Digital Trust & Safety for QSRs

Turning the tables on fraud

Contents

Tech Evolution, Food Revolution 3
Moving at the Speed of Trust 5
Fighting Fraud in Real Time 8
Looking Ahead: What's On the Menu for QSRs. 10
Sources. 11

Tech Evolution, Food Revolution

If the state of today's technology is hallmarked by anything, it's the human desire for convenience. Instant gratification and ease of use shape go-to-market strategies for nearly every brand around the globe, even driving major decisions for industry leaders that have no intention of losing market share.

Nowhere has this shift been more drastic than in the food industry, a world dominated by fast-casual dining and quick-service restaurants (QSRs). Companies that let you order ahead for scheduled pickup, or that enable food delivery to virtually anywhere, have perfected what pizza parlors figured out long ago: people want what they want, when they want it — and they're willing to pay for the privilege.

Still, no one should be fooled by dollar menus and marginal delivery fees. The quick-service food industry earns and spends billions of dollars every quarter, and boasts some of the healthiest global stock performances in history. In 2018, the world's most well-known coffee shop secured the #2 slot on the QSR 50, reeling in record-breaking consolidated net revenues of $6.3 billion in Q4 alone. They were beaten out of the top spot only by the makers of the classic Happy Meal, who reported an operational cash influx of $7 billion and free cash flow of $4.2 billion in 2018, a 14% increase from the previous year. These brands are growing rapidly, expanding exponentially, and meeting people wherever they are, whenever they're there.

> QSRs offering kiosk and mobile orders are seeing tickets worth 20%+ more than the average counter purchase.

But with all of that unbelievable growth and revenue comes risk, and lots of it. These QSRs are operating well beyond the scope of traditional cash-for-goods exchanges, with mobile apps and pre-order kiosks becoming the first stop for busy, hungry consumers. Research from BRP Consulting found that smartphones and other mobile devices play a key role in over one-third of dining experiences, and businesses that offer on-the-go ordering options are preferred by most consumers. Additionally, early stats from QSRs offering in-store kiosk and mobile-driven orders are seeing tickets worth upwards of 20% more than the average counter purchase, demonstrating that putting the consumer in control of where and when they order could have a serious impact on revenue going forward.

Tech's high impact on modern dining

Breakdown of how smart devices are used in the QSR market.

1. **Smartphones + mobile devices impact 1/3 of dining experiences**

2. **Mobile augments or enhances 38% of all dining experiences**

3. **20% of people pre-order food before they enter a restaurant**

4. **30% of people check restaurant ratings and reviews on mobile while in the restaurant**

Source: BRP & Windstream Enterprises, Restaurant Digital Crossroads: The Race to Meet Guest Expectations

These relatively young digital channels are a global playground for fraudsters. Their techniques for payment fraud and widespread account takeovers have become more sophisticated where legacy, rules-based fraud solutions have not. That's because these methods are reactive. They don't scale, limit growth, and consistently cause unnecessary friction for good users. According to a recent survey conducted by Sift, **60% of companies using traditional fraud prevention end up blocking legitimate customers.** Additionally, these rules aren't even keeping criminals from orchestrating attacks; **45% of respondents reported that rules do not effectively prevent fraud.**

The data doesn't lie, and that's bad news for QSRs that must exist with such thin margins for error, and in a crowded, on-demand market worth billions. This industry's value, the volume of transactions, and the extremely short window of time over which the full user journey takes place makes the quick-service restaurant market especially vulnerable, and an ideal target for criminals. Thanks to internet anonymity, fraudsters have seemingly endless ways of getting what they're after, and waste no time changing tactics when they meet resistance. As a result, there aren't enough rules in the world to help fraud analysts manually prevent these crimes or the damage they do to revenue, customer loyalty, and brand reputation — and that's where Digital Trust & Safety can make a valuable difference.

Legacy rules fall short

60%

of companies using rules for fraud prevention say rules **BLOCK** legitimate customers

60%

say rules **DO NOT** allow them to deliver a frictionless experience

45%

say rules **DO NOT** prevent fraud effectively

44%

say rules **ARE NOT** efficient for the team

Source: Sift Digital Trust & Safety Survey, 2019

Moving at the Speed of Trust

Digital Trust & Safety is an approach that aligns risk and revenue decisions by fundamentally changing the mindset, processes, and technologies associated with a business's fraud prevention strategy. Using machine learning to accurately separate suspicious behaviors from legitimate ones, this approach can enable QSRs to deliver great experiences to good customers and stop fraudsters in their tracks. Because it's automated, it's also scalable, making it an ideal approach for QSRs whose primary focus is protecting millions of customers as they interact with websites, mobile apps, and other digital channels around the clock and around the world.

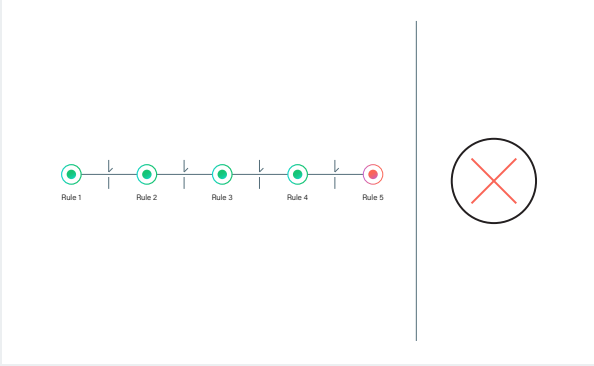
Before a Digital Trust & Safety methodology can be applied, though, it's important to understand how the underlying technology works. A lot of the time, machine learning (ML) is talked about in the context of artificial intelligence (AI), and technically, it is a subcategory of AI. But the critical difference between ML and AI is *purpose*. AI agents are designed to do what humans can do by thinking how they think, developing perspectives on the world around them, or making decisions about how to achieve a goal. Machine learning, on the other hand, enables computers to analyze information, understand the complex patterns within it, and then use those findings to accurately predict future outcomes. And, it's done at a scale and speed well beyond what humans are capable of doing on their own.

When it comes to fighting fraud in a digital landscape, though, legacy solutions use neither. Instead, they sit on a foundation of inflexible, reactive rules — all of which rely on massive teams of fraud analysts, constant tweaking, hours of manual review, and imperfect human intelligence in order to stay relevant and accurate.

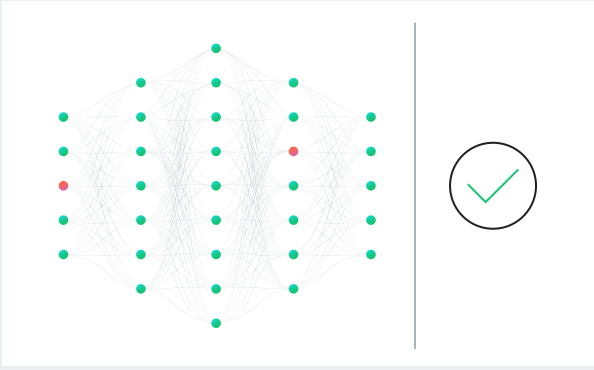
And while it's true that fraud analysts can logically, confidently identify certain risky attributes and actions — like temporary email addresses or spammy domains — it takes time.

Rules vs. machines: On the frontlines of fraud

While rules-based systems allow for some discrimination between legitimate and fraudulent interactions, solutions that use machine learning offer unmatched speed and accuracy.



Rules-based systems work like a series of gates, subjecting every user to the same scrutiny based on individual criteria. This makes rules easy for fraudsters to outmaneuver, while trusted users get caught in the net. As shown above, even if a trusted user passes most rules (green), it only takes one failed rule to block their journey on your site.



Machine learning (ML) assesses interactions using multiple signals, surfacing patterns that allow you to think holistically about risk levels while relying on the speed and accuracy of ML to deliver the right experiences at the right time. Above, green dots represent low-risk signals, while red dots represent higher risk signals.

It takes a lot of time, a lot of data review, and a lot of humans, especially as a company's user base gets larger. Putting the math in context, a single fraud analyst might need three minutes to manually assess the risk tied to just one transaction before blocking it or moving it through. If your business sees a thousand transactions per day that require manual review, a lone analyst would need about 50 hours to look through a single day's worth of activity; you'd need a team of seven people working nonstop to get it done in an average, 8-hour workday — something that could easily lead to mental fatigue and inconsistent decisioning. Even then, customers won't wait around for hours and hours before you accept their money; they're going to get what they want somewhere else.

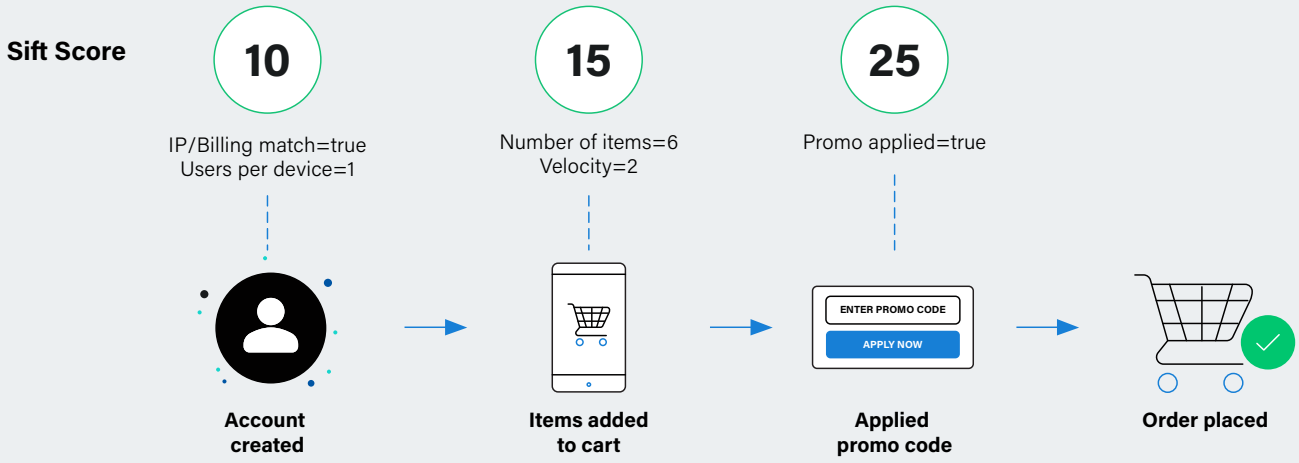
Rules-based solutions were built with the idea that there would always be room (and time) for manual review, but it's not even an option for QSRs. With an average fulfillment window of just 10-15 minutes, the only possible choice is to accept or reject a transaction — drastically upping the chances of letting through fraudsters and blocking legitimate users.

No brand wants to conduct business so inefficiently, which is why rules-based fraud platforms emerged in the first place. Giving an expert ways to define set thresholds for what likely constitutes good and bad behavior, and use technology to monitor activity, turns that mountain of manual work into a more manageable molehill. It enables businesses to react more quickly to fraud attacks, account takeovers, and chargebacks. But what it doesn't do is help companies predict and prevent fraud — let alone with the pinpoint accuracy and scalability required for the quick-service industry.

Enter machine learning, and its unmatched ability to process massive amounts of data, categorize behaviors, unearth patterns, and make connections that humans can't. Sift does this by assessing multiple signals throughout the user's journey, connecting them to signals from thousands of merchants in the global data network, and developing a composite score on a scale from 1-100. On this scale, a score of 1 suggests a high level of trustworthiness for a customer interaction (e.g., creating an account or placing an order), and 100 indicates a high likelihood of fraud; middle-of-the-road scores are surfaced for manual review.

How Sift's machine learning works

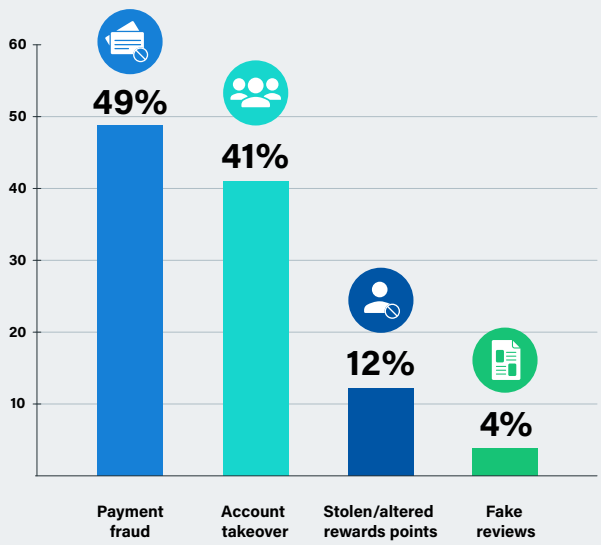
Sift's machine learning models surface new risks, patterns, and changes in fraudulent behaviors in real time by assessing multiple signals throughout the user journey and global data network, developing a composite score on a scale from 1-100. On this scale, a score of 1 suggests a high level of trustworthiness for a customer interaction, and 100 indicates a high likelihood of fraud; middle-of-the-road scores are surfaced for manual review. This score becomes exponentially more accurate over time.



Having the ability to better understand fraud types and patterns is particularly important for QSRs, since fraudsters rarely limit themselves to a single type of fraud. They're industry agnostic and, if unable to complete their first fraud attempt, will often move on to a different type, a new vendor, or another marketplace altogether. That's why being part of a global data network that gets smarter every second gives QSRs significantly more protection against attacks — including a major head start on identifying fraudsters and predicting risk.

Consumers' top QSR fraud concerns

Sift commissioned a series of Dynata surveys in September and October 2019. The poll included 1,000 US consumers each, ages 18 and above, and aimed to understand their top QSR fraud concerns.



Digital Trust & Safety enables QSRs to meet and exceed their customers' expectations for speed and convenience by moving known customers from intent to purchase in seconds. Because trusted users are ushered safely through the buying process without unnecessary friction, they're less likely to abandon their carts or seek out alternative vendors in the future. Meanwhile, suspicious behaviors or interactions are identified, scored, and when necessary, stopped — allowing merchants to save any tedious manual verification for situations that truly call for it. In some cases, this can free up as many as 30 hours per week for fraud teams.

> Merchants using Digital Trust & Safety never have to choose between what's best for the company and what's best for the customer.

Because QSRs can't bother with manual review in the first place, the accuracy of these lightning-fast decisions is critical to reducing false positives during what is a nearly instantaneous decision-making process. The ability to rapidly process tons of data at scale means that QSRs can stay well ahead of threats to users and proprietary information, instead of being forced to eat the cost of fraud. It helps them maintain healthy growth and happy customers, and drastically reduces friction every time users interact with the brand. In a nutshell, merchants using Digital Trust & Safety never have to choose between what's best for the company and what's best for the customer ever again.

Fighting Fraud in Real Time

When someone decides they want coffee, there's no shortage of options. From robot-run kiosks to global franchises that have mastered the art of customization, customers getting what they want isn't the issue — they're focused on how quickly and easily they can get it.

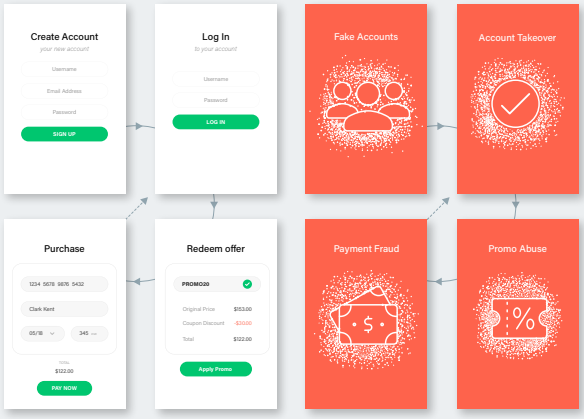
For some, that means finding the brick-and-mortar cafe with the shortest line. But for a growing number of customers, it's all about using a mobile app to browse, pre-order, and pay. Interacting with an app has to be simple. If it's not, that potential buyer won't hesitate to find a different app, and within seconds, your business has lost a customer. In a market this crowded, QSRs quite literally can't afford for users to defect to other vendors without major repercussions. Take the recent stock drop that's hit one of the industry's former leaders, a direct result of fierce competition and too many players. It's tough to accept, but people aren't necessarily loyal to brands — they'll often go where they can find deals and opportunities for convenience. This, coupled with a universally low tolerance for friction, has led many QSRs to adopt one-touch payments and the promise of instant service to keep people on the path to purchase. And while that's great for customer satisfaction, it's also full of opportunities for fraudsters.

Criminal or customer: The game where everyone loses

Here's the major problem QSRs are facing: the more optimization you add to the buyer's journey, the higher the risk of illicit activity. Removing authentication steps speeds things along for everyone, and fraudsters are going to take advantage of that.

The spectrum of online fraud risk

For every revenue-generating call to action on a website, there is a corresponding way for fraudsters to exploit that opportunity.



CALL TO ACTION	FRAUD VECTOR
Create account	Fake accounts
Log in	Account takeover
Buy now	Payment fraud
Create listing/ posting	Scams
Redeem offer/ promotion	Promo abuse
Refer a friend	Fake accounts

But with legacy solutions that depend on static rules and lots of manual review, identifying fraud can be slow, inflexible, and inaccurate, and cause unnecessary friction for legitimate customers. Simply put, rules-based fraud solutions don't work because fraudsters don't play by the rules. Their attacks happen faster than any manual review possibly can, and at least 45% of them will simply move to the next type of abuse on their list if they're prevented from finishing the first. When every transaction is a gamble that could result in lost revenue, shrinking market share, and angry patrons, reactive fraud mitigation starts to quickly lose its appeal.

This is the key reason being part of a global network of data that updates in real time, with information from diverse industries and verticals, is so beneficial, no matter your business. Digital criminals don't always zero in on a business because of what it is, or what it does. They choose it because of what it's missing and where it's vulnerable.

> Rules-based fraud solutions don't work because fraudsters don't play by the rules.

For QSRs, this susceptibility can show up in an unexpected way — like when fraudsters use them as testing grounds for stolen payment methods, gift cards, credentials, or other data. They're not really after free takeout and groceries; they want to make sure their tactics work before they attempt to use them somewhere else for a bigger payoff. But that's not to say that QSRs are in any way immune to more intentional forms of attack; food and beverage fraud continues to rise in tandem with consumer demands for speed and convenience.

Food for thought: Dynamic Friction

It's for this reason that leading businesses, including QSRs and food delivery services like Favor Delivery, Rappi, and DoorDash, are adopting a Digital Trust & Safety mindset that enables Dynamic Friction. This preventative, real-time approach enables businesses to apply friction (e.g., multi-factor authentication) when it's needed, and remove it when it's not. Using Sift's powerful machine learning, they can provide tailored account creation, login, and purchasing experiences for each user based on an unbiased and comprehensive assessment of their risk level. It's a more sophisticated, accurate way to identify and prevent fraud without sacrificing what's good for business, letting trusted users bypass multiple layers of verification, while unknown or potentially risky interactions get additional screening.

Looking Ahead: What's On the Menu for QSRs

Consumers' expectations for QSR experiences that are simple, speedy, secure, and tailored to them will only continue to shape the food industry at large, deeply influencing how brands do business and defining how technologies emerge and evolve. Experts predict that these innovations will be the primary factor in how trends unfold on all fronts of the market, from how food is produced and delivered to how fraud is mitigated and prevented.

For QSRs unwilling to be undermined by digital outlaws, an integrated solution is critical to streamline operations, secure customer interactions, and grow revenue while proactively preventing fraud. Sift puts Trust and Safety teams in control with powerful automation, case management, and real-time reporting. Our machine learning models deliver the most accurate results in the industry. Finally, our global data network processes upwards of 35 billion events every month, so QSRs can stay ahead of evolving threats and attack vectors — even those they've never seen before.

It's time to stop the criminal-or-customer guessing game. Protect your customers, defend your revenue, grow your business, and do it at scale with Sift. To learn more, visit sift.com.

Sources

1. *QSR Magazine, "The QSR 50."*
https://www.qsrmagazine.com/reports/2018-qsr-50
2. *Starbucks, "Starbucks Reports Q4 and Full Year Fiscal 2018 Results."*
https://stories.starbucks.com/press/2018/starbucks-q4-fy18-earnings/
3. *McDonald's, "McDonald's Reports Fourth Quarter And Full Year 2018 Results And Quarterly Cash Dividend."*
https://news.mcdonalds.com/news-releases/news-release-details/mcdonalds-reports-fourth-quarter-and-full-year-2018-results-and
4. *BRP & Windstream Enterprises, "Restaurant Digital Crossroads: The Race to Meet Guest Expectations."*
https://www.windstreamenterprise.com/wp-content/uploads/2018/06/race-meet-guest-expectations.pdf
5. *PYMNTS, "QSRs Ramp Up Mobile Order-Ahead Offerings."*
https://www.pymnts.com/news/retail/2018/qsr-mobile-order-ahead-data/
6. *The Sift Digital Trust & Safety Survey was carried out by Berg Research, in independent research firm. It surveyed 500 professionals at companies of 500+ employees across North America with responsibilities related to fraud, risk, mobile or e-commerce operations, and strategy. From Sift's "Leading the Digital Trust & Safety Transformation."*
https://pages.sift.com/rs/526-PCC-974/images/ebook-leading-transformation-digital-trust-and-safety.pdf
7. *Sift, "How Rently stays one step ahead of ATO and scams."*
https://resources.sift.com/case-studies/rently-case-study/
8. *Chicago Tribune, "Grubhub stock closes down more than 40% as Chicago-based company warns of fierce competition for 'promiscuous' online diners."*
https://www.chicagotribune.com/business/ct-biz-grubhub-stock-falls-20191029-xe7q6dro7ragxfpyfptmkzkwh4-story.html
9. *Campaign Monitor, "What Science Says About Discounts, Promotions, And Free Offers."*
https://www.campaignmonitor.com/blog/ecommerce/2019/10/what-science-says-about-discounts-promotions-and-free-offers/
10. *Sift, "Dynamic Friction: Delivering the Right Experiences at the Right Time."*
https://resources.sift.com/ebook/dynamic-friction-delivering-the-right-experiences-at-the-right-time/
11. *PYMNTS, "Fighting the Friendly Fraud Fight."*
https://www.pymnts.com/news/security-and-risk/2017/fraudulent-transactions-ethoca/
12. *Sift commissioned a series of Dynata surveys in September and October 2019 polling 1,000 consumers each in the US ages 18 and above. From Restaurant Technology News, "Research: 62% Of Consumers Worry Their Online Interactions With Quick-Service Restaurants Are At Risk of Fraud."*
https://restauranttechnologynews.com/2019/10/research-62-of-consumers-worry-their-online-interactions-with-quick-service-restaurants-are-at-risk-of-fraud/
13. *Javelin Strategy, "2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt."*
javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt