sift science

Maximizing Mobile Opportunities

Contents

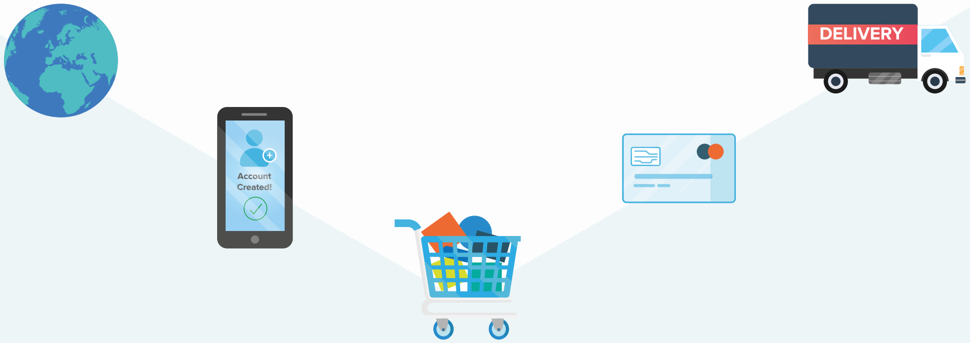
Introduction

Mobile is eating the world

Do you remember a time without smartphones? When up-to-the-moment traffic or breaking news or an update from a friend wasn't just a tap away? If you're like 98% of U.S. Millennials, you own a mobile device, and it's becoming more and more indispensable to how you navigate, communicate, present yourself, and shop.

It follows that if you're a business that wants to grow sales across a rapidly expanding channel, move into new mobile-dominated markets, or own the attention of a coveted audience of younger consumers, a comprehensive mobile strategy is non-negotiable.

Savvy online businesses have already adapted their digital strategy to support the move to mobile. The mobile opportunity is here! Now, it's just up to businesses to fully embrace it. Those who don't will simply be left behind. That's the reality of the mobile shift: adapt or die.



Mobile usage by the numbers

75% of Americans will use a mobile device in 2017 (eMarketer)

1 out of 2 Millennials has downloaded a mobile shopping app (Stanford/Pixlee)

In 2016, mobile and tablet internet usage exceeded desktop for the first time worldwide (StatCounter)

The most used operating system globally is Android (65%), followed by iOS (31%), and Windows Phone (1.9%) (NetMarketShare)

Customers worldwide are buying more on mobile

Mobile commerce is driving nearly 22% of all e-commerce revenue and is projected to reach $600B by 2020 (Gartner)

More than half of Chinese e-commerce purchases happen on mobile – and this will grow to 71% by 2019 (eMarketer)

63% of smartphone shoppers make an online purchase at least twice a month (Internet Retailer)

During the 2016 holiday season, 72% of Amazon customers shopped on a mobile device (Amazon)

Mobile opportunity #1: Over-deliver on omnichannel

It's becoming rarer and rarer for shoppers to leverage a single channel only to interact with an online brand. Instead, consumers hop from physical stores to mobile browsers, from emails to social media, from call centers to apps.

However, the onus falls on brands to ensure the transition from point to point is as smooth as possible.

Omnichannel is omnipresent

31 % of all online transactions involve two or more devices

25 % of all cross-device transactions completed on desktop began on a smartphone

35 % of those completed on a smartphone started on a desktop

Source: Criteo

Omnichannel pays off

A February 2017 Harvard Business Review study found that omnichannel shoppers spent 4% more in store and 10% more online than single-channel shoppers.

As a key player in so many customers' journeys, the mobile channel offers many opportunities to delight and increase sales. You can target promotions to a user's preferences, serve up personalized content, and maximize your brand awareness at key moments.

But if fraud prevention isn't a key consideration of your omnichannel strategy, these opportunities can't be realized. If you can't connect the dots across all the various user touchpoints, you risk (for example) flagging legitimate customers as false positives, or letting fraudulent transactions through.

If you apply the right approach, however, the data you collect across the entire customer experience can also enhance your fraud prevention efforts, which in turn provides the seamless experience shoppers crave.

The more data, the better!

Mobile-specific data you can leverage to fight fraud

Are they using a mobile browser or an app?

How many apps a phone has installed. The average smartphone owner has 26 apps installed (source: Google's Our Mobile Planet), but a fraudster may have many fewer.

Which version of your app is being used? Fraudsters might prefer an older version to exploit a weakness that has since been fixed in a newer version of the app.

Is the phone jailbroken or rooted?

Mobile carrier data + connection speed and type (2G, 3G, etc.)

Extra device ID info: Operating system + type of phone (e.g. Samsung S5) + even serial number of the phone

What type of phone is it? Fraudsters tend to use older and more basic phones, because they're less expensive.

Biometric and behavioral mobile data

Not all of these are widely used to predict fraud – yet. But it's just a matter of time.

- Finger touch pressure
- Tilt of the device
- Swiping vs. typing (humans like to swipe, while bots will type)
- Keystrokes (a bot will type very systematically, at the same cadence)
- Number of pixels firing on the screen

With the right fraud prevention tool, you can know which users to trust, which to block, and which to ask for extra verification – right from the moment they interact with your site or app.

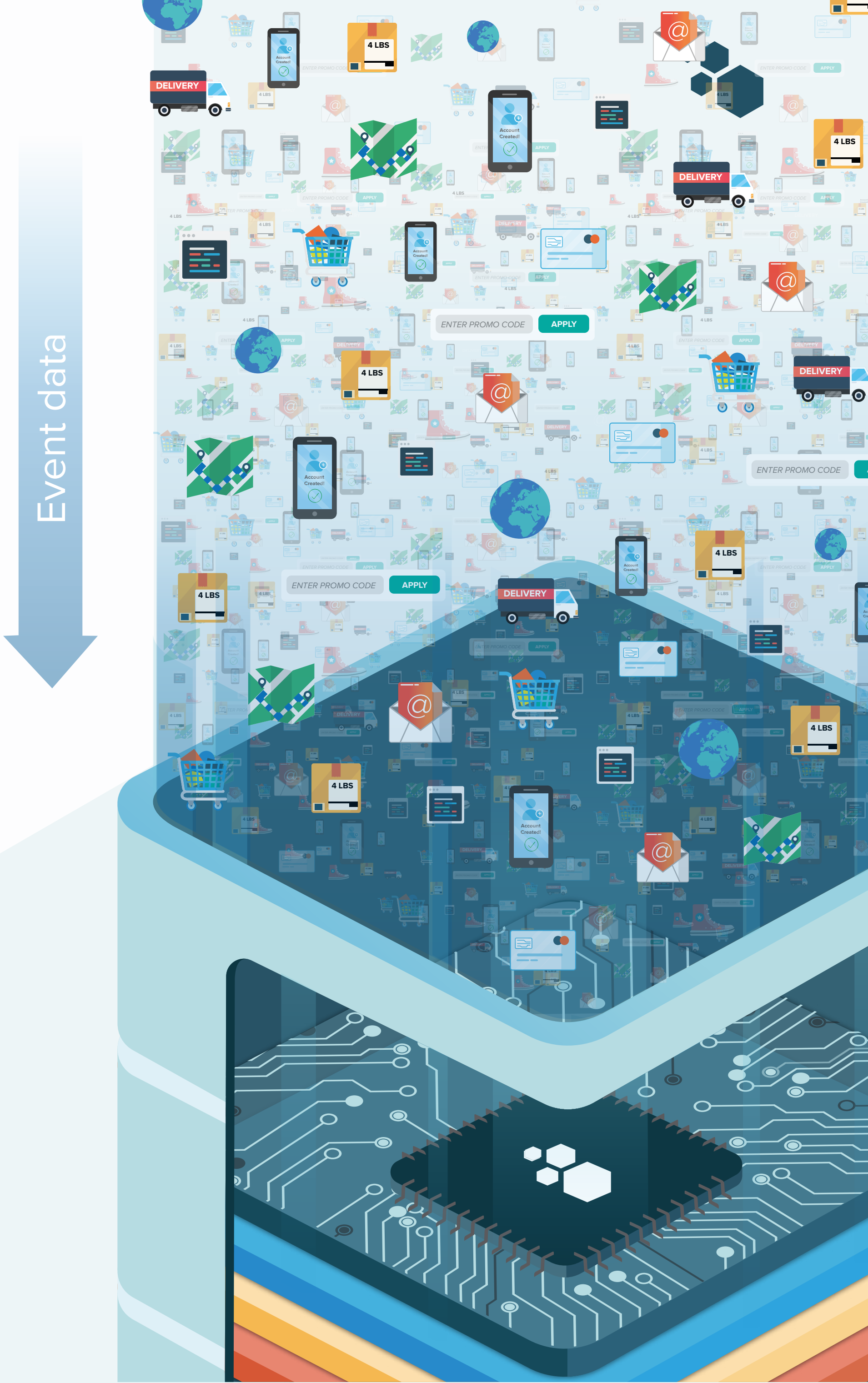
How Sift Science can help

Sift Science ingests multiple types of data in one machine learning platform

Sift Science's machine learning technology is ideal for ingesting multiple types of data, from multiple sources. Passive tracking of mobile-specific data can help you prevent fraud, and it doesn't get in the way of your users' behavior.

Make sure you're leveraging data collected across all stages of the customer journey, irrespective of device. A user may download your app, but have a history of browsing your site and interacting with your brand. Or they may have previous interactions on other websites or apps that can be used to generate a profile of the user, even if they are unfamiliar to your company. Creating traditional rules to mitigate against fraud is highly difficult here, since user behavior is so varied.

Sift Science uses multiple machine learning models – including a model based on our vast customer network of 6,000+ sites and apps – that help us recognize users immediately and provide them with highly accurate risk scores... even if they've never visited your site or app before.



Mobile opportunity #2: Simplify checkout

The company that simplifies the checkout experience will enjoy the spoils of increased sales and happier customers. According to usability studies run by the Baymard Institute, e-commerce sites could increase conversion by as much as 35% by simply offering a better checkout design.

Nowhere is simple checkout more crucial than on mobile. Mobile shopping cart abandonment rates have traditionally been higher on mobile than desktop, and several retailers have been critiqued for not investing in a strategy that streamlines mobile checkout, specifically on mobile browsers.

Shoppers like it simple

27% of shoppers have abandoned a shopping cart due to a too long/complicated checkout process (Baymard Institute)

54% of Millennials said they downloaded a mobile shopping app because the user experience was better than mobile browsing (Stanford/Pixlee)

56% of mobile shoppers say the majority of their online retail purchases in the last year were made on Amazon.com – a site known for simple, streamlined checkout. (Internet Retailer)

Improvements to the purchase experience could range from removing unnecessary form fields to offering the holy grail of checkout: one-click and one-tap ordering, where payment happens largely in the background.

But delivering these simple, streamlined experiences requires a careful balance of security and convenience. Friction and extra hoops are conversion killers. However, by removing friction from your purchase flow, you risk opening yourself up to costly fraud. The key is to find the ideal balance between these two extremes, and to only introduce friction in cases where a transaction is likely to be risky.

How Sift Science can help

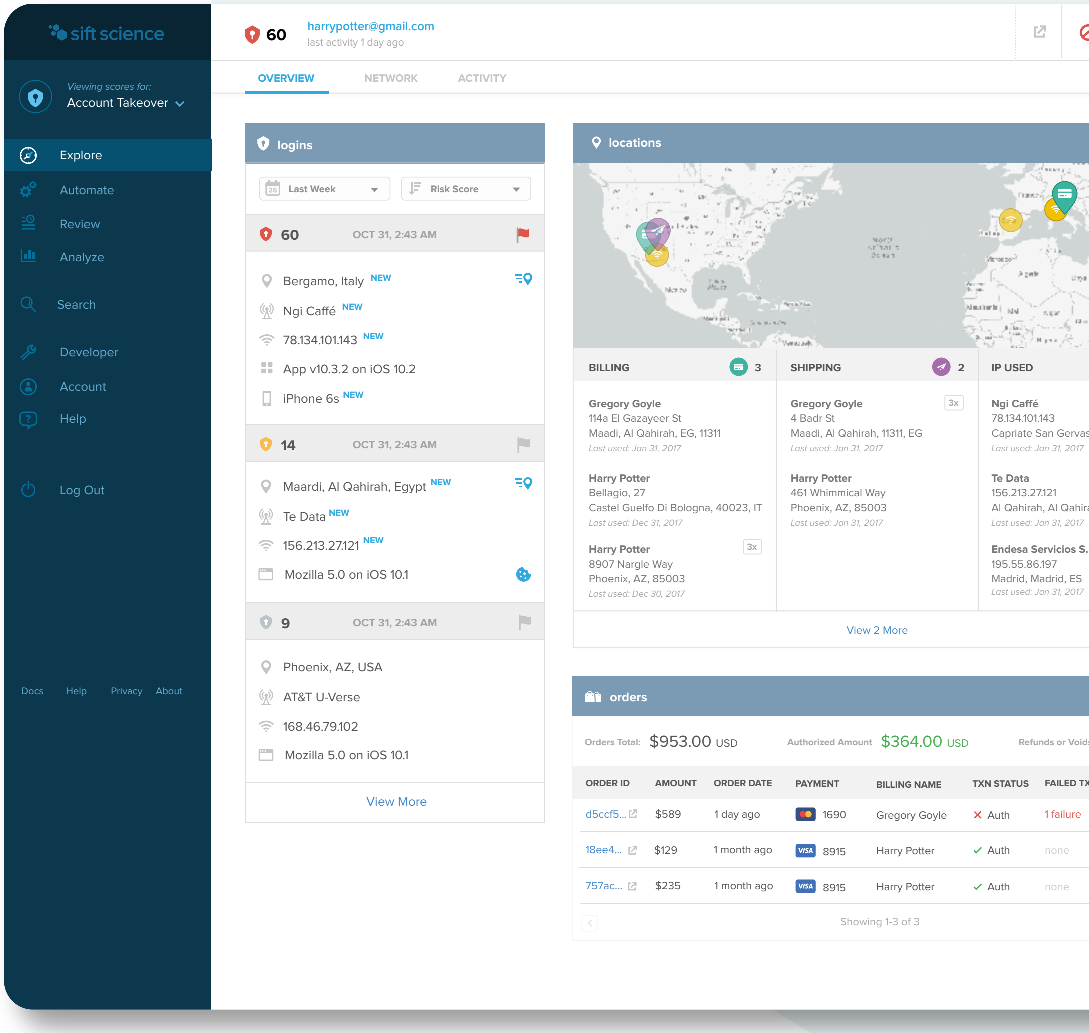
Sift Science’s accurate risk scores enable real-time decisions.

With Sift Science’s machine learning technology, you can quickly and accurately identify fraudulent and legitimate users – so you can serve up tailored experiences based on their risk levels.

First, Sift Science is able to authenticate user behavior through a range of active and passive signals, including behavioral signals, locational signals, and device and network information. Then, our real-time machine learning assigns a risk score to each user as they interact with your app or mobile site. These scores are updated each time the user takes a new action – on your site or app, or on any of the sites or apps across our vast customer network.

Once the user has a risk score, you can set up custom workflows that remove authentication steps for legitimate users, or add additional checks for risky users. For example, based on Sift Science’s risk scores, OpenTable strategically removed the requirement that trusted users enter the CVV code from their credit card.

With Sift Science, not only can you reduce friction, but for your best users the coveted one-tap checkout experience is attainable. And you enjoy the knock-on effects from their simplified experience: more sales. All while keeping fraudsters and bots off of your platform.



60 harrypotter@gmail.com
last activity 1 day ago

logins

60 OCT 31, 2:43 AM
Bergamo, Italy NEW
Ngi Caffé NEW
78.134.101.143 NEW
App v10.3.2 on iOS 10.2
iPhone 6s NEW

14 OCT 31, 2:43 AM
Maardi, Al Qahirah, Egypt NEW
Te Data NEW
156.213.27.121 NEW
Mozilla 5.0 on iOS 10.1

9 OCT 31, 2:43 AM
Phoenix, AZ, USA
AT&T U-Verse
168.46.79.102
Mozilla 5.0 on iOS 10.1

locations

BILLING 3	SHIPPING 2	IP USED
Gregory Goyle 114a El Gazayeer St Maadi, Al Qahirah, EG, 11311 *Last used: Jan 31, 2017*	**Gregory Goyle** 3x 4 Badr St Maadi, Al Qahirah, 11311, EG *Last used: Jan 31, 2017*	**Ngi Caffé** 78.134.101.143 Capriate San Gervas *Last used: Jan 31, 2017*
Harry Potter Bellagio, 27 Castel Guelfo Di Bologna, 40023, IT *Last used: Dec 31, 2017*	**Harry Potter** 461 Whimmical Way Phoenix, AZ, 85003 *Last used: Jan 31, 2017*	**Te Data** 156.213.27.121 Al Qahirah, Al Qahira *Last used: Jan 31, 2017*
Harry Potter 3x 8907 Nargle Way Phoenix, AZ, 85003 *Last used: Dec 30, 2017*		**Endesa Servicios S.** 195.55.86.197 Madrid, Madrid, ES *Last used: Jan 31, 2017*

orders

Orders Total: $953.00 USD Authorized Amount $364.00 USD Refunds or Void

ORDER ID	AMOUNT	ORDER DATE	PAYMENT	BILLING NAME	TXN STATUS	FAILED TX
d5ccf5...	$589	1 day ago	1690	Gregory Goyle	✗ Auth	1 failure
18ee4...	$129	1 month ago	VISA 8915	Harry Potter	✓ Auth	none
757ac...	$235	1 month ago	VISA 8915	Harry Potter	✓ Auth	none

Showing 1-3 of 3

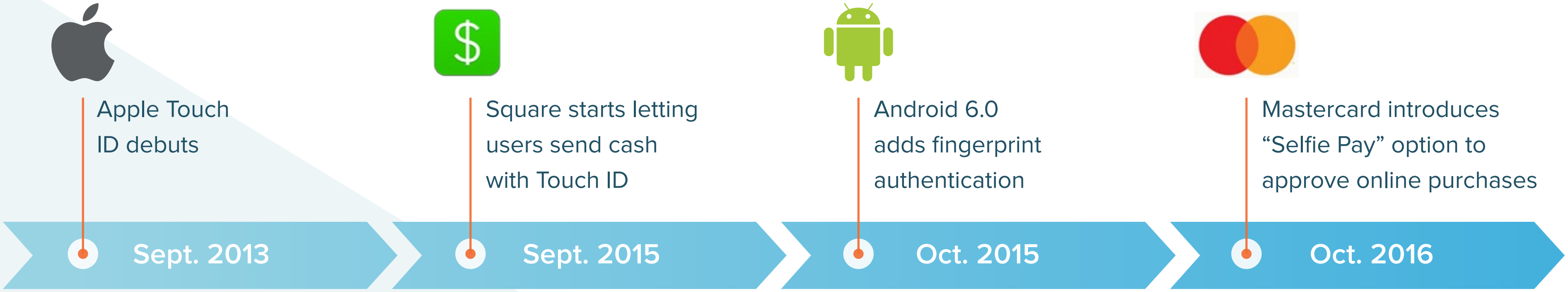
Mobile opportunity #3: Embrace easier authentication

The password should be dead by now. That's the consensus of multiple security experts, who say they're just not secure enough to adequately protect user accounts. Just think about it: over the past few years, massive data breaches at companies including Yahoo, LinkedIn, and Dropbox have flooded the black market with user credentials. Since 59% of people reuse passwords across multiple sites, it's easy for fraudsters to use the stolen passwords to commit account takeover attacks and – ultimately – payment fraud, scams, spam, and more.

But what are the alternatives to passwords for authentication? Steps like 3D Secure, two-factor authentication, and Captchas may work in certain circumstances, but if used too liberally, they are certainly damaging to conversion rates.

On the other hand, mobile devices seem tailormade to authenticate users securely – without adding unnecessary friction. For example, every smartphone is equipped with a camera. Instead of cancelling an order, why not offer the option to prove your identity with a selfie, or a photo of your driver's license?

Fingerprints are another biometric opportunity for authentication that's becoming more and more common. And there are startups launching that are working towards verifying purchases using voice recognition technology.



Apple Touch ID debuts

Sept. 2013

Square starts letting users send cash with Touch ID

Sept. 2015

Android 6.0 adds fingerprint authentication

Oct. 2015

Mastercard introduces "Selfie Pay" option to approve online purchases

Oct. 2016

The bottom line: mobile-unfriendly options like 3D Secure and Captchas don't have to be the default for user authentication. Try leveraging one of the newer, more secure, and less onerous mobile-specific authentication methods as part of your fraud management processes.

How Sift Science can help

Sift Science's automation features save time and offer flexibility

Sift Science offers the capability to automate fraud management, reducing the amount of transactions that require manual review and reducing your dependency on high-friction, high-cost anti-fraud measures like 3D Secure and SMS verification.

This capability is ideal for mobile-only or mobile-first businesses that have the need for speed. For example, if someone is using their phone to book a ride or reserve a last-minute room, there's little time for a team to manually review orders. Users expect their car or their hotel immediately. And even for physical goods, shoppers may be on the go, or unwilling to jump through the hoops expected when they're on their phones.

The Sift Science mobile SDKs for Android and iOS provide comprehensive fraud prevention on a single platform, with a single integration. Capture data across the entire user journey – including mobile apps, mobile browsers, desktop, and backend systems – and create dynamic experiences based on Sift Science's accurate, real-time risk scores. That way, you can improve conversion and reduce fraud across every customer touchpoint.

MOBILE BUSINESSES LOVE SIFT SCIENCE

HotelTonight, a mobile travel app

50% reduction in chargebacks

6.5X more orders blocked automatically

> *Our business is time-sensitive, and we needed to find a solution that quickly and effectively helped reduce fraud issues within our system. Fraud used to keep me up at night – now it doesn't."* **Sam Shank, CEO and Founder, HotelTonight**

Wanelo, a mobile-focused shopping marketplace

77% drop in dispute rate

52% decrease in decline rate

> *We no longer simply react to fraud but can now take a proactive approach to prevent it and create better efficiencies for our business."* **Courtney Bode, Marketplace Operations Manager, Wanelo**

SeatGeek, a ticketing site with 60%+ mobile traffic

60X return on investment

$600K+ monthly savings

> *Sift Science is a holistic and well-rounded fraud solution – we can send any and all the data that we want, and we get back all of the actionable information that we wouldn't have found on our own."*
>
> **Nicole Grazioso, Payments & Risk Manager, SeatGeek**