sift

E-commerce Fraud Prevention: The shortcomings of chargeback insurance

Online merchants are continually adapting operations and offerings to meet the changing needs of consumers while also minimizing risk to their businesses. But costly chargebacks can hinder growth and put fraud prevention teams on the defensive, constantly reacting to fraud after the damage is done. Insurance providers claim to solve merchants' fraud problems by using stringent filters to block potentially fraudulent actions while reimbursing merchants for the fees associated with any chargebacks they may encounter. But these providers only deliver a false sense of security, lack scalability, and force merchants to relinquish control of their fraud operations.

E-commerce companies need to establish proactive and scalable fraud prevention strategies that don't undermine growth for the sake of protection or give up control to an outside team that may not have the merchants' best interests in mind or understand their business. With a solution that accurately and effectively detects all types of abuse across a variety of channels, online businesses can enable their fraud teams to contribute directly to expansion without sacrificing protection—and give them the control they need to refine and scale fraud operations as the business matures.

With that in mind, merchants must consider whether an insurance-based fraud solution or a proactive machine learning solution will be more effective at helping them meet fraud prevention, chargeback reduction, and revenue goals.

Machine learning (ML) instantly calibrates risk assessments based on new data and evolving fraud trends. It's the only way for merchants to achieve the accuracy required to drive online growth while stopping fraud and chargebacks before they happen—all while reducing false positives and lowering operational costs.

The Business Impact of Machine Learning Solutions

The efficiencies and accuracy afforded by machine learning solutions directly drive growth, increase top line revenue, and reduce chargebacks by stopping fraud before it happens, lowering false positives, and eliminating the need for manual tuning as market conditions change.

Insurance providers, however, charge a premium on every insured transaction, whether it turns out to be fraudulent or not. This means the insurance provider will likely take a conservative approach, blocking more transactions than necessary to prevent any chargebacks and the accompanying payouts. The result is more friction for legitimate customers, more false positives, and ultimately lower conversion. Keeping fraud at bay is critical, but if a business focuses solely on chargeback reduction, it could be blocking or applying unnecessary friction to trustworthy interactions where its competitors aren't—ultimately losing out on growth opportunities.

To effectively balance positive user experiences, fraud prevention, and chargeback reduction, accurate risk assessment has to be a priority. Machine learning is highly accurate and an ideal tool for growing online businesses. When fraudsters adopt new tactics or customers change behaviors, ML models automatically ingest and analyze a multitude of incoming signals in real time. This shrinks the number of trustworthy interactions that are blocked or surfaced for review, blocks fraudulent interactions before they turn into chargebacks, and allows merchants to accept more orders while retaining control of their fraud operations.

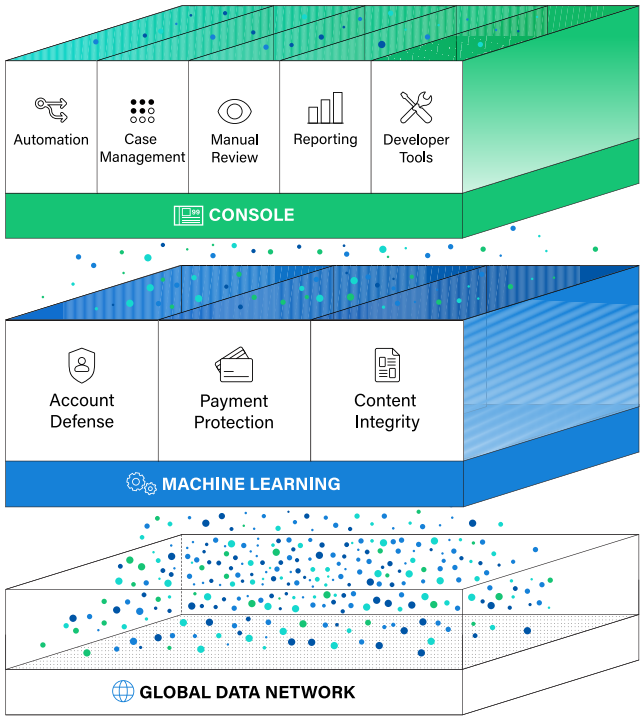
With an ever-growing source of data feeding ML models, they're able to function a lot like a human brain—smarter with more information, and more effective over time.

Business consideration	Insurance Providers	Machine learning solutions
Detection accuracy *How accurate is the solution?* *Can the business control how strategy is deployed?*	**Reactive, narrow approach focuses on fraud symptoms like chargebacks instead of the root cause** (risky interactions, rigid rules). **Limited control**—decisioning and liability for chargebacks shifts from the business to the insurance vendor.	Real-time risk assessment proactively identifies fraud. **Accuracy improves over time as the model ingests more data and refines itself.** Full ownership—merchants can create and **fine-tune policies based on criteria that are important to the business** and machine learning output.
Customer impact *Can the platform address chargebacks without sacrificing growth or customer experience?*	Trusted users can exhibit signals associated with fraud (high velocity or login from a new location) while risky users can fail to trigger rules based on known patterns. **This results in high false-positive and false-negative rates.** Conservative decision-making **increases friction for all customers.**	**Real-time risk assessment enables Dynamic Friction** and allows fraudulent interactions to be blocked before they become chargebacks. **Enables frictionless experiences** like one-click checkout for low-risk interactions, increasing customer LTV, and improving brand loyalty.
Scalability *Can the platform scale with the business as it grows?* *As the business expands, what impact will investing in this solution have on fraud operations and other areas of the company?*	Insurance premiums increase with volume. **Costs increase as the business grows.** **As the cost of insurance grows, scalability decreases** and may negatively impact the business' ability to address market or customer trends.	Adapts in real time, **effortlessly scaling alongside the business** to enable growth while preventing known and unknown fraud, and reducing chargebacks. **Becomes more accurate, efficient, and intelligent with every data point served.** For risk-averse businesses with high-value goods, **insurance can be used in conjunction with machine learning.**

How Sift Works: The mechanics of Digital Trust & Safety

Sift allows trust and safety teams to proactively prevent fraud, streamline operations, and grow revenue using an integrated solution that stops all types of fraud, including account takeover (ATO), payment fraud, and content abuse (spam and scams).

An intuitive Console puts analysts in control with powerful automation, case management, and real-time reporting, while an ensemble of machine learning models provides the highest accuracy in the industry: Sift customers have cut fraud by 80% or more and saved hundreds of hours previously spent on manual review. With learnings from the 60B events processed by Sift's global network every month, businesses can stay ahead of evolving trends and attack vectors—including those that have never shown up on a merchant's website in the past.



> When we started using Sift, Harry's chargeback rate decreased by about 85%, which is great because it helps us continue to be a company that people can trust shopping with.

HARRY'S

Kaity Reagle
Head of Trust and Safety, Harry's

Contact Sift today for a deeper dive into our technology, and to explore how your business can stop more fraud and catalyze growth with Digital Trust & Safety.

End-to-end intelligent automation with Sift

Sift is the leader in Digital Trust & Safety, empowering companies of every size to unlock new revenue without risk. Our cutting-edge platform dynamically prevents all types of online fraud and abuse with intelligent automation that adapts based on Sift's unrivaled global data network of 70 billion events per month. Global brands including Twitter, DoorDash, and Wayfair rely on Sift to catalyze growth and stop fraud before it starts.

Visit us at sift.com and follow us on LinkedIn.