
TRAVEL
CONNECT
DISTRIBUTION:
EVOLVED
BOOK
BOOK
BOOK
41

FIGHTING FRAUD THROUGH COLLABORATION

SPEAKERS

Michael Savicki

Vice President, Risk & Compliance, The Americas and Global Head of Commercial Compliance

AMERICAN EXPRESS GLOBAL BUSINESS TRAVEL

Cornelius Hattingh

Director of Revenue Integrity

ARC

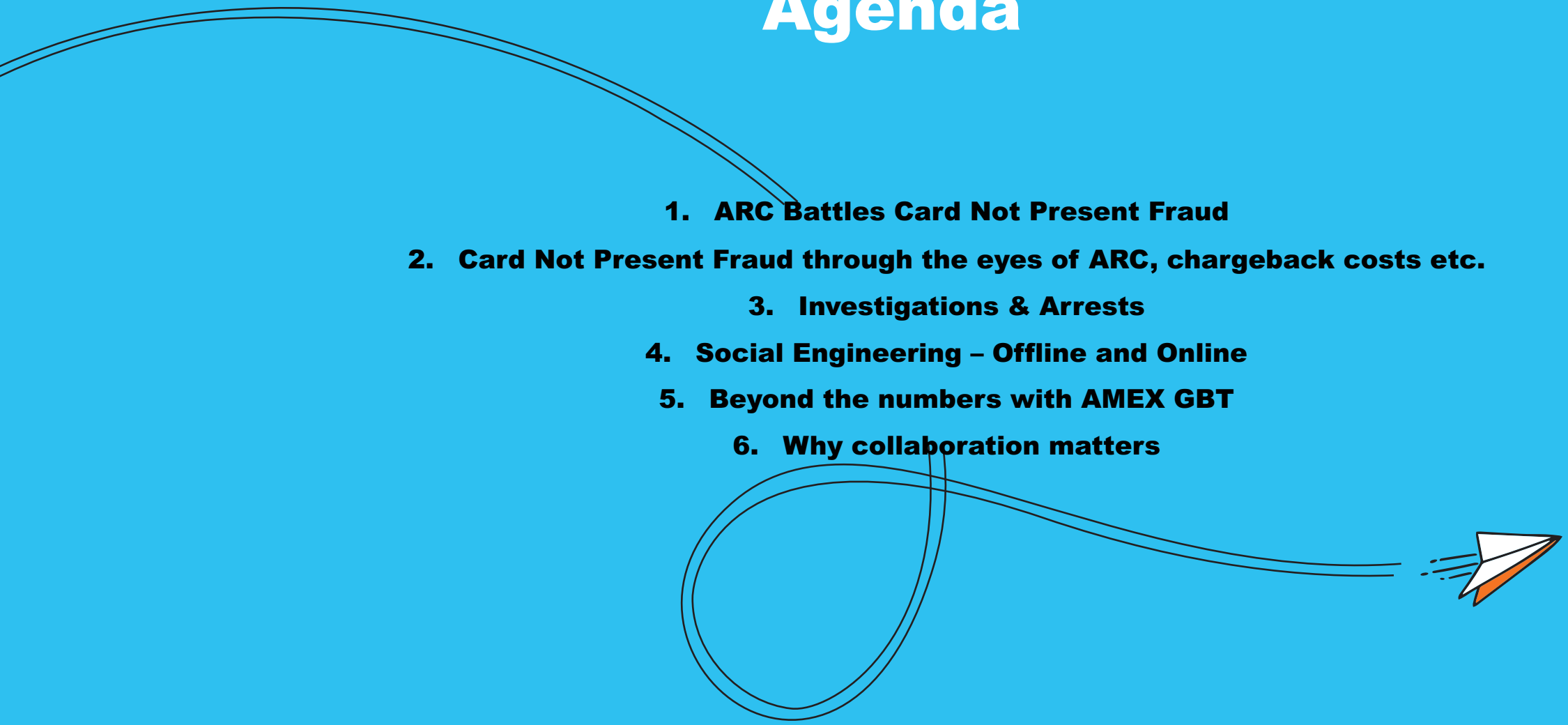
Doug Nass

Fraud Investigations Director

ARC

Agenda

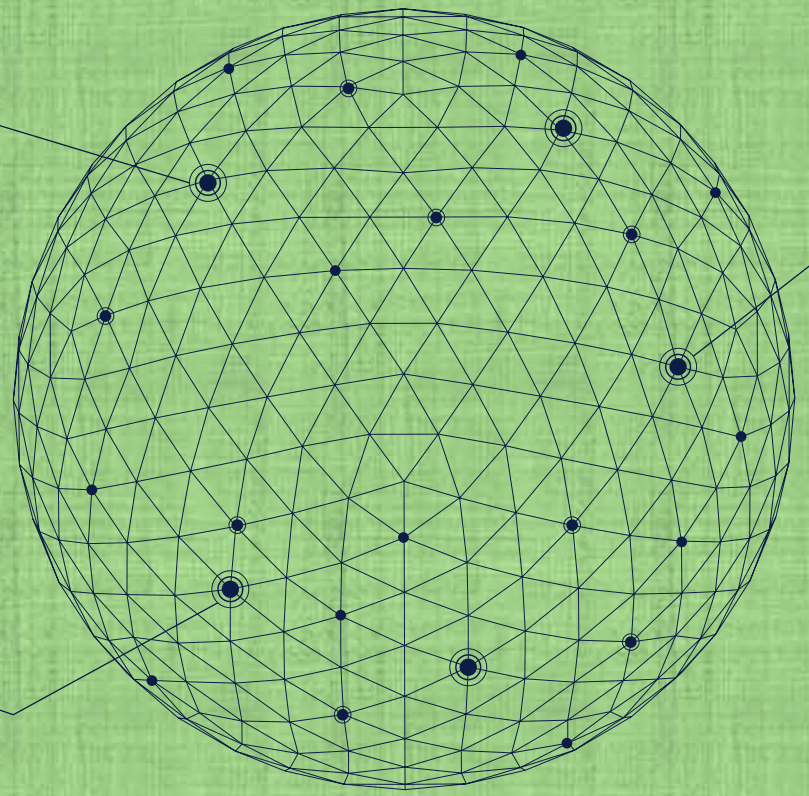
1. ARC Battles Card Not Present Fraud
2. Card Not Present Fraud through the eyes of ARC, chargeback costs etc.
3. Investigations & Arrests
4. Social Engineering – Offline and Online
5. Beyond the numbers with AMEX GBT
6. Why collaboration matters



By the numbers 2018

1% to 2%

Est. that of all flight bookings on websites are associated with fraud attempts



$25Billion

Projected losses across the travel industry in 2020

$858M

Impact of payment fraud on the travel industry

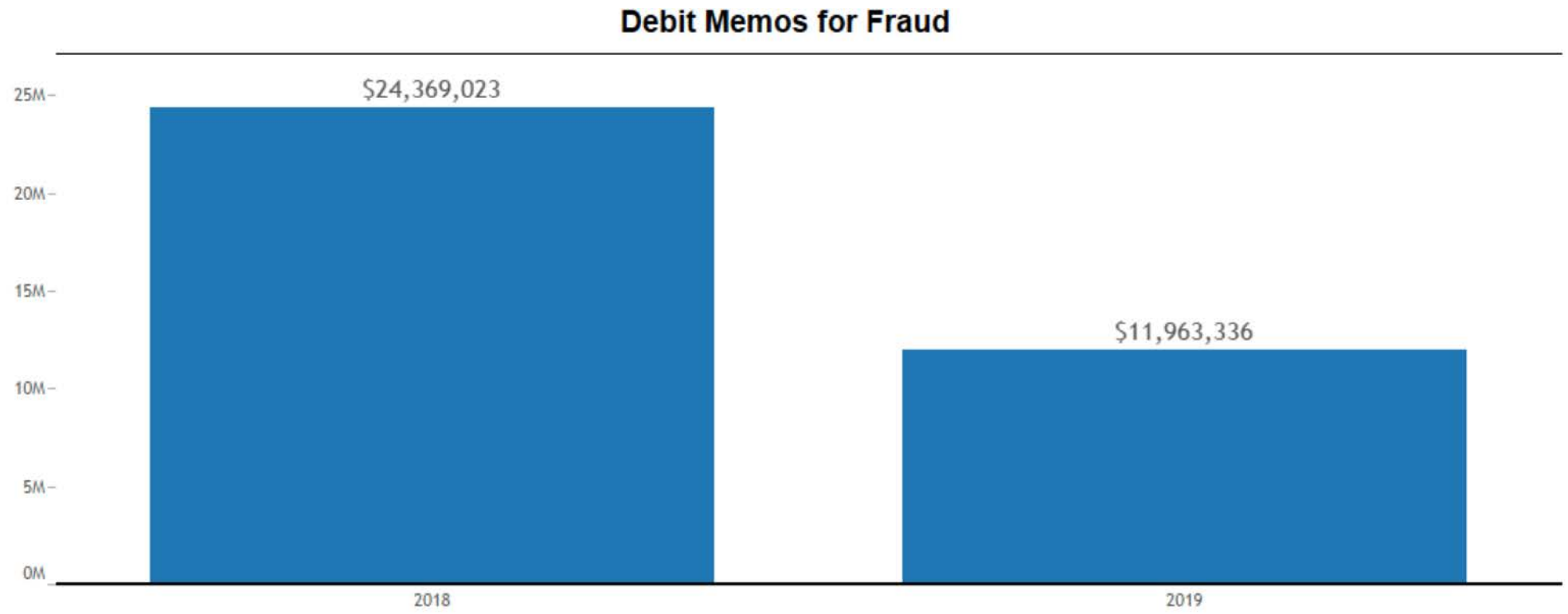
TRAVELCONNECT

1. *See generally*, IATA, *News Brief: Reducing Fraudulent Payment Transactions*, available at https://www.iata.org/pressroom/pr/Pages/2016-01-07-01.aspx.
2. *See generally*, Sift, *Machine Learning: The Future of Fraud Fighting in the Travel Industry*, available at https://pages.siftscience.com/rs/526-PCC-974/images/ebook-the-future-of-travel-fraud-fighting.pdf.
3. Per a global study commissioned by eNett International that Edgar, Dunn & Company carried out in November 2017 – January 2018. *See generally*, eNett International, *It Pays to Know: Fraud in Travel Payments*, available at https://www.enett.com/insights/fraud-form.

ARC

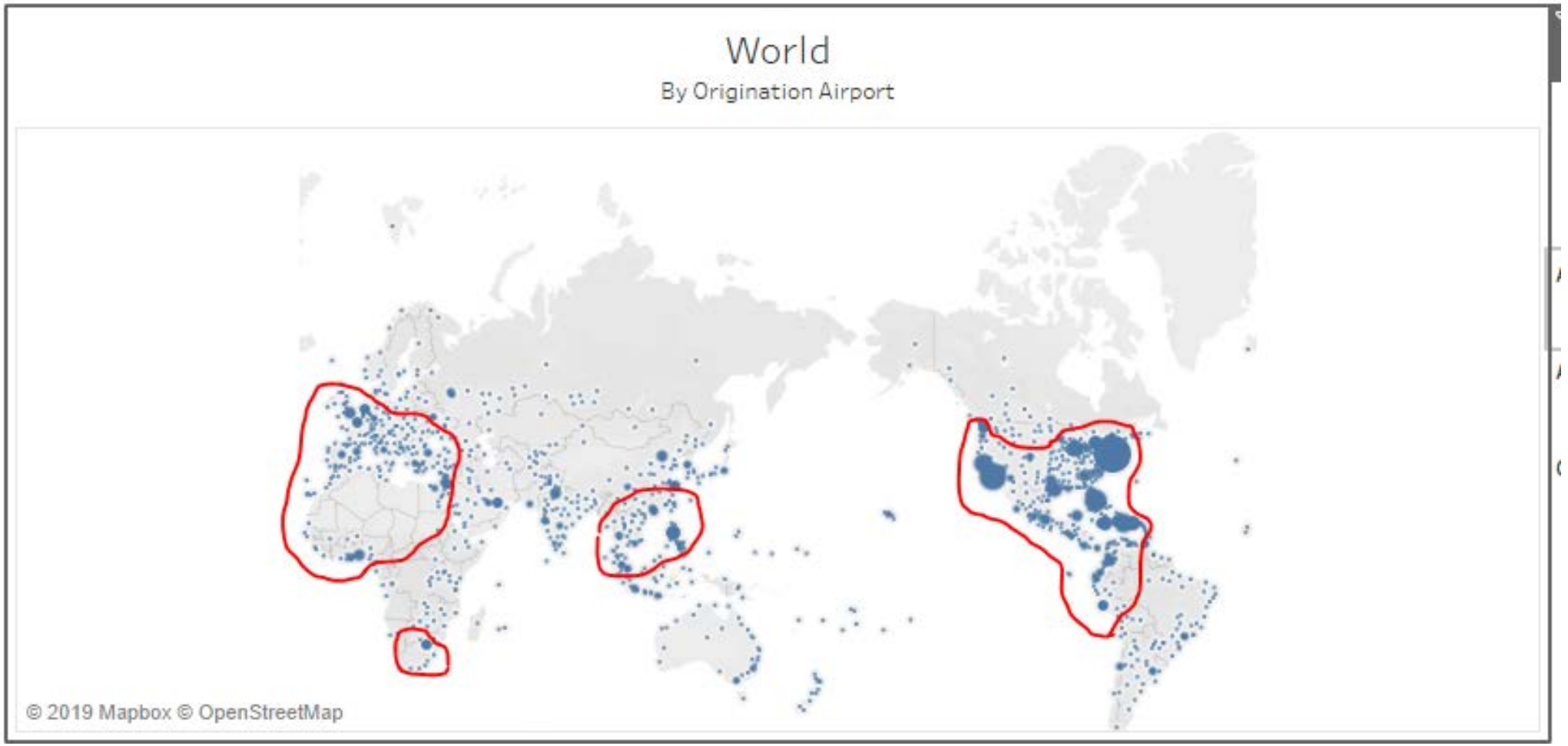
ARC Battles CNP Fraud

Tracking Fraudulent Memos - 2018



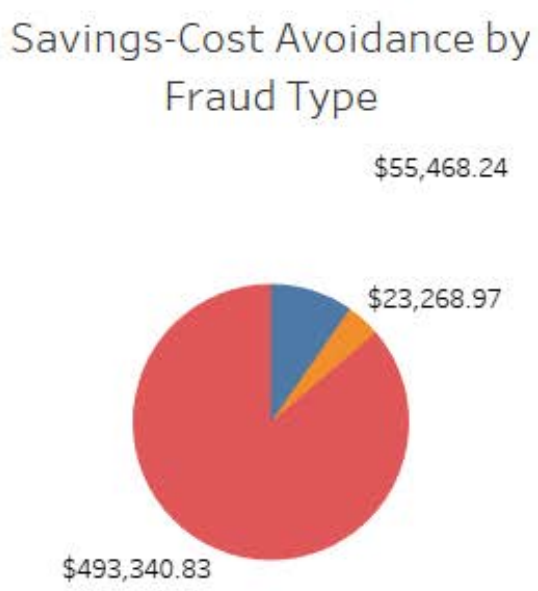
ARC Battles CNP Fraud

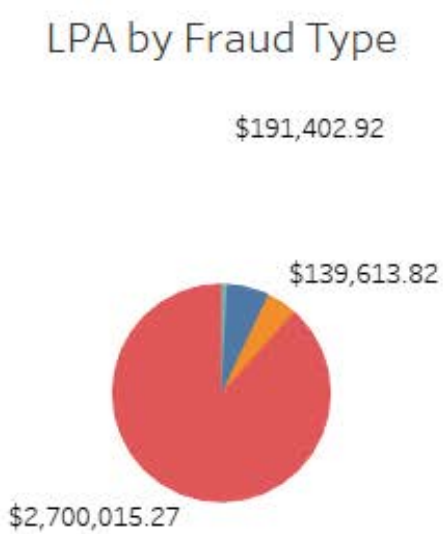
Geography of memos

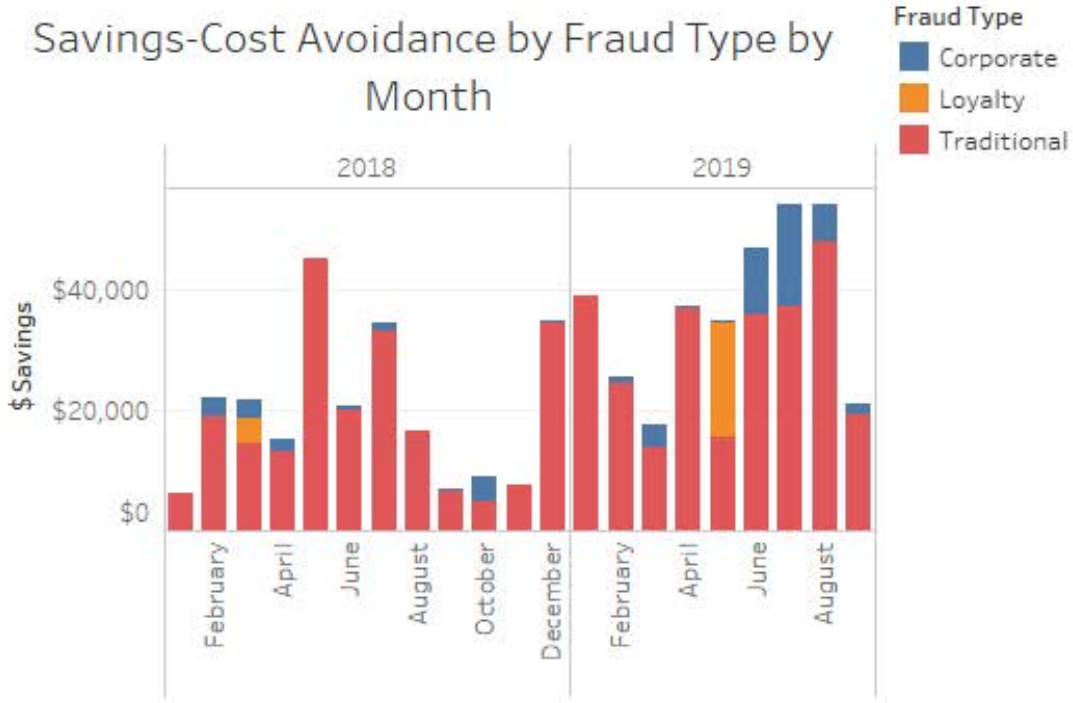


ARC Battles CNP Fraud

Statistics through the eyes of ARC







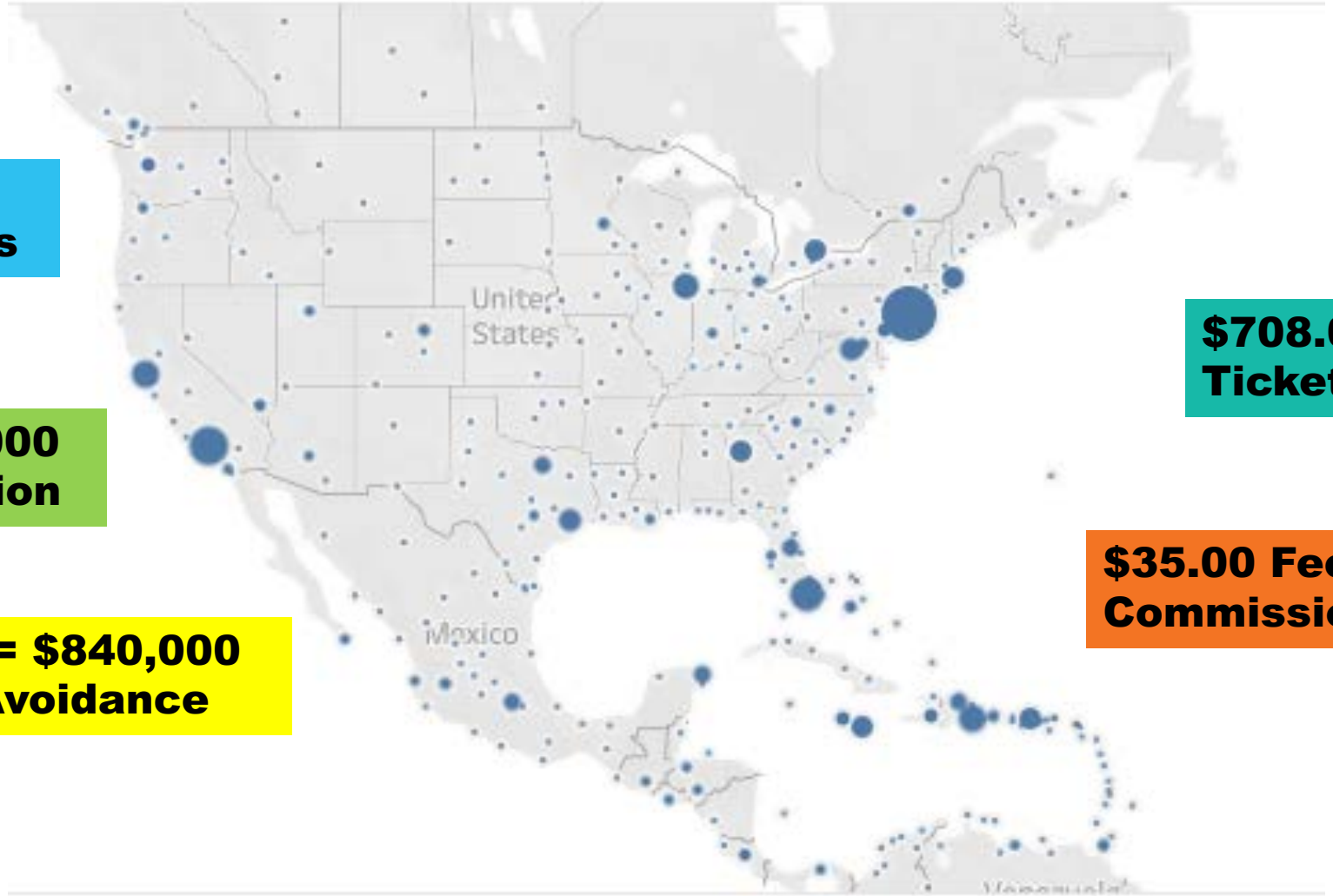
ARC Battles CNP Fraud

Cost of a Chargeback – ARC analysis

20 New Transactions

2017/18 = 25,000 New Transaction

2017/18 = $840,000 in Cost Avoidance

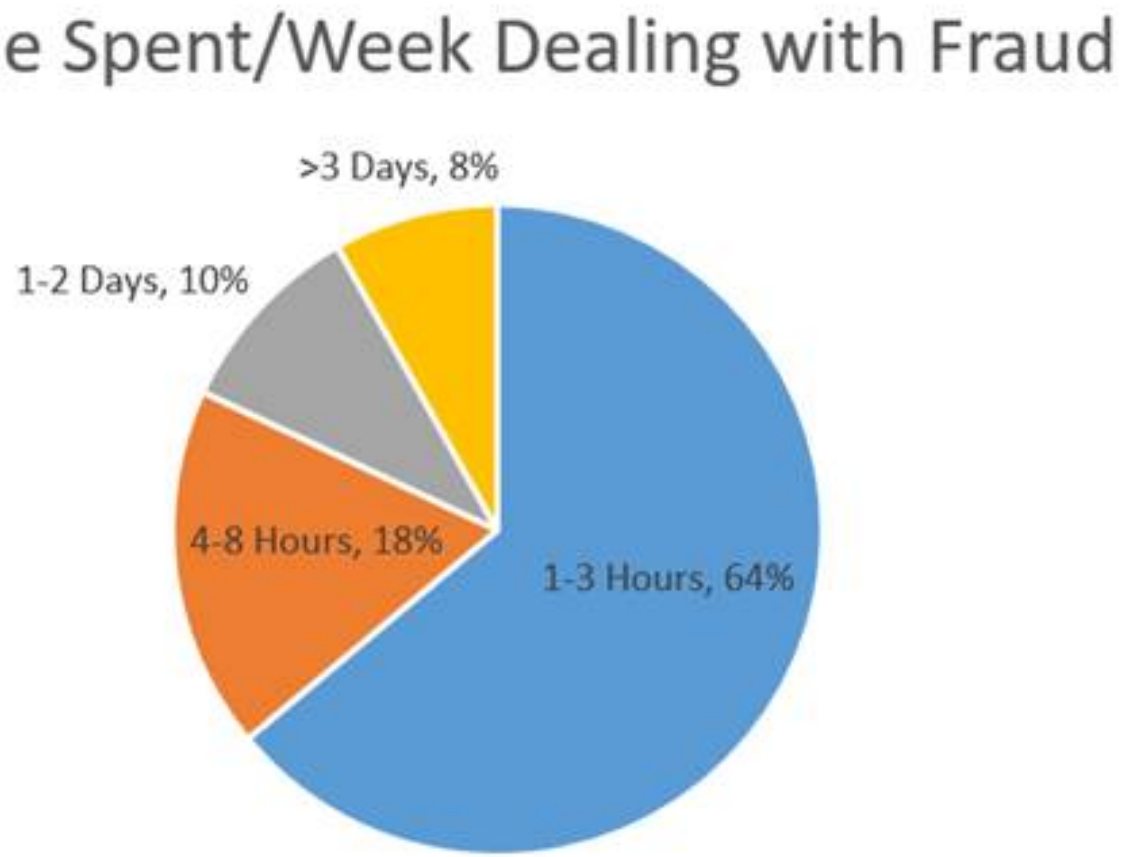


$708.00 Avg. Ticket

$35.00 Fee / Commission

ARC Battles CNP Fraud

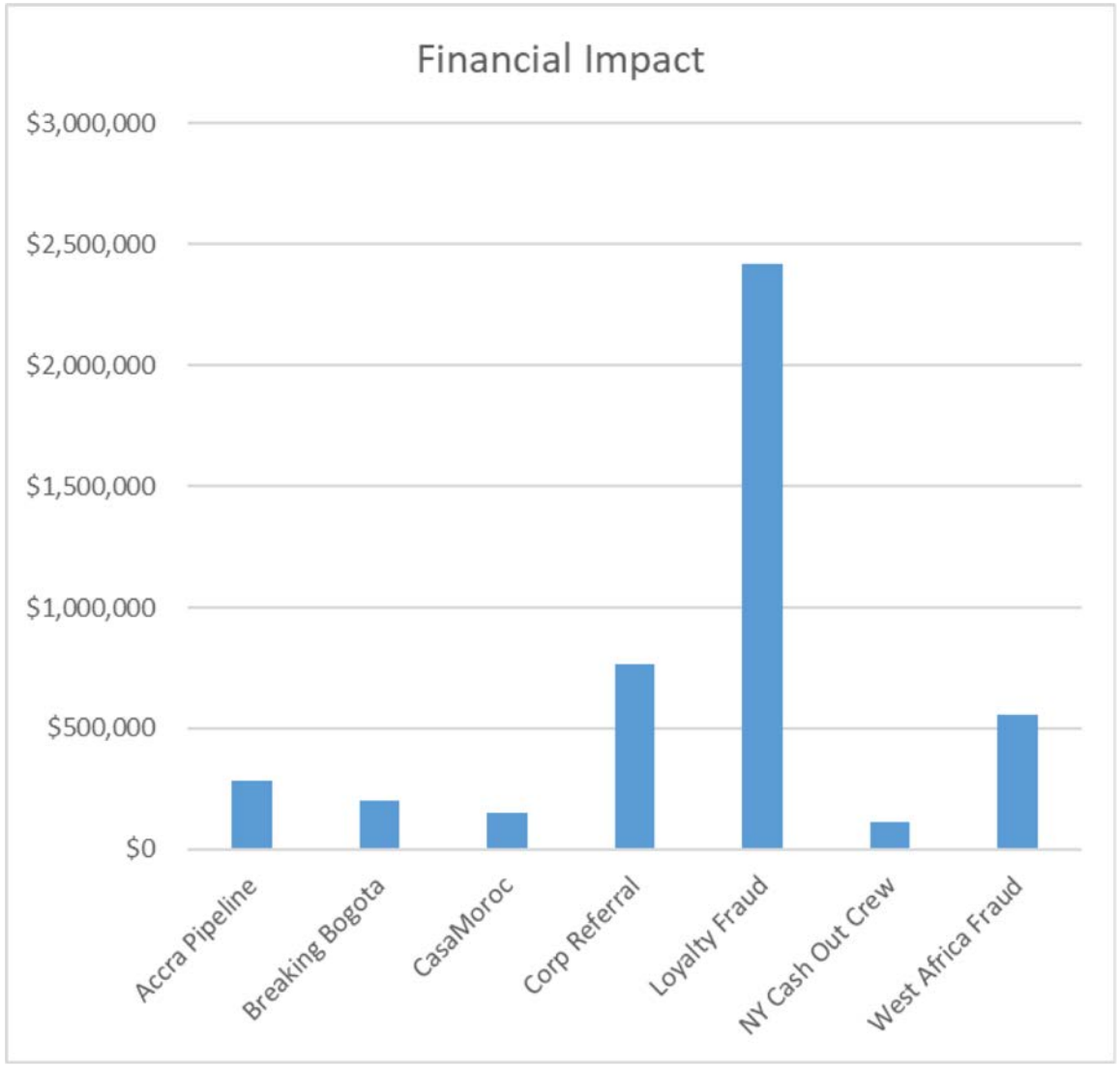
Cost of a Chargeback – ARC analysis

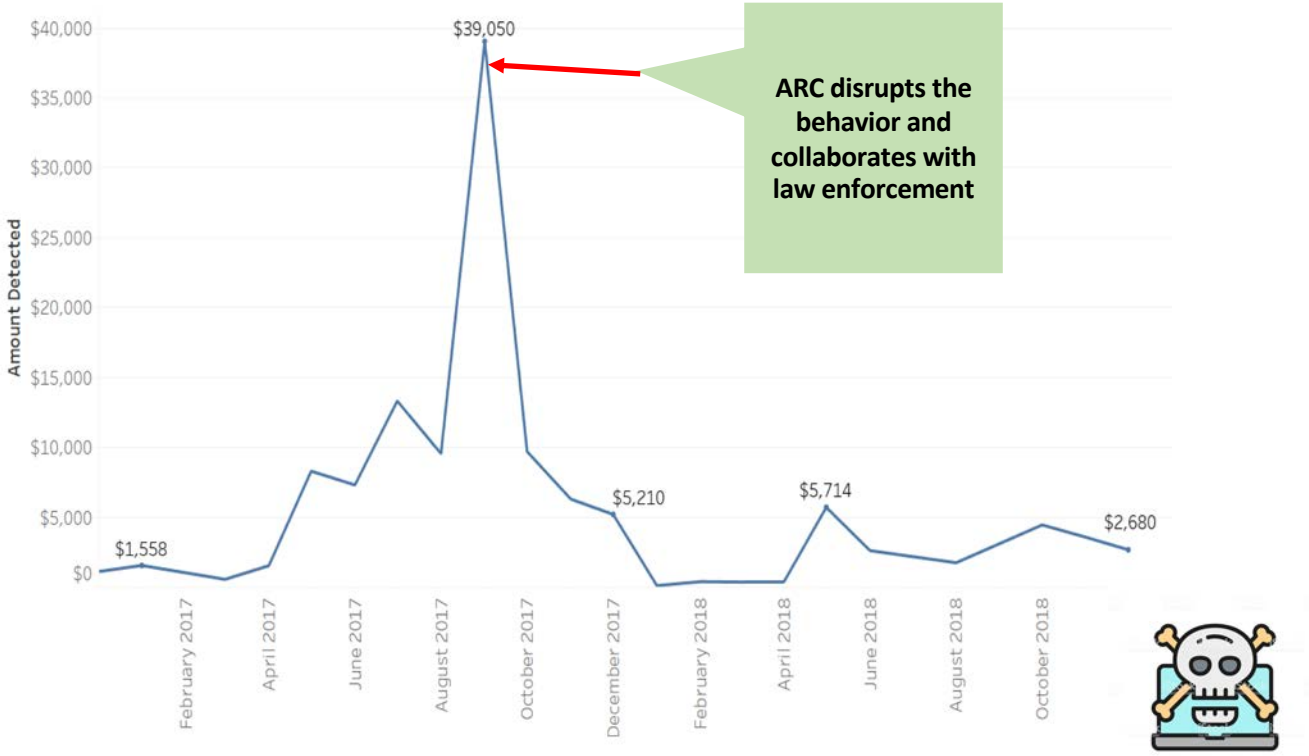


Investigations and Arrests

Positive, Effective and Timely Action - Results

Fraud Investigations





AMEX GBT & ARC

Social Engineering – Offline and Online

Business Travel Risks

Multiple online booking tools

Business travelers are more likely to book travel using a smartphone[1]

Company contact information is readily available online

Each product or service has a unique risk profile

Bad actors can pose as a fraudulent individual or fraudulent entity

Ripe Social Engineering Environment

See generally, Think With Google, *Travel Trends Revealed in Let's-Book-It Moments*, available at https://www.thinkwithgoogle.com/marketing-resources/micro-moments/travel-booking-trends-book-it-moments/.

Fraud Attempts are Increasingly Sophisticated

Impersonating key client contacts

Using spoofed phone numbers or email addresses of known individuals

Knowledgeable about basic authentication information

Targeting after hours desk or out-of-region desks

Social engineering to learn specific details of a travel program or create sense of urgency

Quote specific details about the account or prior travel

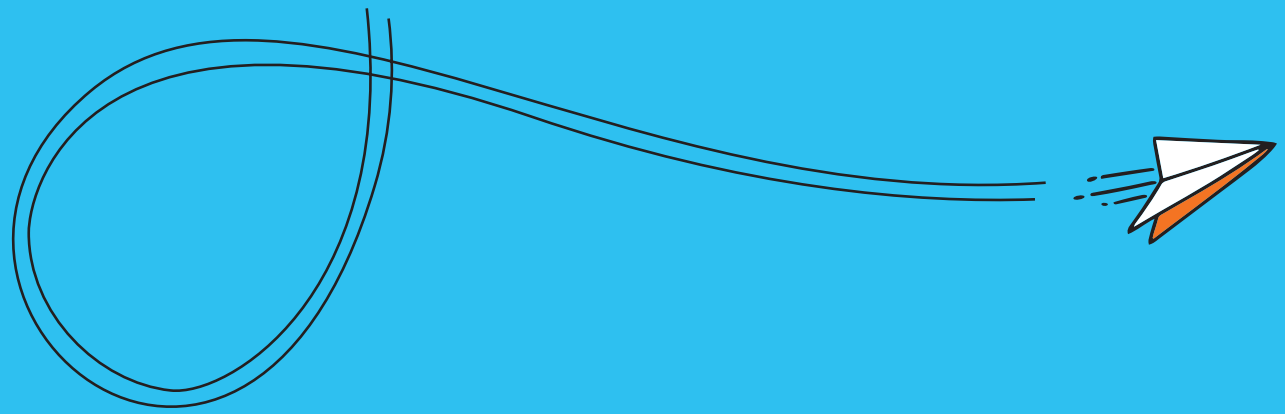
Online risks also prevalent

What Can you do to Mitigate Fraud Risk?

1. Design an effective Compliance Program
2. Understand your clients and their business
3. Implement controls
4. Train your first line of defense to identify red flags
5. Leverage new Technology via Machine Learning, e-verification and AI.

AMEX GBT

Beyond the numbers with AMEX GBT



Regulatory Guidance for Designing an Effective Compliance Program

The U.S. Department of Justice (DOJ) considers the following elements of a Compliance program when evaluating the effectiveness of a company's internal controls[1]:

- -Risk Assessments
- -Policies and Procedures
- -Training and Communications
- -Confidential Reporting Structure and Investigation Process
- Regular Testing & Audits of Program
- -Third Party Management
- -Mergers and Acquisitions

[1] *See generally*, US Department of Justice, Criminal Division, Fraud Section, *Evaluation of Corporate Compliance Programs*, available at https://www.justice.gov/criminal-fraud/page/file/937501/download.

Additional Regulatory Guidance:

Organization for Economic Cooperation and Development

United Nations

World Bank

Federal Reserve

UK's Serious Fraud Office

French Anti-Corruption Agency

Federal Bureau of Investigation

Department of Homeland Security

Other industry partners & data sharing relationships

Understanding Your Client – KYC and CDD

CLIENT INFORMATION AND BEHAVIORS

- Verify the client's true identity - name and address
- Verify the client's business - beneficial ownership information; tax or equivalent government identification number
- Internal risk ratings

PROVIDE BETTER SERVICE

- Understand their business and travel needs
- Recommend additional products or services
- Protect the client

DETECT UNUSUAL OR SUSPICIOUS ACTIVITIES

- Information does not match that which is found online
- Prospective client contact unable to provide details of relationship with client
- Requests information about travel that is not typical of this type of client
- Excessive questions as to legal or regulatory restrictions
- Reluctance to provide information

Authentication Controls

Online	Offline
Two factor authentication	Ask additional questions • DOB • Last 4 digits of credit card on record • Employee ID (where available)
E-verification	Two-factor authentication in offline environment (send an email to the email address on file or call the number on file)
Ensure log-ins are from an existing corporate email address	Contact the client travel manager to verify a request
Trusted IP address list	Prior travel history

Training & Technology Controls

- Communicate responsibilities to your first line of defense and client managers
- Prepare letters and talking points for client-facing teams
- Provide frequent and updated training on red flags and fraud escalation procedures
- Certification requirements
- Machine learning and Artificial Intelligence- predictive analytics for abnormal travel patterns
- Automated fraud routine – establish criteria to reject or flag potentially suspicious records
- Digital profiling – profile created from data based on every time a traveler interacts with a service, app, or webpage
- High-risk jurisdiction suppression directly in booking tool
- Remove auto-ticketing for high-risk jurisdictions so those bookings undergo an additional review
- Turn off “guest booking” feature

ARC

Training Your First Line of Defense

The first line of defense must be alert for red flags

Caller cannot answer client validation questions – be cautious as many details are easily obtained online or through criminal activity; nor confirm most recent travel or other prior bookings

Caller requests changes to email address, phone number, or email or phone numbers that do not match client standards

Travel requests that violate client policy

Caller is focused on refunds or exchanges

Caller cannot confirm payment details within profile / used in previous bookings

Caller uses an unusual or unprofiled method of payment and/or requests the method of payment to be updated

Method of payment is declined, and/or multiple methods of payment are attempted and declined

Caller cannot pronounce the name of the client company

Unusual travel routing (e.g. intra-African travel for a US-based traveler)

Excessive flattery or sense of urgency-- this is called social engineering and used to manipulate you (e.g. claims to be a client VIP (CEO or Chairman) or key client contact (Travel Manager)

Enhanced Screening Controls

Sanctions Lists

- Office of Foreign Assets Control (OFAC) of the US Department of the Treasury
- Her Majesty's Treasury – Office of Financial Sanctions Implementation
- EU Consolidated List
- US Department of State – Terrorist Exclusion List; Iran, North Korea, and Syria Nonproliferation Act

Internal Lists

- Known Fraudulent Travelers
- Prohibited Transactions (individuals and entities)

Third Party Screening Tools (e.g., LexisNexis Bridger, BAE NetReveal, Dow Jones)

Additional Information Screening (DOB, payment history, past travel)

What to do if fraud is suspected

Place a reservation on hold until the traveler's identity can be verified

Document the fraud attempt and escalate internally

Report substantiated fraud to appropriate law enforcement

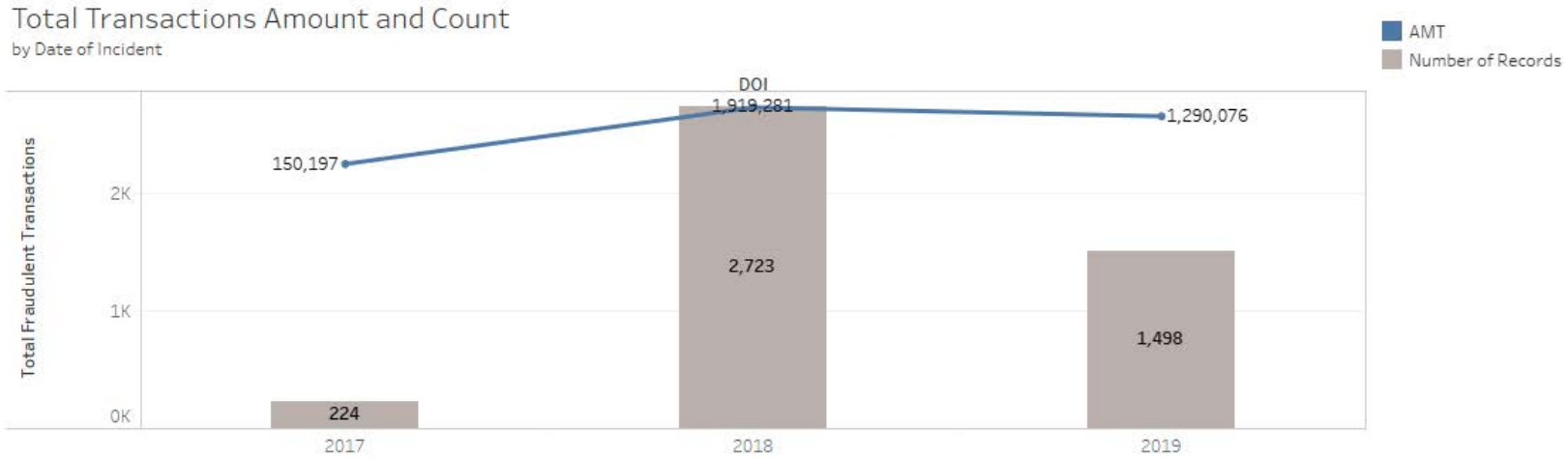
Debit memo impact & reduction

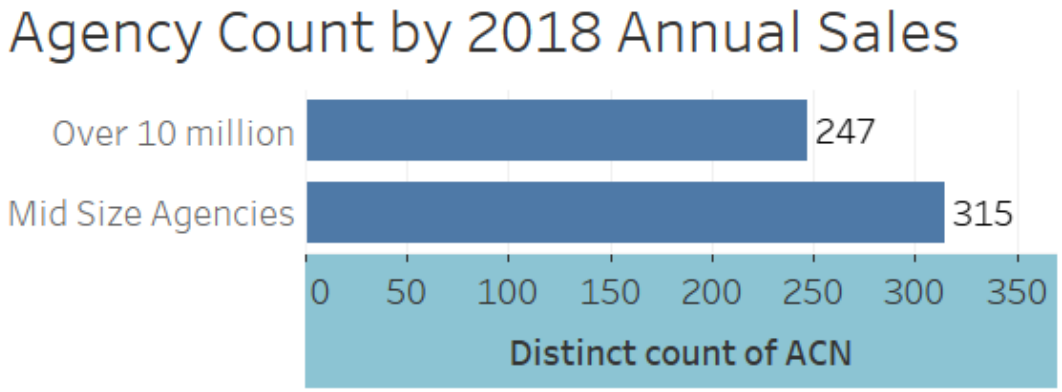
AMEX GBT & ARC

Why collaboration matters

ARC Battles CNP Fraud

Statistics through the eyes of ARC





Industry Information Sharing

- ARC Fraud Alerts and Best Practices
- ARC Risk Check Powered by Perseuss
- IATA Industry Fraud Prevention Initiative
- Strategic Industry Partnerships
- National Cyber-Forensics & Training Alliance

ARC Risk Check

Fraud Detection for the Travel Industry

ARC Risk Check, powered by Perseuss, is a global fraud-mitigation tool for small to mid-sized travel agencies made stronger by the combined intelligence of its participants.

Artificial Intelligence (AI)

Using AI algorithms, ARC Risk Check searches 3.2 billion data elements for instances of fraudulent activity, including **real, world-wide travel bookings**.

Community

What makes ARC Risk Check unique is the combined intelligence of **actual reports** from people throughout the travel industry.

Risk Score

ARC Risk Check delivers a **data-driven Risk Score** that agencies can use in making decisions whether to accept or block a potential customer.

Backed by Professionals

Only ARC Risk Check makes ARC **fraud mitigation professionals** available to subscribers at no additional cost.