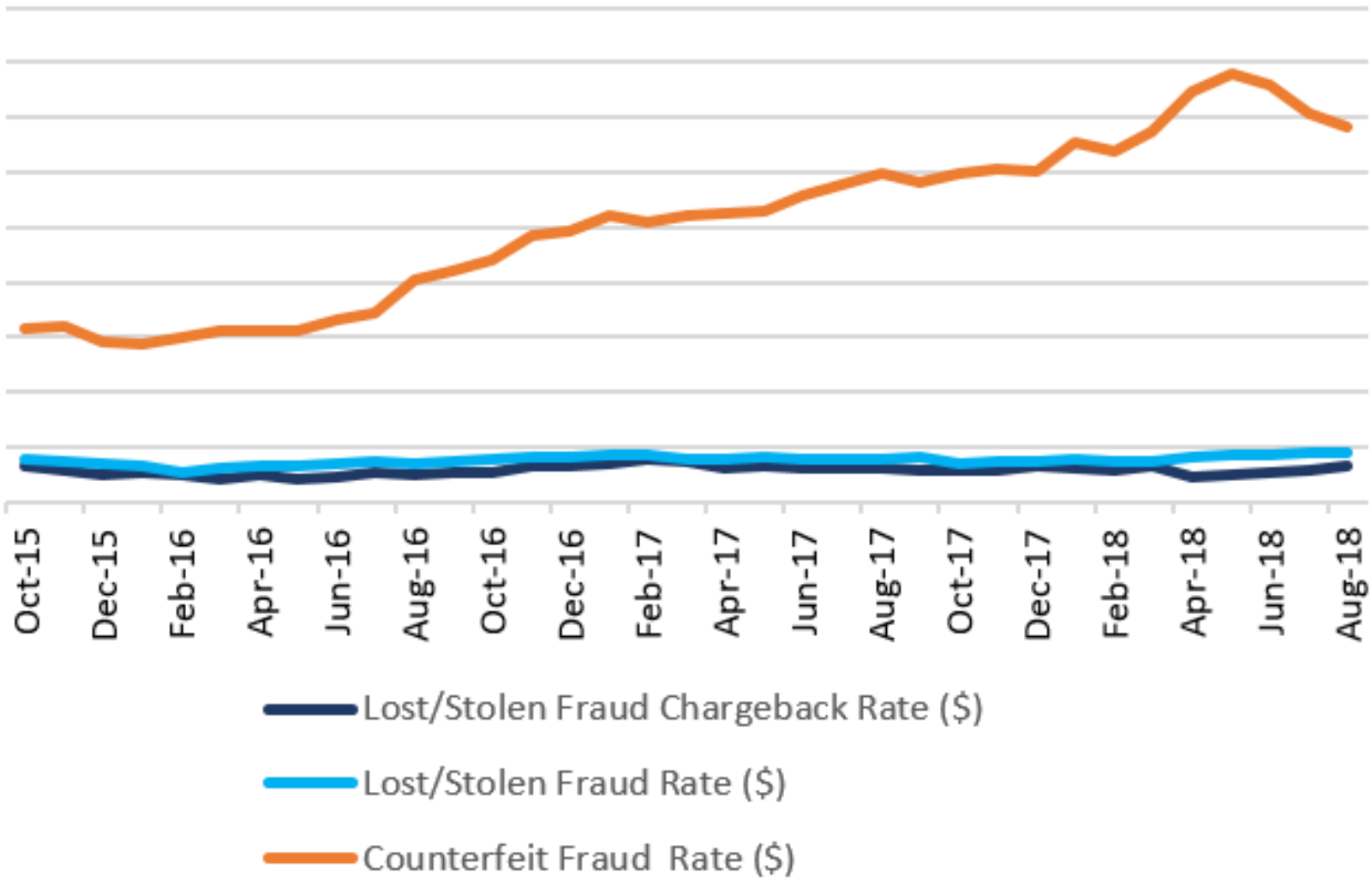
Presentation Agenda

- Automated Fuel Dispenser Fraud Trends
- Key Rules and AFD Fraud Monitoring
- Automated Fuel Dispenser Fraud Mitigation Best Practices and Tools Review
- Automated Fuel Dispenser Fraud Landscape
- Resource Publications

Case studies, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. does not make any warranty or representation as to the completeness or accuracy of the information within this document, nor assume any liability or responsibility that may result from reliance on such Information. The Information contained herein is not intended as legal advice, and readers are encouraged to seek the advice of a competent legal professional where such advice is required.

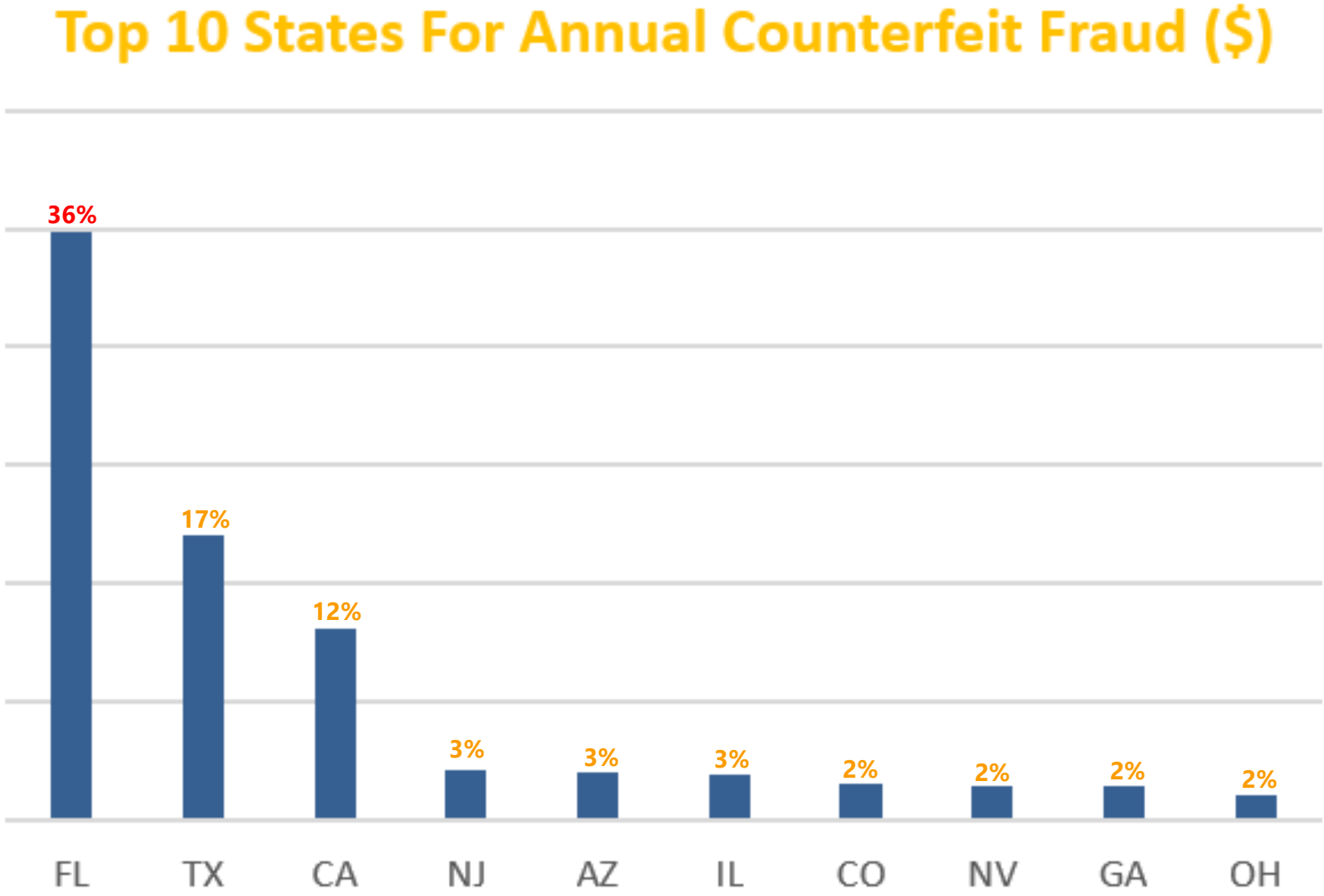
Automated Fuel Dispenser Fraud Trends

AFD 5542 Reported Fraud & Fraud Chargeback Trends



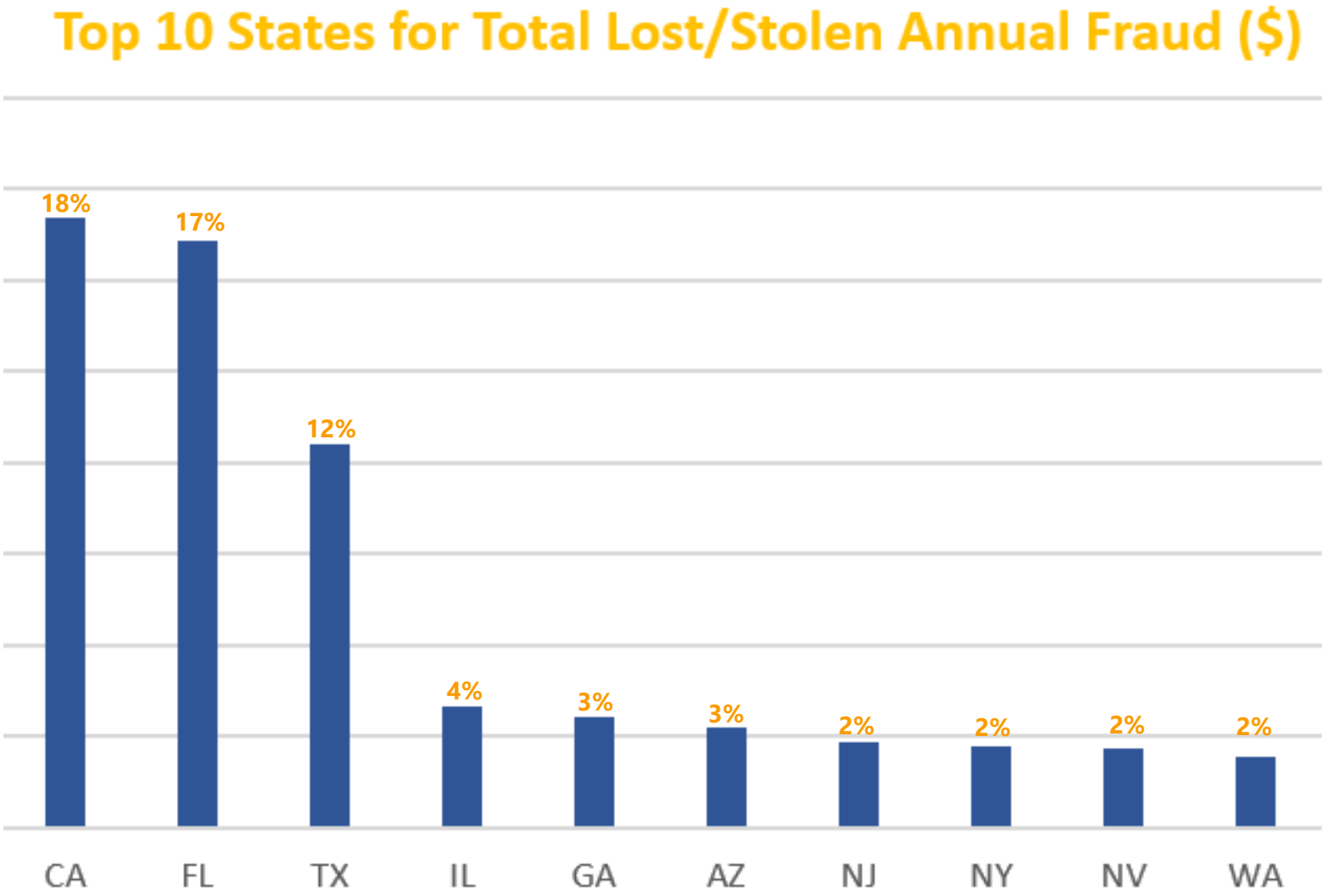
Source: VisaNet

AFD 5542 Counterfeit Fraud By State



Source: VisaNet for the period Q3 2017 through Q2 2018

AFD 5542 Lost/Stolen Fraud By State



Source: VisaNet for the period Q3 2017 through Q2 2018

Automated Fuel Dispenser Key Rules and Fraud Monitoring Program

Liability shift for AFD counterfeit fraud

U.S.	Card	AFD	Liability
Prior to October 1: - **2017 AFD XBorder** - **2020 AFD US Dom**	Mag stripe only	Mag stripe only	Issuer
After October 1, 2017 AFD XBorder	Mag stripe only	Mag stripe only	Issuer
	Mag stripe only	EMV chip	Issuer
After October 1, 2020 AFD US Domestic	**EMV chip**	**Mag stripe only**	**Acquirer**
	EMV chip	EMV chip	Issuer

There is **no EMV liability shift** on
contactless or lost/stolen fraud transactions

Liability shift for AFD lost/stolen fraud

Global	Card	AFD	Card Read	Liability
As of April 15, 2014	Mag stripe only	Mag stripe only	Mag stripe	Acquirer
	Mag stripe only	EMV chip	Mag stripe	Acquirer
	EMV chip	EMV chip	Mag stripe "fallback" transaction	Acquirer
	EMV chip	**EMV chip**	**EMV chip (Contact or Contactless)**	**Issuer**

Consider sending AFD fallback inside for completion

AFD Fraud Monitoring Program

Key program attributes:

- Applies only to U.S. domestic transactions at AFDs
- Identification at the merchant location/outlet level
- Program will review the previous calendar month's domestic counterfeit fraud dollar totals and the domestic counterfeit fraud-to-sales ratio
- Two program thresholds
  - Standard Program - monthly basis thresholds met or exceeded
    - $10K in domestic counterfeit fraud, and
    - 0.20% domestic counterfeit fraud amount to domestic sales ratio
  - Excessive Program – monthly basis thresholds met or exceeded
    - $10K in domestic counterfeit fraud, and
    - 2.00% domestic counterfeit fraud amount to domestic sales ratio
- Remediation considered successful if below at least 1 threshold for 3 consecutive months
- Any U.S. AFD merchant outlet that re-enters the program within 12 months of completing remediation will automatically escalate to the Excessive Program timeline
- Program will end October 2020

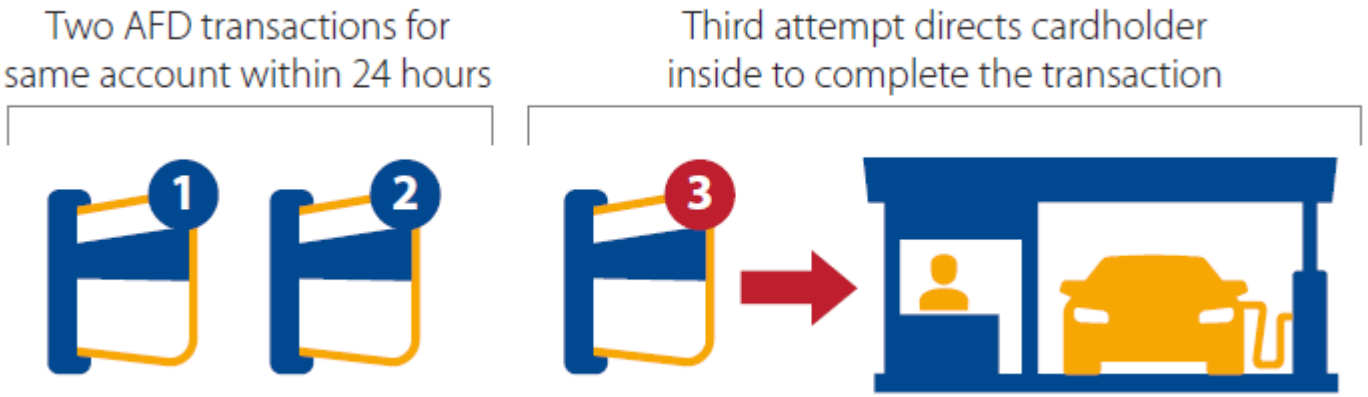
Automated Fuel Dispenser Fraud Mitigation Best Practices and Tools Review

EMV Chip

- The most effective way to eliminate AFD counterfeit fraud
- Customers prefer to transact in a more secure environment when they are able to use their chip cards in a chip-reading AFD
- Changing an AFD from mag-stripe to chip-reading is a complex undertaking that requires time to plan, certify, test, and implement
- Delays in AFD chip implementation will result in counterfeit fraud migrating from all merchants that have already implemented chip acceptance to those that haven't

Velocity Checks

- Velocity checking monitors the frequency of transactions on the same account number
- Visa recommends maintaining velocity checking programs that monitor card usage by each location as well as across all locations for the merchant brand
- The "Two-and-In" strategy is a good policy to apply for velocity checking
  - ➢ Two AFD transactions for the same account number within a 24-hour period at the same location, or across the brand, will cause a third attempt to be directed into the store to complete the fuel purchase transaction



Address Verification (AVS)

- Address Verification Service (AVS) verifies the five-digit billing statement postal code of the customer who is paying with a Visa card at an AFD
- The postal code is included in the authorization request message to Visa.
- Helps to mitigate AFD counterfeit and lost/stolen fraud
- "No-Match" response should be sent inside for transaction completion
- Support for Canadian cardholders

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.
FOR EXAMPLE:				
A2B 3C4	+	00		23400

AFD AVS Mandate

Effective **January 20, 2018** an Automated Fuel Dispenser (AFD) in the US Region must perform an Address Verification Service (AVS) ZIP inquiry if either:

- The AFD location has been identified under the Visa AFD Counterfeit Fraud Monitoring Program
- The AFD location is located in high-fraud area, as specified in the AFD AVS ZIP Mandate for US Fuel Merchants in High-Fraud Geographies:
  - The entire state of Florida
  - Greater Los Angeles California area
  - Houston, Texas
  - Louisville, Kentucky
  - Kingman, Arizona
  - Brooklyn, New York
  - Atlanta, Georgia
  - Fresno, California
  - Las Vegas, Nevada
  - Detroit, Michigan

Visa Transaction Advisor (VTA) for U.S. **Fuel Merchants**

Visa Transaction Advisor is a service being used by merchants to help reduce their fraud through **Visa risk intelligence data sharing** to help in determining the likelihood of fraud

How it works

1

Visa works with acquirer to determine VTA score threshold (1-99)

2

Consumers use their Visa cards at a participating automated fuel dispensers (AFDs)

3

Each transaction is scored and reviewed against the VTA threshold rules

4

Transactions that score above the threshold trigger a response that sends the consumer inside the store to complete their purchase

- ✓ Works for Visa non-PIN, US acquired transactions
- ✓ Supplements existing tools (i.e. no changes to AVS or merchant velocity checks)
- ✓ Assists with cross border
- ✓ Easy implementation
- ✓ No changes to liability associated with the service
- ✓ Visa & acquirer set the threshold score

VTA objectives and overview

Objectives

- No development required for merchants
- Retain a positive cardholder experience
- Synergistic with existing tools
- Provide a tool for cross-border card review
- Bridge the gap prior to, and supplement post chip roll out

Service overview

- Merchant risk service sold through acquirers
- During the standard authorizations, reviews Visa non-PIN transactions at the pump
- If the transaction appears to be high risk, sends back a soft decline
- Message to the pump to ‘see attendant’ or similar

VTA Transaction Risk Scoring

Uses up to 500 variables to calculate the transaction risk.

TRANSACTION VIEW

VisaNet

Creates
a long-term profile of a card account to establish patterns of use based on past activity

Compares
the short-term account activity against the long term profile

Evaluates
the account for any reported unauthorized card activity

Creates and relays
a score from 01-99 that indicates the transaction risk level (higher value correlates to higher risk)

VTA solution implementation

Service setup

1. Confirm your acquirer/processor's participation
2. Merchant signs service agreement with acquirer/processor
3. Work with acquirer/processor and Visa to determine activation date
4. Acquirer will add Visa designated Merchant Verification Value (MVV*) to your authorization requests

---

Cardholder swipes card for authorization at for Visa fuel txns, enters Zip if prompted

Merchant payment host or acquirer sends authorization request to Visa

Visa performs VTA scoring on the authorization request and sends a recommended step-up response code to merchant via the acquirer

*MVV=unique merchant ID, assigned by Visa, added by acquirer/processor

VTA update

- General status:
  - AFD: 34 fuel brands with more than 86K locations active:
    - **~63%** of Visa non-PIN AFD txns participating
  - Inside: 23 fuel brands with more than 58K locations active
    - **~52%** of Visa non-PIN inside txns participating
- Success:
  - Fraud rate comparison for fuel locations in the Las Vegas area

Merchant	L/S fraud rate by amount	Counterfeit fraud rate by amount	VTA subscriber
A	.297%	5.5%	✓
B	1.55%	29.9%	✗

- Brands using/testing the service include:

Source: VisaNet data as of Sept 2018

Automated Fuel Dispenser Fraud Landscape

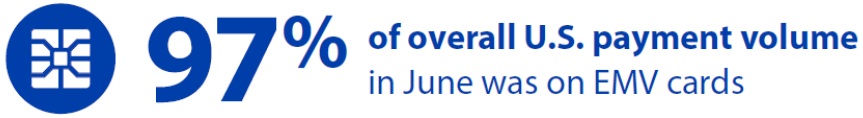
Fraud and skimming is accelerating at AFD terminals

How bad is it?

- Visa card fraud reported for U.S. fuel pumps increased 42% YoY for Q2 2018
- AFD represents nearly one quarter of all U.S. domestic card present fraud

Why is this happening now?

- 67% of U.S. storefronts now accept chip cards
- 69% of Visa credit and debit cards in the U.S. are chip capable



- As chip adoption continues to grow, fraudsters are increasingly turning to POS environments where stolen magnetic stripe data can be monetized
  - Ecommerce
  - Manipulated fallback
  - ATM and Fuel Pumps

Suspicious Activity at Fuel Service Stations

- Fuel stations in remote locations or near highways are frequently targeted, typically at night or during other periods of slow activity
- Customer approaching multiple fuel pumps
- Filling large non-vehicle containers, vehicles with modified tanks, or multiple vehicles in a single visit or during the same day
- Inserting payment cards for authorization without pumping gas (card testing)
- Individual approaching other vehicles, who may be offering to pump fuel with their payment card at a discount in exchange for cash
- For employee safety, do not directly confront individuals who are actively perpetrating fraud. Contact local law enforcement and wait for their arrival before addressing a live situation.

Criminal Activity Update

- The black market for fuel is expected to proliferate through October 2020 or until a mass conversion to EMV at the pumps takes place.

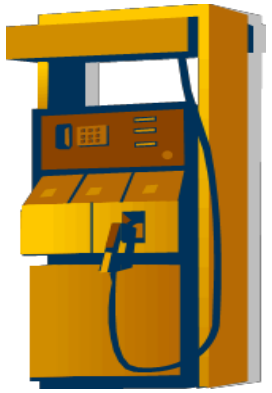
  - Florida continues to be identified with significant skimming deployment and the perpetration of payment card fraud for fuel purchases. Activity is concentrated within a 5 mile radius of southeast Florida, including Miami and its surrounding areas
    - The Secret Service has arrested dozens of organize crime fraudsters perpetrating AFD fraud and continues to carry out sophisticated sweeps in the area.

- Other states with high incidents of AFD fraud are Texas, Arizona and California. Skimming and its subsequent counterfeit fraud sometimes occur in different locations.

- Training and awareness are critical components of this campaign

- Visa continues to be notified of successful apprehension of criminals in this space.

Practices to Minimize Risk



- Educate employees to inspect pumps daily for signs of tampering
  - Broken or missing seals, missing screwed, drilled holes, or extra wiring.
  - Unusual decals or stickers that may be added to cover inflicted damage.
  - Be vigilant – modern skimmers and overlays are becoming increasingly sophisticated and difficult to detect (wireless, battery powered, easy to deploy, pin hole cameras)
- Ensure that access to the interior of an AFD is locked with a secure key and only accessible by specific employees. Keys should have limited pump access and be securely stored.
- Install bright lighting throughout the fuel station
- Use CCTV video cameras to deter, monitor, and detect suspicious activity. This especially applies if pumps are not staffed 24/7
- Work with vendors to upgrade equipment and install anti-tampering safeguards.
- Have a clear response plan for employees if a skimming device is discovered

What to do if a skimmer is detected

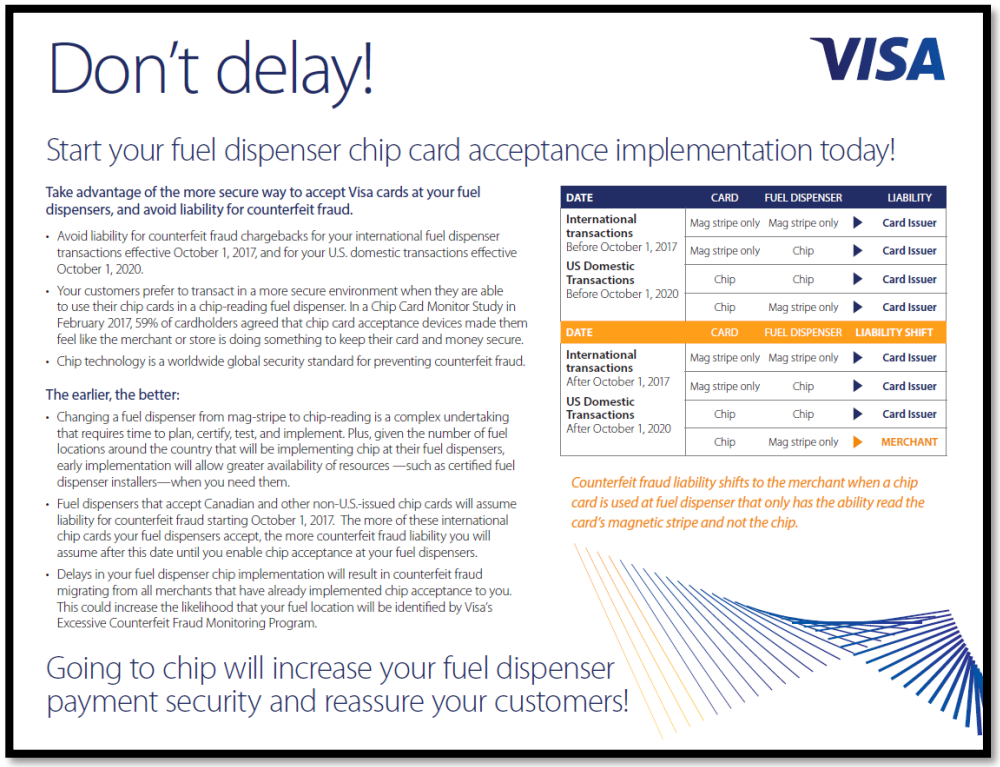
- DO NOT meddle with the device, as evidence may be damaged
- Notify corporate office, franchisor or distributor
- Notify local law enforcement, FBI, and/or U.S. Secret Service field office
- Keep any video surveillance that may aid in the investigation and identify the window of exposure
- Notify your acquiring bank or processor
- Contact Visa Investigations team: usfraudcontrol@visa.com
- Maintain a summary of the event:
  - Document the date and time of discovery
  - Provide photograph of device
  - Timeframe the device was operating, if known
  - (Acquirer) Provide payment card numbers that were processed while skimmer was in place so that issuers can be notified of at-risk accounts
- Implement additional controls to avoid a repeat incident

Resource Publications

Publications Specifically for Fuel Retailers

Publically available on Visa.com

- AFD Chip Acceptance Awareness
- AFD Fraud Prevention Best Practices
- Fuel Merchant Acceptance Best Practices



Don't delay!

VISA

Start your fuel dispenser chip card acceptance implementation today!

Take advantage of the more secure way to accept Visa cards at your fuel dispensers, and avoid liability for counterfeit fraud.

- Avoid liability for counterfeit fraud chargebacks for your international fuel dispenser transactions effective October 1, 2017, and for your U.S. domestic transactions effective October 1, 2020.
- Your customers prefer to transact in a more secure environment when they are able to use their chip cards in a chip-reading fuel dispenser. In a Chip Card Monitor Study in February 2017, 59% of cardholders agreed that chip card acceptance devices made them feel like the merchant or store is doing something to keep their card and money secure.
- Chip technology is a worldwide global security standard for preventing counterfeit fraud.

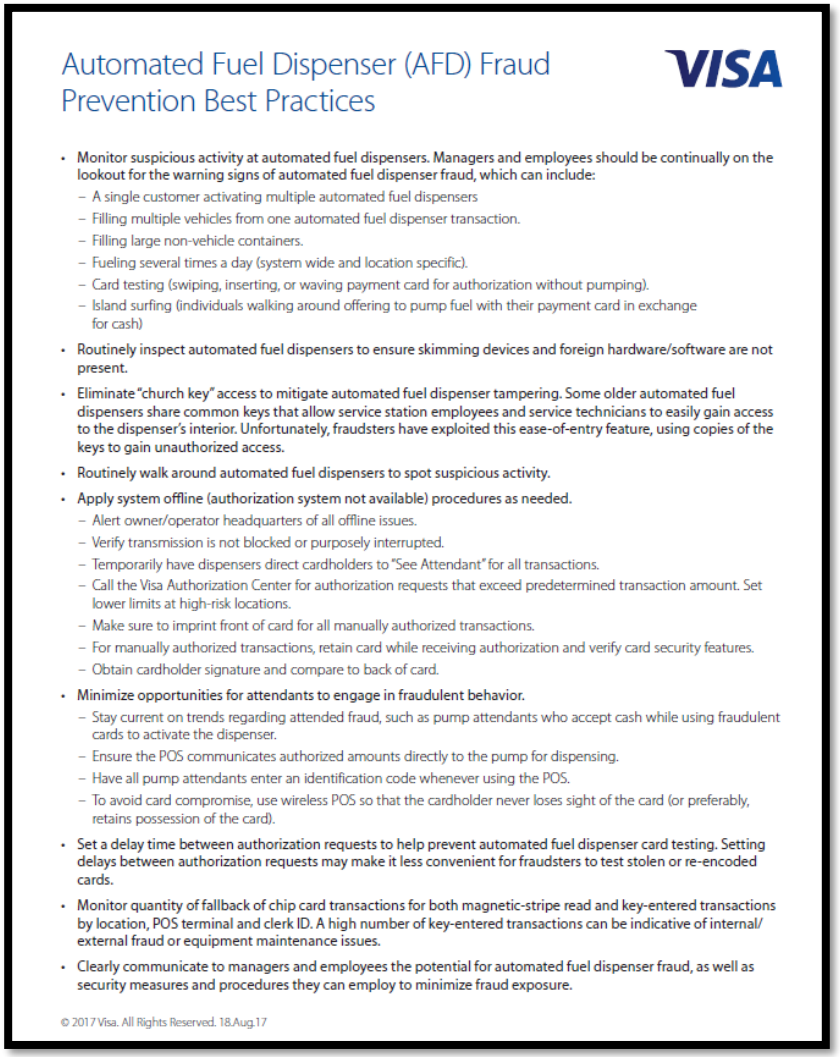
The earlier, the better:

- Changing a fuel dispenser from mag-stripe to chip-reading is a complex undertaking that requires time to plan, certify, test, and implement. Plus, given the number of fuel locations around the country that will be implementing chip at their fuel dispensers, early implementation will allow greater availability of resources —such as certified fuel dispenser installers—when you need them.
- Fuel dispensers that accept Canadian and other non-U.S.-issued chip cards will assume liability for counterfeit fraud starting October 1, 2017. The more of these international chip cards your fuel dispensers accept, the more counterfeit fraud liability you will assume after this date until you enable chip acceptance at your fuel dispensers.
- Delays in your fuel dispenser chip implementation will result in counterfeit fraud migrating from all merchants that have already implemented chip acceptance to you. This could increase the likelihood that your fuel location will be identified by Visa's Excessive Counterfeit Fraud Monitoring Program.

DATE	CARD	FUEL DISPENSER	LIABILITY
International transactions Before October 1, 2017	Mag stripe only	Mag stripe only	**Card Issuer**
	Mag stripe only	Chip	**Card Issuer**
US Domestic Transactions Before October 1, 2020	Chip	Chip	**Card Issuer**
	Chip	Mag stripe only	**Card Issuer**
DATE	**CARD**	**FUEL DISPENSER**	**LIABILITY SHIFT**
International transactions After October 1, 2017	Mag stripe only	Mag stripe only	**Card Issuer**
	Mag stripe only	Chip	**Card Issuer**
US Domestic Transactions After October 1, 2020	Chip	Chip	**Card Issuer**
	Chip	Mag stripe only	**MERCHANT**

Counterfeit fraud liability shifts to the merchant when a chip card is used at fuel dispenser that only has the ability read the card's magnetic stripe and not the chip.

Going to chip will increase your fuel dispenser payment security and reassure your customers!



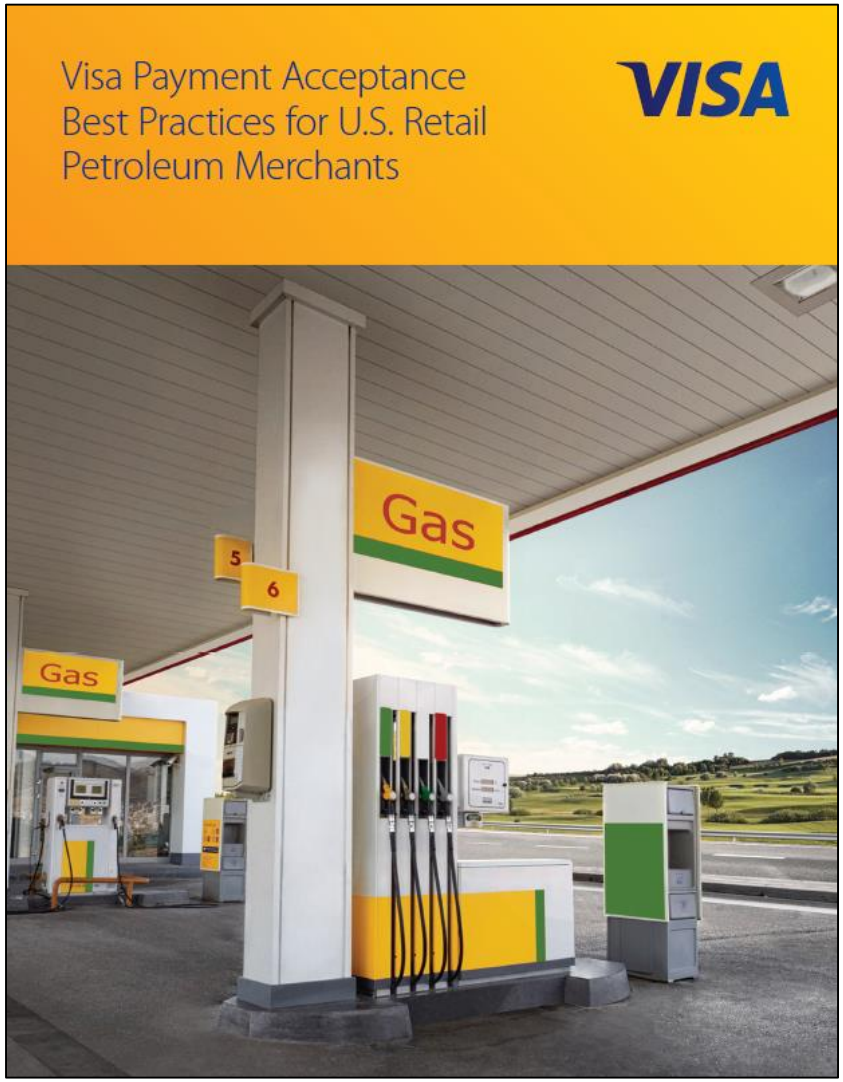
Automated Fuel Dispenser (AFD) Fraud Prevention Best Practices

VISA

- Monitor suspicious activity at automated fuel dispensers. Managers and employees should be continually on the lookout for the warning signs of automated fuel dispenser fraud, which can include:
  - A single customer activating multiple automated fuel dispensers
  - Filling multiple vehicles from one automated fuel dispenser transaction.
  - Filling large non-vehicle containers.
  - Fueling several times a day (system wide and location specific).
  - Card testing (swiping, inserting, or waving payment card for authorization without pumping).
  - Island surfing (individuals walking around offering to pump fuel with their payment card in exchange for cash)
- Routinely inspect automated fuel dispensers to ensure skimming devices and foreign hardware/software are not present.
- Eliminate "church key" access to mitigate automated fuel dispenser tampering. Some older automated fuel dispensers share common keys that allow service station employees and service technicians to easily gain access to the dispenser's interior. Unfortunately, fraudsters have exploited this ease-of-entry feature, using copies of the keys to gain unauthorized access.
- Routinely walk around automated fuel dispensers to spot suspicious activity.
- Apply system offline (authorization system 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 Attendant" for all transactions.
  - Call the Visa Authorization Center for authorization requests that exceed predetermined transaction amount. Set lower limits at high-risk locations.
  - Make sure to imprint front of card for all manually authorized transactions.
  - For manually authorized transactions, retain card while receiving authorization and verify card security features.
  - Obtain cardholder signature and compare to back of card.
- Minimize opportunities for 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 attendants enter an identification code whenever using the POS.
  - To avoid card compromise, use wireless POS so that the cardholder never loses sight of the card (or preferably, retains possession of the card).
- Set a delay time between authorization requests to help prevent automated fuel dispenser card testing. Setting delays between authorization requests may make it less convenient for fraudsters to test stolen or re-encoded cards.
- 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 key-entered transactions can be indicative of internal/external fraud or equipment maintenance issues.
- Clearly communicate to managers and employees the potential for automated fuel dispenser fraud, as well as security measures and procedures they can employ to minimize fraud exposure.

VISA

Publications Specifically for Fuel Retailers (Cont.)



Questions?