Travel Industry
Age of Digital Commerce

Advancements in data technology especially social, mobile, analytics and cloud have transformed the travel industry completely.
Digital Disruption in the Travel Industry

The proliferation of smartphones has provided consumers across the globe with the ability to conveniently search for, compare, and book travel. With the power to plan and execute at their fingertips, consumers have shifted their behavior and increased their expectations. Heavily influenced by technology, consumers are demanding immediate gratification and seamless experiences.

Today’s leading brands are constantly innovating in order to stand out in a highly competitive industry. Customized offerings, frequent communications, attractive loyalty programs, and streamlined experiences are some of the strategies travel businesses are using for growth and retention. In addition, businesses that are able to protect customer data and provide assurance around payment and account security, will have a competitive advantage.
One of the Largest and Most Complex Industries

Travel and tourism now accounts for a staggering 10.2 percent of global GDP and includes both leisure and business travel. Ranging from small agencies to multinational aggregators, the travel industry includes a diverse range of players. Each one of these players varies in region, scope and scale of business as well as in technological involvement.

Highly mobile, the travel industry is ranked fifth in global industry mobile technology adoption. Travel apps are one of the most popular categories in the Apple App Store with a 3.9 percent share of all active apps.

Seasonality introduces additional complexity for travel businesses, along with changes in climate and economic conditions.

Sources: Deloitte, 2018; Statista, 2019
Customers Are Dictating the New Age Language of Travel Behavior

Race for Extreme Personalization
In an age of choices and discovery, customer loyalty is harder for businesses to maintain. Travelers demand best-in-class experiences that are most relevant to them. Personalized marketing and experiences show promising potential as brands hustle to be top-of-mind for customers.

The New Customer Impulsiveness
Unlike meticulously planned travel arrangements made far in advance, today's customers are finding value in the flexibility of last-minute bookings for flights, hotels, and rentals. Impulsiveness and immediate gratification have become the new norms guiding customers’ purchasing decisions.

Rise of the Sharing Economy
To get best-in-world experiences without spending to own, customers have become open to sharing and renting as opposed to owning. Using this to their advantage businesses are trying to go asset-lite as well. As a result, today’s biggest ride hailing service owns no fleet and the largest accommodation marketplace has no rooms of its own. As consumers share more, the only asset worth investing remains the brand.

Consequences of Bad Customer Experience
The digital world has enabled users to validate online claims through user reviews. Thus, many consumers today are often guided by influencers or opinion leaders. Powered by review systems and amplified by social media, the bad experiences of a few can now have detrimental effects on a business’ reputation and brand.
Travelers Are Looking for a Seamless Experience

- Easily Accessible Information
- Friction-free Bookings
- Confirmed Payments
- Secure & Reliable
Businesses Are Trying to Put Their Best Foot Forward

Digital-First Operations

Digital payments, digital itineraries and digital check-ins have paved the way for completely differentiated customer experiences.

Personalized Offers

Using customer history, businesses are tailoring offers to retain customers and bolster their brands through programs that provide rewards based on continued interactions.

Customer Experience

Technology has enabled businesses to improve the customer experience, making it easier and more convenient than ever to plan and book travel.

Monitoring for Security and Assurance

To strengthen their brands and provide customer security, businesses are proactively managing cyber threats and fraud attacks.

Digital payments, digital itineraries and digital check-ins have paved the way for completely differentiated customer experiences. Using customer history, businesses are tailoring offers to retain customers and bolster their brands through programs that provide rewards based on continued interactions. Technology has enabled businesses to improve the customer experience, making it easier and more convenient than ever to plan and book travel. To strengthen their brands and provide customer security, businesses are proactively managing cyber threats and fraud attacks.
Number of Fraud Attacks Continue to Rise

The travel industry is an attractive target for fraudsters aiming to monetize stolen payment credentials or take over unsuspecting customer accounts. Leveraging peak periods to launch attacks, fraudsters attempt to remain undetected among the scores of travelers planning their holiday getaways.

Across multiple types of attacks, the number of fraudulent cases detected by Simility continues to show a steady uptick.

Source: Internal Simility data, 2018
Most Common Fraud Attack Types

Fraud continues to grow in complexity and sophistication as fraudsters devise different tactics to evade detection. Some of the most commonly observed fraud types include:

**Payment Fraud**
• The use of stolen payment credentials to make unauthorized purchases
• Results in chargeback losses

**Identity Fraud**
• The use of stolen or synthetic identity credentials to open accounts
• Often to sell stolen or counterfeit goods

**Account Takeover Fraud**
• Gaining unauthorized access to another user’s account
• Often not immediately caught because the fraudster initially appears as the registered, trusted user
Multiple Travel Services Are Increasingly Being Exploited by Fraudsters

Once fraudsters find a way to defraud the system through fraudulent payments or unauthorized access to a user’s account, they typically don’t stop there. In order to maximize returns, fraudsters target a variety of travel services.

While fraudsters move between services, they learn about vulnerabilities and try to exploit the same weaknesses across other services offered by the platform. Connections between their devices, profiles, and behaviors vary drastically from those of a normal user.

The challenge faced by organizations with multiple travel service offerings is to consolidate data from different services and derive meaningful analytics that can then be used to fight fraud.
As mobile traffic continues to rise, mobile fraud has remained relatively low at 29.8%. Although customers use mobile devices to research and explore travel options, they’re more inclined to make final arrangements on a desktop.

Desktop transactions are over 40% more risky given it is easier to launch large scale attacks from a desktop. Mobile is used to a greater extent for browsing, searching and social.

Fraud in the travel industry typically originates from traditional website bots. These bots use desktop browsers and continue to account for a majority of overall fraud experienced by travel customers today.

Source: Internal Simility data, 2018
Obsolete Technology Continues to Pose Challenges

Simility’s data from the travel vertical suggests that the highest fraud rates are experienced on outdated desktop operating systems.

The use of older operating systems enables fraudsters to avoid crucial security and anti-piracy updates. These vulnerabilities are often overlooked.

Due to the limitations of orchestrating BOTs and hacking attacks on mobile devices and guided by controlled mobile app experiences, fraud on mobile operating systems has managed to stay within a limited range.

Source: Internal Simility data, 2018
Commonly Found Fraud Identifiers Across Diverse Fraud Types

Simility analyzed data across multiple fraud types to identify common fraud indicators.

In a majority of cases, usage of common identifiable risky elements denotes the fraud attacks targeting travel businesses. These vary in choice and complexity of device attributes, network attributes, as well as the choice of account credentials.

Identity spoofing accounted for 23.7% of total fraud cases analyzed, which ranged from downloading masking software on mobile phones to the usage of anonymized proxies.

Cases from repeat offenders accounted for 18.9% of total fraud cases. Entities associated with these attacks were previously associated with one or more fraudulent cases. These cases could be tied back to those entities by using Simility data intelligence, blacklists and historical profiles of device, user, etc.

Interestingly, in 15.3% of the total fraud cases, fraudsters tried to operate using a standalone BOT or as a part of distributed BOT attacks. Depending on device discrepancies as well as user behavior across multiple checkpoints, these cases easily stood out from genuine users.

Source: Internal Simility data, 2018
The ABCs of BOT Attacks

Hackers or fraudsters write a small script, wrap it in freeware and distribute it over the internet. This script has the ability to follow its maker’s commands and act accordingly.

By remotely activating numerous BOTs spread across the internet, fraudsters create brute force attacks to extract information or gain control of genuine accounts.

This is an example of a BOT attack launched from a single device by a fraudster, scaling up to 25 login attempts from the same BOT network.

Source: Internal Simility data, 2018
7 Identifiers to Holistic Fraud Management for Travel Businesses

With more connected and complex business services, the data generated is equally diverse and complicated. Travel businesses need a solution that combines various disparate data sources and adapts over time to keep pace with evolving fraud.
The Age of Machine Learning

Successful use of machine learning as a defense against fraud requires:

• Most Relevant Feature Creation
• Accurate Supervised ML Models
• Auto Training and Retraining
• Unsupervised Learning for Anomalies
• Explainability for ML Scoring
Online Travel Agency in South Africa

BUSINESS SCENARIO
- High chargebacks
- High manual reviews
- Long process and turn around time to implement changes to rules
- Friction for genuine customers

SOLUTION
- Complex decision orchestration considering booking timings and journey details
- Accurate Device Recon to incorporate device related risk
- Link Analysis to map the relationships between different entities

RESULT
- Automated 99.5% of bookings
- Stabilized chargeback rates to 0.08% per month
- Analysts can easily change rules and maintain watchlists
- Accurate and faster manual review and decision per case

(SCALABILITY)

(Fraud types experienced: Payment Fraud)
Results shown are specific to this travel agency. Other results may vary by industry, customer, and use case.
Conclusion

As the travel industry and allied services continue to grow, the complexity of doing business and retaining happy customers grows as well. Travel businesses must effectively manage and harness huge amounts of diverse and disconnected data as well as protect business interests from rising fraud.

Travel businesses need a solution that can consolidate big data and derive meaningful insights to proactively uncover patterns indicative of fraud and block threats before they affect the bottom line. Furthermore, newer technologies like clear-box machine learning with explainability and retraining can assist in detecting changing behaviors over time while automatically adapting to evolving fraud.

By successfully mitigating fraud, travel businesses can promote trust in their brand—making planning, booking, and traveling an amazing experience for their customers.
ABOUT SIMILITY

Simility, a PayPal service, offers real-time risk and fraud decisioning solutions to protect global digital businesses. Simility’s offerings are underpinned by the Adaptive Decisioning Platform built with a data-first approach to deliver continuous risk assurance. By combining artificial intelligence and big-data analytics, Simility helps businesses orchestrate complex decisions to reduce friction, improve trust, and solve complex fraud problems. Built by industry veterans, Simility is trusted by some of the world’s leading consumer brands across financial services, payment processors and commerce merchants. For more information on Simility, visit Simility.com