Comprehensive Fraud Prevention: Empowering Merchants to Offer Seamless Customer Experiences
Merchants require an advanced fraud solution to rapidly identify a customer across multiple channels, markets and payment types; and to determine whether transactions initiated by that customer are genuine, while presenting as little friction as possible.

Consumer demand for convenient and fast experiences has contributed to the rise of eCommerce. Meanwhile, with the continued growth in digital commerce, the potential reward for fraudsters is also growing. Massive data leaks, automated bots and phishing attacks have left merchants vulnerable. Moreover, innovations in mobile payments, omnichannel experiences, and cross-border commerce have become new avenues for online fraud.
Factors Contributing to the Growth of Ecommerce

1. **Increase in internet usage**
2. **Increase in smartphone users**
3. **Increase in availability of global products**

Retail e-commerce sales worldwide from 2014 to 2021 (in billion U.S. dollars)

Global Retail eCommerce sales will reach $4.5 trillion by 2021 making up 17.5 percent of total retail spending.

eCommerce is getting hypercompetitive, moreover consumers are in firm control of every aspect of a transaction. Merchants are aiming to enhance customer experience in order to satisfy high customer expectations.

Merchants continually strive to drive conversion. Striking a delicate balance between friction and convenience can improve conversion rates by reducing shopping cart abandonment and improving customer lifetime values.

As new business models and strategies emerge, such as the sharing economy, alternative payment methods and omnichannel experiences, businesses fight to keep their stake in the ground. Falling asleep at the wheel by failing to adapt to a constantly changing competitive landscape can be detrimental.

As global eCommerce transactions increase, so will the risk of fraud. Increasing cross-border commerce is forcing merchants to deal with regional government regulations to prevent online fraud and cybercrime.

Along with fraud liability, merchants bear the cost of goods, shipping and ordering charges, chargeback fees, and other administrative costs and penalties. Keeping these costs at a minimum can positively impact a business' bottom line.
Each dollar that merchants have lost to fraud in 2018 has cost them about $2.94 in overall losses, up from $2.77 a year ago.\(^2\)

- Increased chargeback
- Lost Revenue
- Lower customer lifetime value
- Diminished customer loyalty and trust
- Reputational damage
- Lower sales
- Lost merchandise
- Increased operational cost
- Brand erosion
- Increased manual reviews
- Increasing Costs of Ecommerce Fraud

Drivers of Ecommerce Fraud

EMV Shift
The adoption of EMV chip technology has shifted payment fraud from in-person to online.

Data Breaches
Widespread data breaches coupled with careless online consumer practices are exposing massive amounts of personally identifiable information, including payment and retail account details, bank card numbers, and more – giving fraudsters everything they need to launch complex attacks.

Omnichannel commerce
As consumers engage with merchants through online, in-store and mobile applications, cybercriminals have more channels to target, leaving merchants at an increased risk of fraud.

Cross border commerce
As consumers increasingly shop outside of their local markets, eCommerce merchants are seeing fraud go global as well.

Evolving payment options
New payment technologies like digital currencies, mobile wallets, and peer-to-peer payment methods serve as new pathways to facilitate fraud.
Most fraud for merchants stems from sophisticated CNP fraud, which involves automated, machine-driven attacks such as bots, device spoofing and location masking. In addition, any change in a merchant’s business strategy, introduces new opportunities for fraudsters to exploit.

Online merchants view fraud as inevitable

Merchants want to solve the growing fraud problem, however they also weigh those efforts against the impact on revenue generation and customer experience.

Key Complexities

• **Availability of automated fraud tools**
  Cybercriminals use automated tools to carry out high-speed attacks. These tools are available at low or no cost, or on a fraud-as-a-service basis.

• **With international commerce comes greater risk**
  Selling goods beyond local markets requires merchants to have both an understanding of how customer buying behavior differs and of various fraud profiles within each country.

• **Every business is now a target**
  Easy availability of cheap stolen card details on the thriving dark net markets have made all ecommerce businesses - ranging from high profile airline, electronics, designer goods to food delivery services - susceptible to fraud.

• **Ecommerce fraud peaks during busy shopping times**
  Fraudsters try to blend in among good shoppers during busy shopping seasons when merchants are at peak volume.

• **Poorly implemented security measures let fraudsters exploit vulnerabilities in mobile commerce**
  Unencrypted traffic and credentials, malicious apps on mobile result in a variety of fraudulent techniques and practices that are increasingly difficult to manage.
Identity Fraud
Data hacks, security breaches, and outright theft have made personally identifiable information (PII) for millions of customers potentially available to identity thieves. Compromised PII together with new EMV chip-enabled cards have led to the dramatic growth of fraudulent accounts. These accounts are then used for monetary gain, promo or referral abuse, money laundering schemes, to steal confidential information, and to spam good users.

Account takeover losses reached $5.1 billions in 2017.4

Login Fraud
Cybercriminals use stolen account information from mass data breaches, social engineering, advanced malware and phishing to gain control of legitimate users’ accounts. By taking remote control using automated bots, accounts are misused in several ways – making unauthorized purchases, stealing loyalty points, or accessing stored information.

Chargebacks
With increasing data breaches and the rise in sophisticated fraud, cybercriminals steal users’ debit or credit card numbers or other personal information to make unauthorized purchases. Chargebacks from these fraudulent transactions not only results in revenue and product loss, but also in high operational costs – impacting a merchant’s bottom line.

Fraud Varies Across the Customer Lifecycle - Major Fraud Concerns

Identity Fraud
As of 2017, identity theft amounted to $16.8 billion in losses.3

In 2017, the US merchants incurred nearly two-thirds ($19 billion) of a total chargeback loss of $31 billion.5

Account takeover losses reached $5.1 billions in 2017.4


In 2017, the US merchants incurred nearly two-thirds ($19 billion) of a total chargeback loss of $31 billion.
Too conservative legacy fraud prevention tools based on static rules can lead to the blocking of genuine transactions, resulting in revenue losses and defection to competitors.

**Legacy Fraud Solutions Can’t Keep Up**

Too conservative legacy fraud prevention tools based on static rules can lead to the blocking of genuine transactions, resulting in revenue losses and defection to competitors.

**Legacy Solutions:**

- Reject legitimate customers due to the inability to take any specific circumstances into account
- Are unable to uncover emerging fraud patterns
- Are dependent on manual reviews resulting in delays in order confirmation and fulfillment
- Add time-consuming authentication processes
- Are difficult to scale during peak periods, such as Black Friday and Holiday shopping, because of slow adaption to changing buying trends and needs

**MERCHANTS REJECT AROUND 3% of orders due to suspicion of fraud.**

---

**Machine Learning**
An Efficient Way to Identify and Prevent Fraud

**Data Ingestion**
A vast trove of varied data is processed and analyzed continuously to understand the subtle patterns that are beyond human comprehension.

**Training Algorithms**
Sophisticated algorithms are trained based on an organization’s historical data, and the algorithms evolve as new data emerges.

**Prediction**
Quick probabilistic scores are generated using predictions, resulting in increased fraud detection and reduced false positives.

- Machine learning is essential in the detection and prevention of eCommerce fraud at multiple levels spanning merchant category, channel and geography.
- Machine learning based fraud prevention can handle vast amounts of data to predict the likelihood of fraud with speed, accuracy and efficiency.
- Fraud solutions powered with machine learning detect anomalies, perform predictive modeling and find clusters to identify new and emerging fraudulent activities.
Merchants Need a Robust Machine Learning Based Fraud Prevention Solution to Reduce Fraud Without Sacrificing Customer Experience.
Simility’s Adaptive Decisioning Platform
An Innovative Approach

Simility is a comprehensive fraud prevention solution that detects, reports and mitigates omnichannel eCommerce fraud in real time.

Simility’s Adaptive Decisioning Platform works in conjunction with fraud-centric data lakes, dynamic rules and robust machine learning models to not only detect and block fraud, but also to recommend additional customized, industry-specific fraud filters to authenticate transactions or flag suspicious events, helping merchants:

• Increase revenue while reducing risk
• Reduce manual reviews and operational costs
• Improve customer experience and loyalty
As the threat landscape becomes more complex, merchants need an advanced solution to quickly and accurately predict fraud, while preserving the customer experience.

Dynamic rules augmented with explainable machine learning models help businesses link multiple data elements to fulfill orders faster, reduce friction for legitimate customers, and quickly identify high-risk transactions and logins.

**Declining** too many transactions with static rules can limit revenue.

**Striking a Balance**

**Accepting** transactions with blackbox ML alone might result in chargebacks and losses.
Simility’s Adaptive Decisioning Platform for merchants utilizes machine learning to dynamically learn and recognize anomalies or fraudulent behaviors across merchant profiles, geographies, and channels - quickly and at scale. Simility’s machine learning engine begins with experience from an array of business verticals, then quickly adapts to a merchant’s unique needs. It detects patterns of fraud before they are perceptible to human analysis or become a problem, keeping businesses ahead of fraudsters.

• With advanced machine learning capabilities, Simility discovers patterns in streaming or historical data to suggest new fraud detection rules.

• Machine learning suggests changes to existing rules for efficient performance. This makes the rules smarter and more incisive.

• Through big data predictive analytics, the fraud model evolves based on every rule and decision, continuously enhancing the detection of anomalous patterns.

Stay One Step Ahead with Superior Machine Learning
Simility's advanced device fingerprinting technology identifies unique devices—desktop or mobile—by their fingerprints and uses device risk scores and clustering to determine the fraud probability for any device, even one that has never been seen before.

- Analyzes hundreds of mobile and desktop device characteristics and behaviors including browsers, language, location, operating system, and even mobile emulation and battery level to fingerprint devices and determine if a device is associated with fraud.

- Uses proprietary machine-learning models to see through fraudsters’ techniques to determine whether two different device fingerprints belong to the same fraudster.

- Enables fraud teams to build specialized rules in the fraud model such as geolocation that compares device location to shipping location or billing location.
Simility’s adaptive rule builder comes with multiple data transforms precomputed, meaning anyone can quickly and easily add a rule based on category, region and channel to capture extremely complex logic and test it on their company’s own data.

- Easily adjust effective rules with a simple UI allowing for full governance testing and rule optimization to fit the overall strategy of a business while adapting to newer fraud trends as business evolves.
- Merchants can run champion/challenger rule sets to combat new fraud patterns by balancing multiple constraints in real time, while ultimately boosting results.

Detect Evolving Fraud with Powerful Rule Builder
Simility’s fraud solution enables merchants to provide customers with a smooth and quick checkout experience while providing protection from fraud, thus reducing customer abandonment.

- Stay in compliance with real-time, risk-based analysis of transactions based on device, location, historical, biometrics, transactional and cross-channel data.
- Easily and quickly ingest and analyze fraud related data feeds from third-parties for more accurate fraud insights.
- Seamlessly invoke an authentication layer for dynamically identified, high-risk transactions that are potentially fraudulent in nature.
Key Benefits of Simility’s Machine Learning Based Fraud Prevention Solution

**Attain Comprehensive Protection:** With the ability to collate and correlate data from various heterogeneous data sources, merchants obtain a comprehensive view behind an application, a login, or a payment to effectively tackle fraud.

**Balance Customer Experience and False Positives:** Enables merchants to balance chargebacks, customer experience, and false declines as per key business targets.

**Catch Evolving Fraud Faster:** Machine learning and dynamic rules enrich each other’s performance for proactively and accurately measuring evolving fraud.

**Address Compliance and Transparency:** Advanced analytical models enable merchants to explain why the system made a decision. Enables merchants to understand the logic so that decisions can be audited for compliance.
Simility Solution:

The high-end nature of luxury fashion retailer’s merchandise exposed it to sophisticated card-not-present attacks. While chargebacks from fraudulent transactions represented a significant loss, erroneous transaction denials also had a significant impact on revenue, as the denied transaction resulted in a lost customer and negative brand perception.

With fraud constantly evolving, the online retailer was looking for an adaptive solution to not only detect fraud, but also eliminate friction for legitimate customers and improve customer loyalty.

Simility’s Adaptive Decisioning Platform with self-optimizing machine learning models enabled the online retailer to identify complex fraud patterns and accurately distinguish between legitimate and fraudulent orders by dynamically analyzing data related to customers, devices, historical and behavioral information, card details, shipping and billing information, phone numbers and geo location.

Business Outcome:

With Simility, the online fashion retailer is able to identify anomalies in real time to differentiate fraudsters from legitimate shoppers, while significantly reducing false positives, manual reviews, and fraud, all without negatively impacting customer experience.
Conclusion

Global omnichannel commerce with multiple payment methods combined with constantly evolving fraud requires merchants to invest in intuitive, human-like reasoning when evaluating transactions. By leveraging a fraud prevention platform that is based on machine learning, merchants can effectively analyze large datasets to correlate customer and transactional data across various channels and devices in order to uncover patterns indicative of fraud.

Simility’s Adaptive Decisioning Platform with dynamic rule builder and advanced machine learning capabilities can help businesses accurately differentiate fraudsters from legitimate customers in real time, and quickly adapt to new fraud schemes. This helps merchants stay ahead of evolving fraud while offering legitimate customers a seamless experience across the entire customer journey, designed to lead to increased conversion, lower chargebacks, less manual reviews, and higher customer lifetime value.
About Simility

Simility, a PayPal service, offers real-time risk and fraud decisioning solutions to protect global 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