sift

Dynamic Friction

Delivering the right experiences at the right time

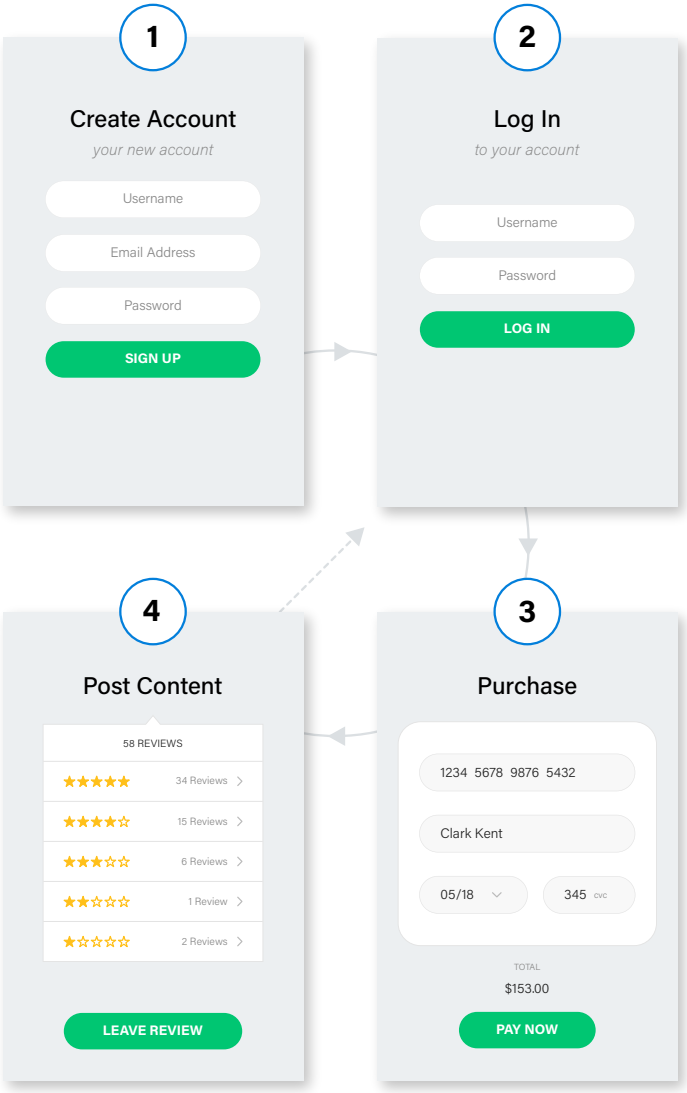
Contents

Dynamic Friction: Delivering the right experiences at the right time

The expectations of online consumers have drastically changed in recent years. Not so long ago, shipping times hovered in the 2-4 week range. Now, even 2-4 days seems like an eternity to wait. Consumers want the least amount of friction in their online experiences — from account creation to checkout and beyond. And with thousands of companies vying for their business, users have the upper hand. Price alone will not delight and retain valuable users; speed and convenience are what sets apart market leaders from their lagging competitors. Successful businesses are prioritizing customer experience above all else.

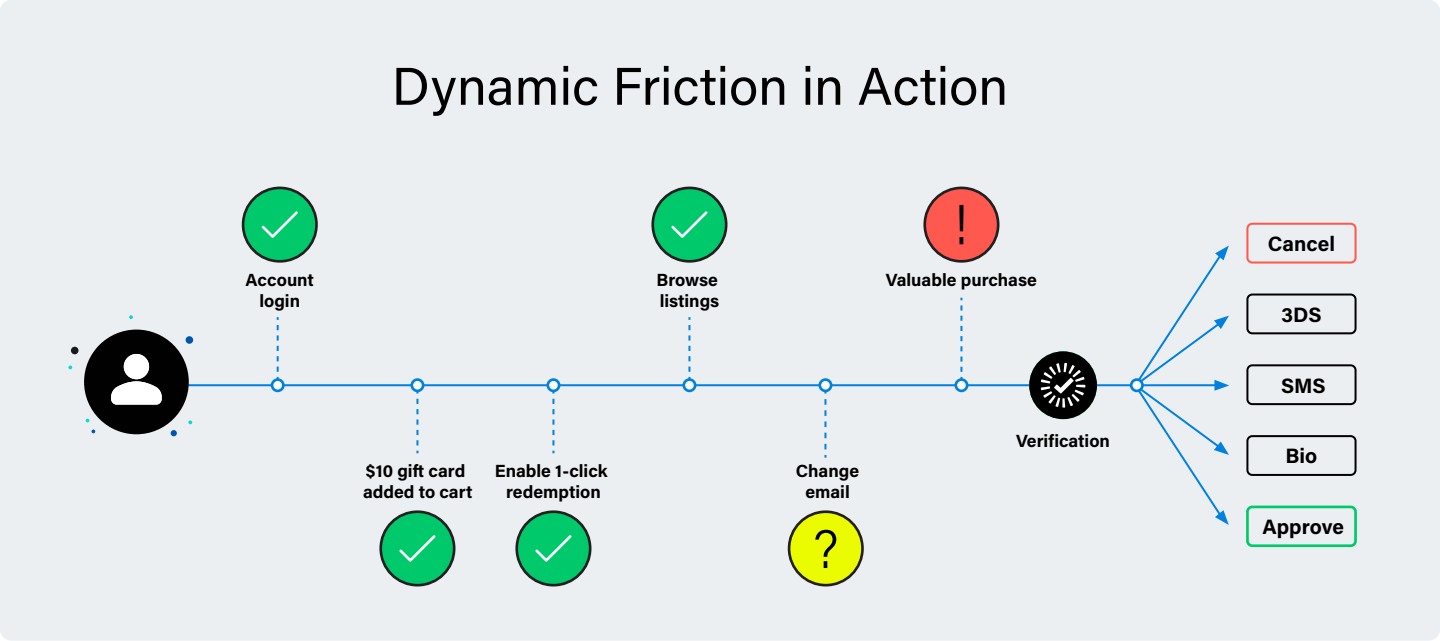
But this prioritization can't be reckless; some amount of friction is required to stop fraud. Additional layers of authentication — multi-factor authentication (MFA), card verification values (CVV), etc. — are needed to challenge fraudsters and weed out suspicious activities. But indiscriminate authentication comes at a cost. Friction lowers conversion rates and increases the chances of insulting your trusted customers, driving them to switch to your competition.

So how do you deliver delightful experiences to your trusted users, block the bad actors, and thoughtfully apply friction to those users that may need an additional level of authentication?



Set roadblocks for fraudsters, and remove barriers for good users — with Dynamic Friction

Authentication of potentially risky users doesn't need to turn an online experience into an invasive airport screening. Trusted users can bypass additional authentication, while unknown or potentially risky users get additional screening. This philosophy is at the core of a new approach called Dynamic Friction: the optimal application of friction to user journeys based on behavioral and situational attributes, so your protection against fraud doesn't result in customer insult for legitimate users. Dynamic Friction is powered by Digital Trust & Safety, which strategically aligns risk and revenue decisions, and is supported by processes and technology.



The above image illustrates a user journey, from account login to checkout. As a user moves through the journey, each interaction is evaluated for risk. If the level of potential risk hits a certain threshold, additional authentication is applied. If the interactions are deemed trustworthy, the additional authentication is removed, giving the user a more streamlined experience.

This method of dynamically applying friction to the user journey stands apart from legacy solutions, which apply friction in the same way to all users, even at the risk of alienating good users and causing false positives. Additionally, legacy solutions only look at one specific event in a user journey, while Dynamic Friction considers the user journey holistically, from end to end. Obsolete solutions are killing growth — and potentially damaging users' trust in businesses.

Use case: Dynamic Friction and account takeover

While Dynamic Friction can be applied to every point in a user's journey, let's look at it through the lens of account takeover (ATO). Account takeover is a rapidly growing, industry-agnostic problem that shows no sign of slowing down. The issue has become so ubiquitous that it's likely either your business or one that you're familiar with has been the victim of a successful or attempted ATO attack. According to the Sift 2017 Fraud-Fighting Trends Report, 48% of online businesses experienced an increase in ATO in 2016. For businesses, the need to protect against this threat has never been stronger.

One effective way to combat ATO is to apply additional authentication to login events by introducing MFA, biometric authentication, and other authentication methods. But many businesses shy away from these methods because they introduce friction, which creates pain points for users. The thought of introducing speed bumps into the user experience seems counterproductive and the fastest way to send a customer right to the competition. While there is some truth to that belief, it mainly applies to the indiscriminate application of friction — which Dynamic Friction eliminates.

Historically, businesses have relied on a one-size-fits-all approach that doesn't differentiate between known, trusted users and fraudsters, delivering identical experiences to both groups. From CAPTCHAs to other clunky security features, these methods deliver poor customer experiences, while fraud teams find themselves playing a never-ending game of catch-up to accomodate for fraudsters' ever-evolving tactics and strategies.

For businesses to remain competitive, they must embrace the smarter, more streamlined approach to combating ATO: introducing MFA, and applying it discriminately via Dynamic Friction.

Account takeover (ATO) at a glance

48%

of online businesses observed a rise in ATO in 2016

$2.3b

in consumer losses from ATO in 2016

61%

increase from 2015

Source: Sift 2017 Fraud-Fighting Trends Report

MFA and Dynamic Friction: a smarter, more efficient approach to authentication

No matter the vertical your business is in, MFA is one of the strongest methods for securing user accounts, because fraudsters don't often have access to the additional factor required to authenticate.

MFA requirements

Users must have two of following three credentials to access their account

Something you know
(i.e. passwords, PINs)

Something you have
(i.e. security fob, phone, ATM card)

Something you are
(i.e. biometrics like fingerprints and voice/facial recognition)

Microsoft and Google are strong proponents of MFA: according to Microsoft, users that enable MFA for their accounts will block 99.9% of ATO attempts, while Google found that device-based challenges have high rates of success in blocking attacks. On-device prompts — a more secure alternative to SMS verification — block 100% of automated bots, 99% of bulk phishing attacks, and 90% of targeted attacks.

Users can no longer rely on passwords as their sole form of security against unauthorized account access. Credential stuffing and phishing, two of the most common fraud strategies that facilitate ATO, make passwords useless once they're in the hands of fraudsters. It doesn't help that both strategies prey on users practicing poor password hygiene: 62% of people admit to reusing passwords across sites (inadvertently bolstering the effectiveness of credential stuffing), while phishing attacks exploit a person's curiosity or fear, depending on the content of the attack.

The data is clear: MFA is significantly more effective at securing accounts and stopping ATO attempts than passwords alone. So why aren't more businesses adopting this method of fraud prevention?

The fear of friction.

Smart businesses worry about creating negative customer experiences in an environment where customer expectations for convenience are increasing, from one-click checkout, to instant delivery, to on-demand services. Churn and reduced engagement are often big concerns — will my customers go to a competitor if they feel inconvenienced? Do they feel as though they're being treated as fraudsters rather than trusted, legitimate users — guilty until proven innocent?

With Dynamic Friction, inconvenience and customer insult are no longer the foregone conclusions of introducing MFA. When you apply friction in a smart and strategic way, good users aren't caught in the net of the indiscriminate application of roadblocks and authentication. Introducing Dynamic Friction into your fraud prevention process is one step on your journey towards a full Digital Trust & Safety transformation — because Dynamic Friction is an application of the Digital Trust & Safety methodology.

Ending customer insult with Digital Trust & Safety

Adopting a Digital Trust & Safety mindset will enable your business to focus not just on fraud prevention, but on creating the user experiences that build brand loyalty and customer trust. Digital Trust & Safety is an alignment of risk and revenue decisions — protecting against fraud and growing your business. This alignment isn't achieved simply with the addition of a new tool or product, but by fundamentally changing the mindset, processes, and technologies associated with a business's fraud prevention strategy.

Executive leadership embraces a customer-centric mindset
Company priorities aren't centered solely around protecting the bottom line, but on delivering outstanding user experiences while mitigating risk.

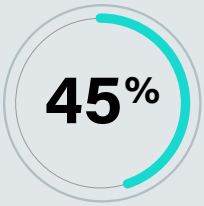
Organizational processes and structure support a growth mindset
Cross-functional Trust & Safety teams are formed and have aligned goals that take into consideration risk and revenue. Products are built with growth and protection in mind. Customer data is leveraged across all teams to make decisions that balance growth initiatives with risk policies.

Machine learning powers fraud prevention technologies that adapt to the user journey
Machine learning fraud prevention leverages customer data to assess risk in real time and route users to the appropriate experience based on that risk.

Dynamic Friction is an application of the mindset, processes, and technologies at the center of Digital Trust & Safety. The key to creating positive customer experiences (growth) and maximizing fraud prevention (protection) — the core goals of Digital Trust & Safety — is to introduce Dynamic Friction into the user journey with Sift.

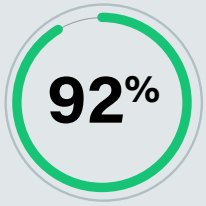
Connecting the Dots

Sift ingests 35 billion events per month to uncover millions of fraudulent events. We looked at cross-sections by abuse type and vertical over three months to uncover patterns of fraud.



of fraudsters commit more than one type of fraud

of fraudsters engage in ATO plus other types of fraud, and 1/3 of ATO fraudsters have also dabbled in payment fraud



of fraudsters who first commit ATO move on to other types of fraud including payment fraud, content abuse, and promo abuse

Sift — the only true holistic Digital Trust & Safety solution

Sift is the only true Digital Trust & Safety solution that enables Dynamic Friction — and is the ideal approach to providing customized user experiences in real time while protecting your business against fraud. With Sift, your business benefits from the alignment of risk mitigation and positive customer experiences, in addition to the optimal application of friction that considers all steps in the user journey. And you get it all in one solution.

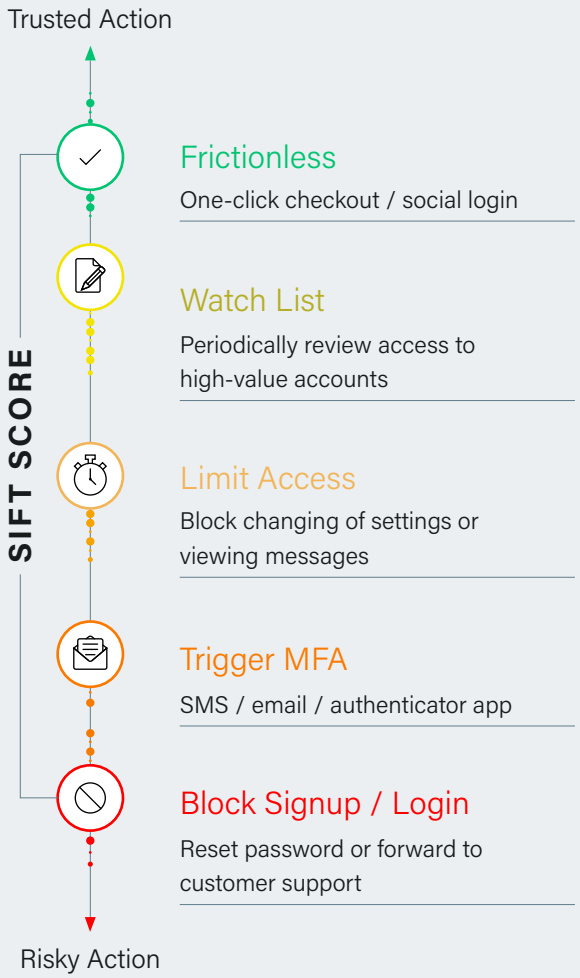
Sift has made it easy to leverage Dynamic Friction with the release of Authentication, a feature that allows businesses to introduce MFA not as a blanket, mandatory authentication process every user experiences in the same way, but as the thoughtful application of friction based on user actions and behavioral attributes.

Sift's real-time machine learning reviews thousands of signals to identify risky behavior across the user journey, enabling businesses to determine what level of authentication is the most secure for a given user. By determining the riskiness of actions via a Sift Score, businesses can provide seamless experiences with no friction for trusted customers. With unparalleled accuracy, this real-time risk assessment determines what level of authentication a given user needs: riskier actions with more red flags trigger MFA, while good actions ensure a frictionless experience. Trusted customers enjoy a painless login, while potential fraudsters are met with challenges, like MFA or limited access to account features. In the riskiest cases, login will be blocked entirely.

As customer expectations rise, so too does the need to stop treating your best users like fraudsters — making it more critical than ever to leverage Digital Trust & Safety and the rich data of Sift's global network to protect your business and its users from multiple types of fraud while providing the best possible experience to your trusted user base.

Identify trusted and risky actions in real time

With Dynamic Friction, you can create customized experiences based on risk



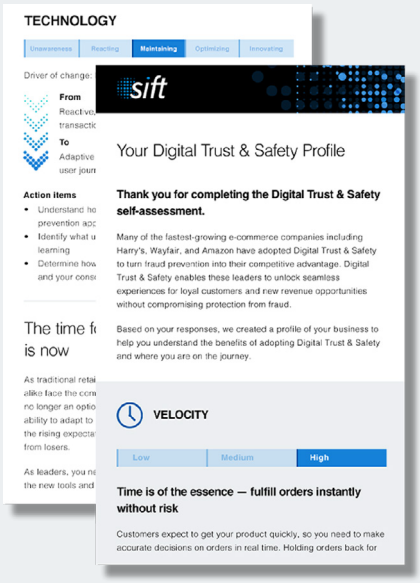
It's time to stop treating customers like criminals

The time to implement Dynamic Friction into your fraud prevention strategy is now. Users are expecting convenience and a lack of friction not as luxuries, but as the new standard for online experiences. In order to stay competitive, you have to start by no longer treating users as guilty until proven innocent. Learn how your business can deliver on customer expectations while remaining secure with a Digital Trust & Safety Assessment. Our Trust & Safety Architects will provide you with custom recommendations to effectively align your business around the Digital Trust & Safety approach, enabling you to achieve growth while stopping fraudsters in their tracks — before they make it onto your platform.

Your Digital Trust & Safety Assessment

By answering a few simple questions about your business, Sift will create a profile to help you understand where you are on the journey to adopting Digital Trust & Safety, and becoming a leader in your market.

GET STARTED



 | © 2022 Sift Science, Inc. All rights reserved. Sift and the Sift logo are trademarks or registered trademarks of Sift Science, Inc.