Leveraging Geolocation Technology, Machine Learning & AI to Detect and Mitigate Mobile Payment Fraud

Presented by Donald Frieden, CEO, P97 Networks

IDENTITY & PAYMENTS SUMMIT
SECURE TECHNOLOGY ALLIANCE | Feb 24-26, 2025

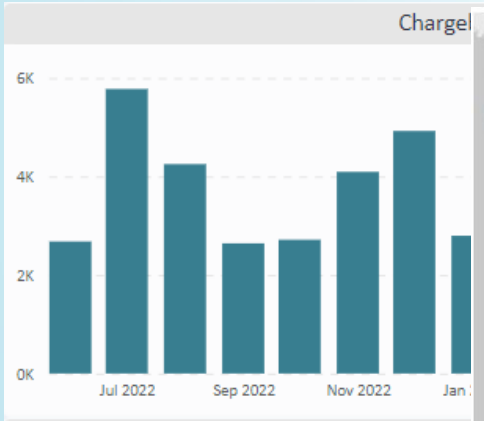
Fraudster Behavior & Trends with Digital Wallets

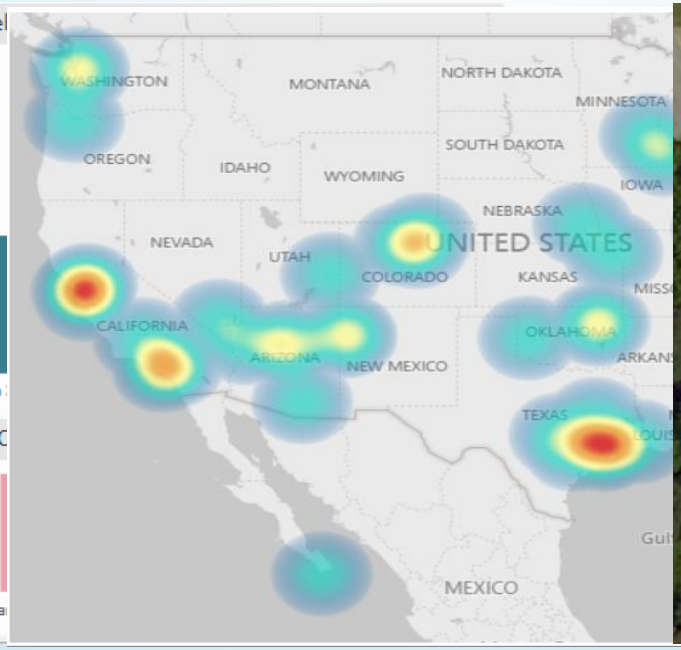
Our Fraud Mitigation Journey & Learnings

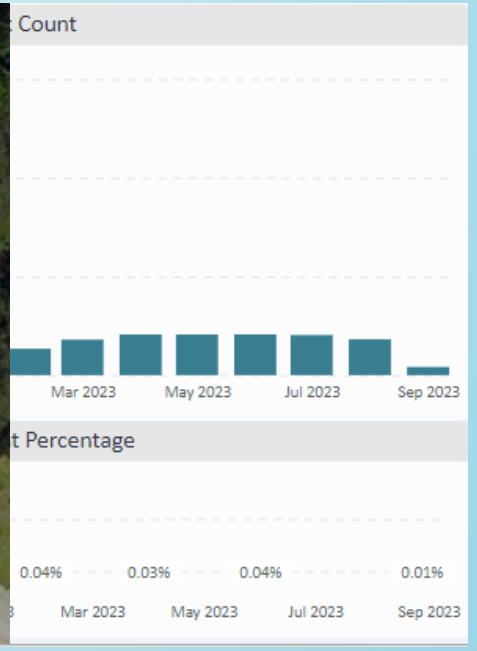
July 2022: With ~50,000 retails sites and 20M registered users, our clients started experiencing a surge in fraud and higher than normal chargebacks

2022/23: P97 started developing an Advance Fraud Detection and Monitoring Platform , including 120+ new mobile payment data & fraud monitoring tools, ML models and fraud blocking techniques

Dec 2023: P97 's Advanced Fraud mitigation solution built on a multi-layered, machine learning and automated scoring engine has reduced our enterprise-wide chargebacks from 0.30% to 0.01%, with a flat decline rates





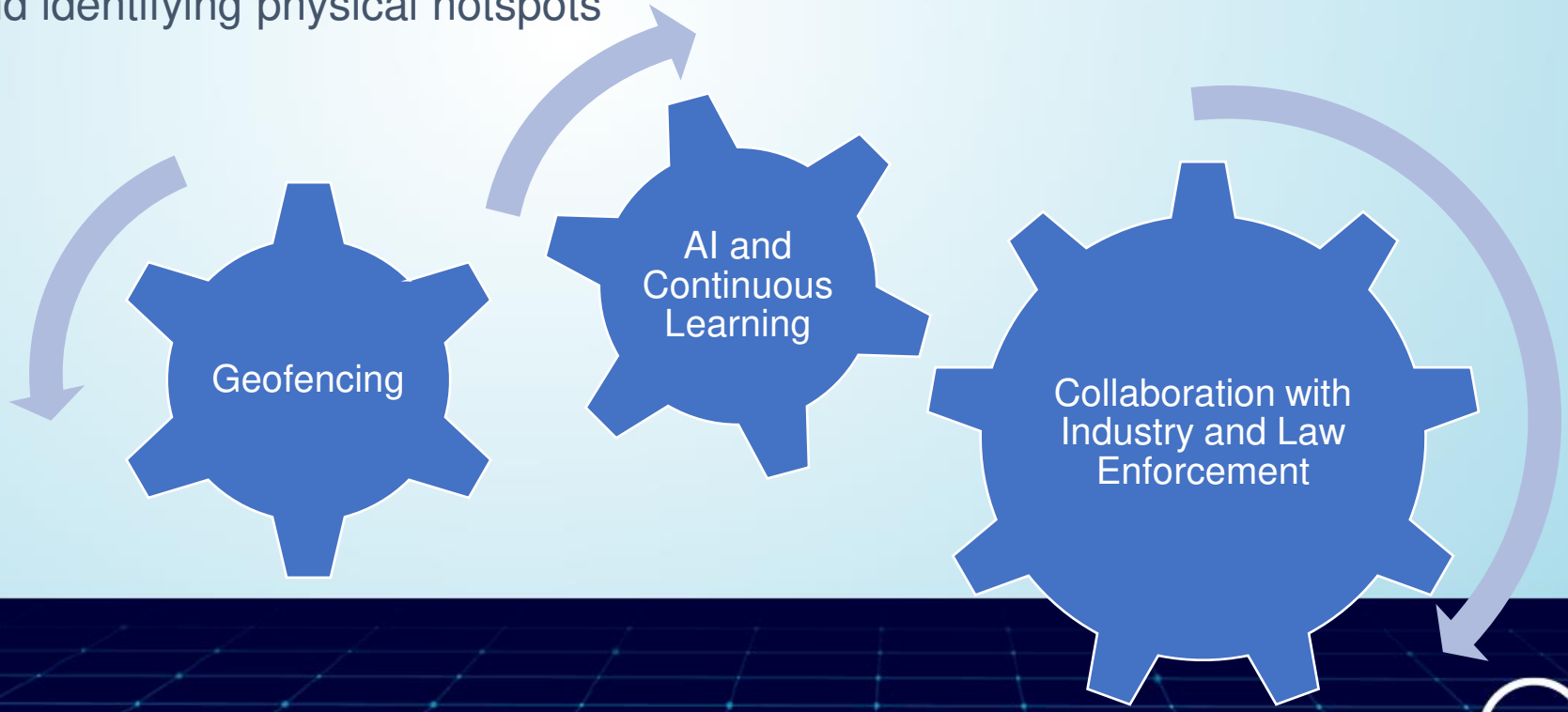


Understanding Fraudulent Behavior

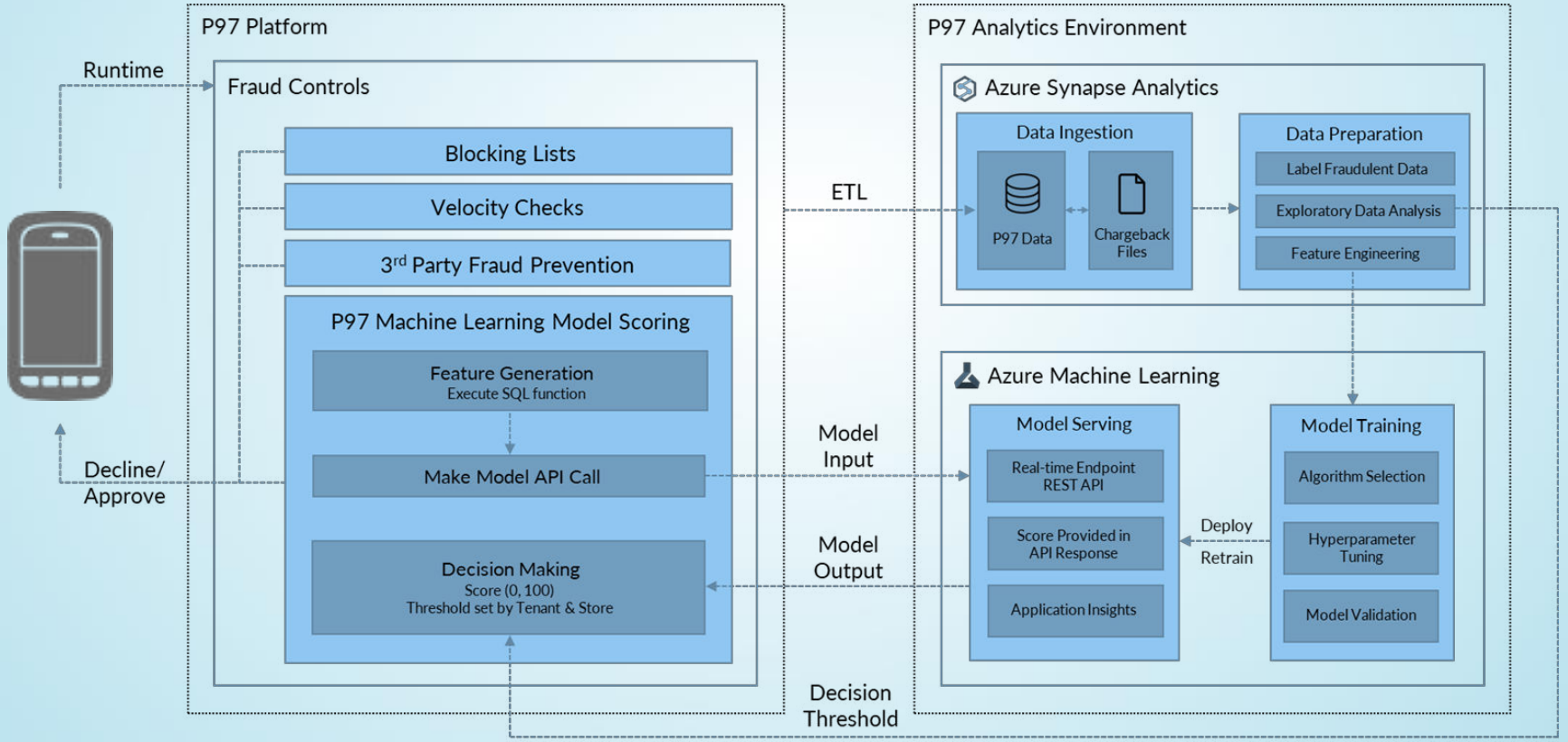
1. **Fraudsters Acquire Lists of Stolen Credit Cards**
   - Bulk purchasing of credit card lists often sourced from the dark web
2. **Download Mobile Payment Apps & Create New User Accounts**
   - Leverage apps and generic email for automating identities and authentication
3. **Use Mobile Apps to Enroll Cards and Test Status**
   - Load stolen credit cards in mobile payment apps and attempt ‘pre-authorizations’ to test status, but do not finalize transactions
4. **Distribute Validated Cards**
   - Fraud rings distribute PAN data to their networks
5. **Fraud Rings Target Outdoor Payment Terminals and Fuel Sites**
   - Fraudster purchase fuel using Blatter Trucks to maximize value against pre-auth limits

Using Geolocation Technology and Analysis to Proactively Detect and Mitigate Fraud

- **Locating and Preventing Criminal Activity:** Using geolocation technology and multi-layered, automated systems that leverage machine learning and scoring models provide tools for combating fraud and identifying physical hotspots



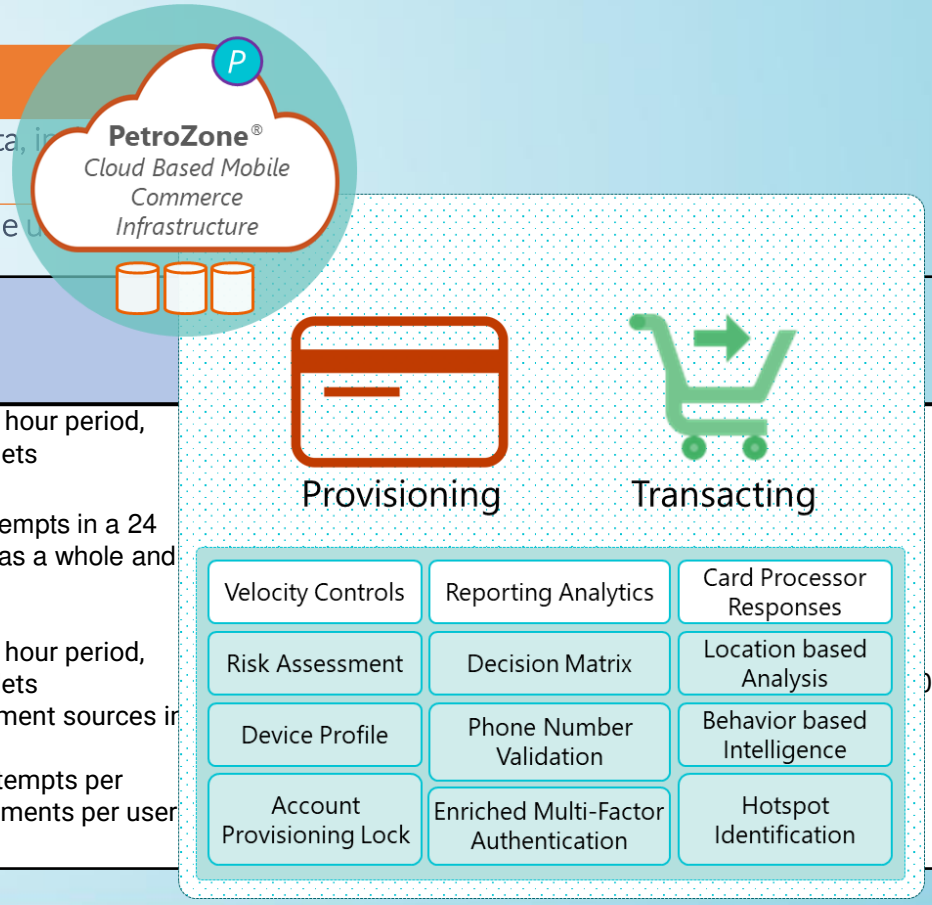
Developing a Fauld Analytics & ML Platform



100's of Rules and Methods

Method Name	Summary
Model Zero	Evaluation of user payment source token data and mobile device geolocation data, i… distance of provisioning event from billing zip code
Distinct Count Billing Postcode	Dimension on Model Zero, count of distinct billing zip codes provisioned by single u…
Model One	
Hotspot	
Phone Number	
Email Evaluation	
Blocked User and T… Network	

P97 Rule Name (blocking rules, reporting rules, accepting rules)	P97 Action	P97 Definition
Velocity.DailyPurchaseAttempts (configurable as a whole and for wallets)	AuthDecline	limit the number of attempts in a 24 hour period, configurable as a whole and for wallets
Velocity.Device.DailyPurchaseAttempts (configurable as a whole and for wallets)	AuthDecline	The number of allowed purchase attempts in a 24 hour period for device, configurable as a whole and for wallets
Velocity.DailyPurchaseAttempts configured by wallet combined with Velocity.WalletCardsUsageLimit	AuthDecline	limit the number of attempts in a 24 hour period, configurable as a whole and for wallets the number of allowed different payment sources in a chosen period for device can limit the number of purchase attempts per wallet and the number of card enrollments per user and device



Key Techniques, Data, Methods, and Analytic Models for Detecting Fraudsters

Billing Postcode Analysis

- Monitoring distance between billing zip codes and provisioning location

Geolocation Analysis

- Monitoring identified fraud ring hotspots, locations, and geolocation epicenters

Phone Number Analysis

- Validating phone numbers by carrier network, contract type, and user connections

Email Evaluation Analysis

- Verifying email address by domain name, top-level domain(TLD), and ICANN registered lists

Key Tools Developed for Detecting and Blocking Mobile Payment Fraudsters

Emulation Protection

- Tools to prevent fraud transaction attempts through sophisticated Device Emulation associated with large-scale fraud rings

Industry Wide Fraud Prevention Network

- Automated and network wide blocking of fraudsters by Device, Payment Credential, Token, User, Email, Phone Numbers, or other data collected from hot spots, chargeback data, and fraudulent behavior

Continuously Learning Models And Real-Time Fraud Data

- Dynamically adapting models based on real-time fraud data, evolving payment methods, behaviors, patterns, and locations that fraudsters try to exploit

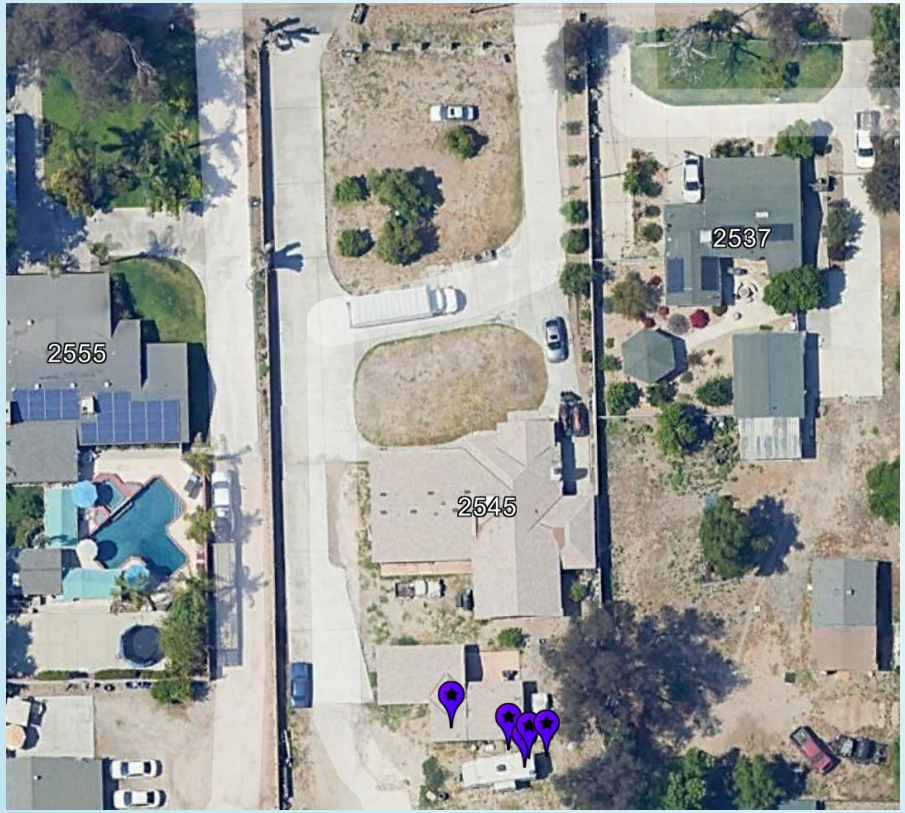
Partnering With Law Enforcement

- Collaboration with Financial Crimes Task Forces and payment acquires to expose criminal behavior using data points from confirmed fraudulent transactions and behaviors

Using Geolocation Data to Proactively Mitigate Fraud

- **Locating Criminal Activity**: We leverage geolocation data from confirmed fraudulent accounts to identify physical hotspots where fraudsters frequently load stolen credit cards.
- **Geofencing**: When an event occurs within a geofenced area, our advance fraud detection service immediately tags associated attributes for automatic blocking and updates our transaction scoring models to further improve fraud detection.
- **Customer-Agnostic Protection**: We harness fraudulent data across our entire tenant portfolio, empowering us to proactively prevent fraud for all P97 customers

Anything look interesting or unusual in these pictures?



Applying Geolocation Technology and ML to Detect and Mitigate Mobile Payment Fraud

- **Outstanding Results:** Fraud at less than **0.01% of sales** across all P97 managed clients.
- **Proven and Powerful**: Multi-layered, automated systems that leverage machine learning and scoring models to combat fraud from multiple angles.
- **Collaborative Fraud Management**: Trusted by the industry leading brands to proactively identify trends and refine/adjust controls to ensure optimal protection against evolving threats.
- **Adaptive and Self-Training**: Continuously learning from real-time fraud data, dynamically adapting to evolving payment methods, behaviors, patterns, and locations that fraudsters exploit.
- **Automation Across industry**: Directly integrated with acquirers to pull chargebacks in near real-time, blocking fraudsters and continuously updating our fraud models with new fraud data and ensuring constant adaptation to new fraud patterns.
- **Law Enforcement Partnerships**: Actively collaboration with local law enforcement task forces, sharing insights to stop fraudsters and extend fraud prevention efforts beyond our platform.