sift

Welcome to the new Era of Account Security

A layered approach to stopping account takeover fraud

Contents

Securing User Accounts in an Evolving Fraud Landscape

Legacy account security—e.g., passwords and usernames—is nearing the end of its usefulness as a means to protect against account takeover (ATO) fraud. In fact, ATO is growing exponentially. Accelerated by the global pandemic, more consumers are relying on online services rather than brick-and-mortar stores—leading to a reliance on digital accounts and the need to protect those accounts from cybercriminals who want to exploit the contents of said accounts, like stored value, payment information, demographics, and personally identifiable information (PII).

The proof is in the pudding: according to Sift research, **ATO attacks against the fintech sector alone soared 850% between Q2 2020 and Q2 2021.** During the recent 2021 Black Friday/Cyber Monday shopping period, account takeover fraud rates rose by a gut-wrenching **2,950%** in the omnichannel retail sector, on top of a **62%** increase in attempted payment fraud. And of the consumers who responded to a recent Sift-sponsored survey, **almost half (48%) of ATO victims have had their accounts compromised between two and five times**, meaning it's not just a one-time inconvenience, but an ongoing threat.

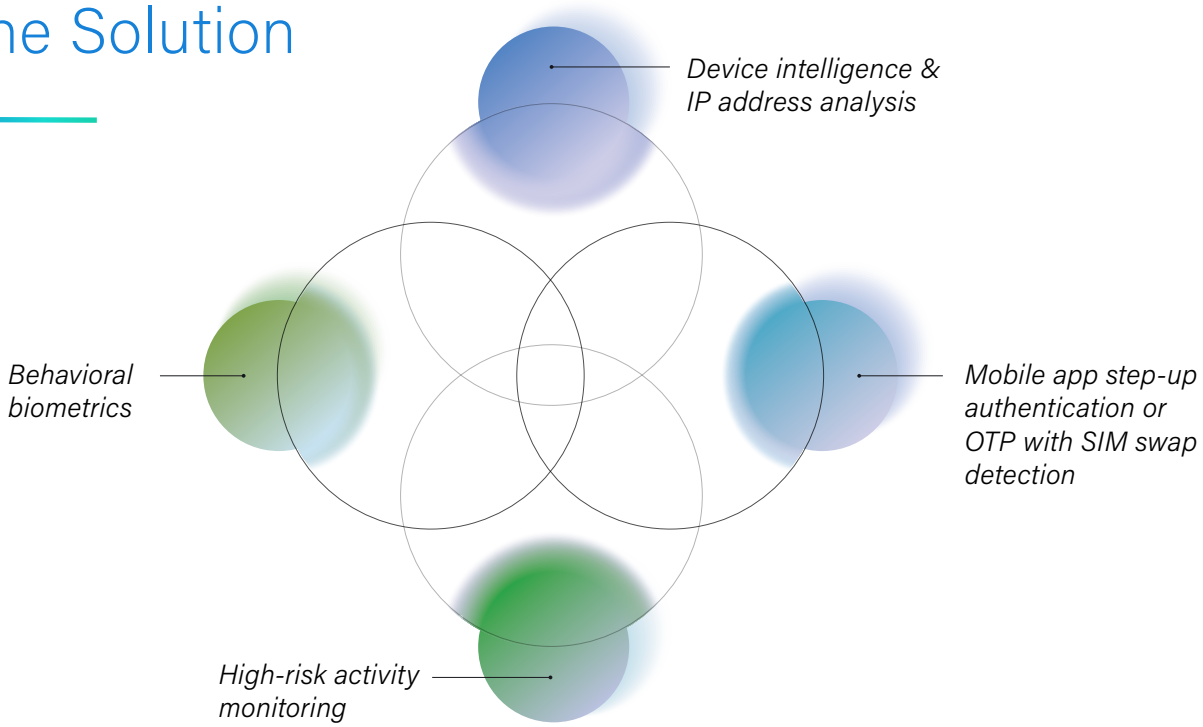
ATO attacks against the fintech sector alone soared 850% between Q2 2020 and Q2 2021.

The digital-first nature of modern business presents unique challenges in comparison to brick-and-mortar institutions. Many online businesses only have a digital presence, and therefore never interact with users in-person, making identity verification challenging. Universally poor password hygiene has contributed to the success of rising social engineering attacks—**the average person reuses a single password as many as 14 times across various accounts***, and research from LastPass shows that **65% of people globally use the same password for every account they own**. With widespread data breaches revealing PII and login information for millions of users, and more fraudsters applying sophisticated tactics like bots and credential stuffing, protecting accounts is becoming increasingly difficult, and will only become more challenging in the future.

And this isn't just a matter of security—there's a real financial impact to businesses that don't effectively secure their users' accounts from takeover attempts. In a recent survey, **74% of consumers would stop engaging with a site or app and select another provider if their account was hacked on that site or app**.

Successful online businesses need a multi-pronged, layered approach that addresses every step of the user journey, authenticates users, secures accounts, and stops ATO while also future-proofing against the more aggressive fraud attacks that are emerging every day.

The Solution



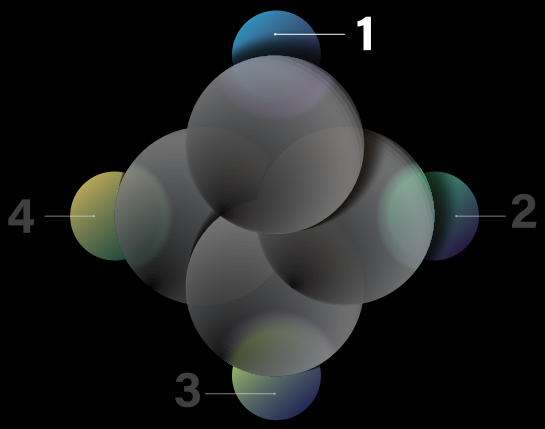
While it's common for security vendors to encourage organizations to implement a layered defense strategy for account security, this concept can mislead some into believing all risk controls within those layers are universally applicable. The ideal approach is to develop an account security framework and strategy that uses the right balance of passive detection and **Dynamic Friction** within the context of your business and user expectations. Before selecting which layers are relevant to your account security strategy, it's important to understand the intention of each layer through the lens of an attack and defense framework. In this framework, a defense is tailored to specific attack vectors with special attention being made to include the most common risks an organization encounters.

Each layer can be viewed as a tool among many to be deployed to address the different points of the user journey. Before addressing solutions, it's important to understand some of the common attack methods.

Stolen login credentials	***Credential stuffing***	***OTP attacks***

First Layer of Defense:

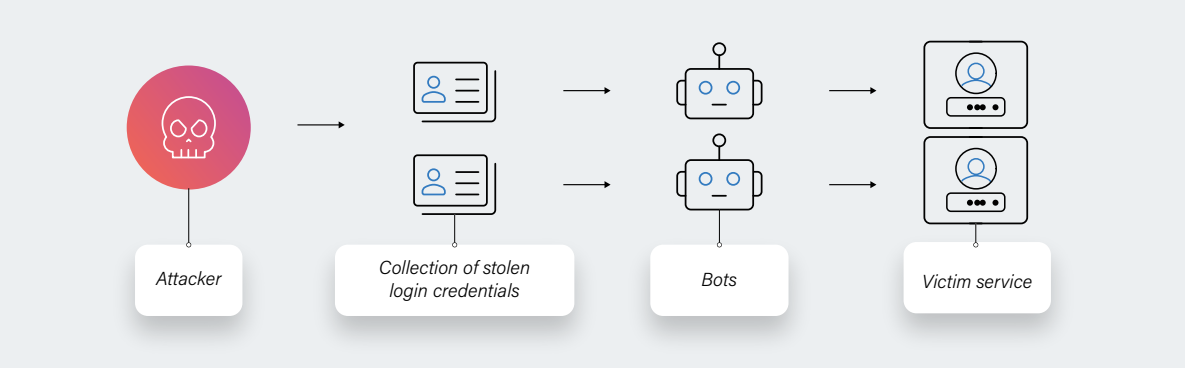
Device intelligence & IP address analysis



Stolen login credential attacks & credential stuffing attacks

While it's become common for fraudsters to gain access to compromised account credentials (whether that's through the dark web, phishing, or some other means), it's much less common for nefarious actors to gain control over a victim's device. With this in mind, a common way to detect an account takeover attempt is to analyze the device being used to login. Because legitimate consumers use multiple devices and commonly switch out old devices for new ones, an unfamiliar device is not necessarily indicative of fraud. Instead, device intelligence is often more useful in detecting trusted return users than it is to detect fraudsters. In addition to analyzing the device, it's also important to analyze the connecting IP address to determine if this is an IP the customer has used in the past. A login to an account with an unfamiliar device that has a familiar and commonly used IP address may be a signal that the legitimate user has a different or new device. If both the device and IP address are unfamiliar, this indicates a higher-risk login event.

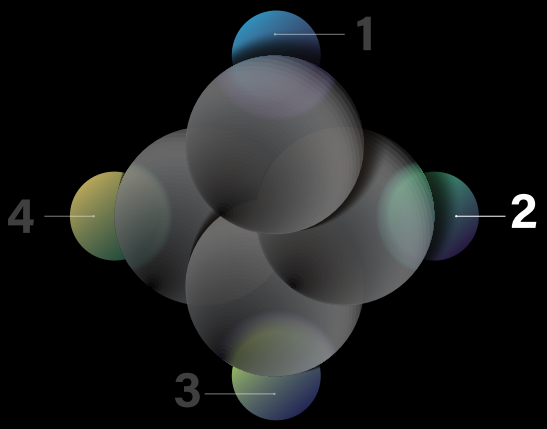
Credential stuffing attacks are a form of stolen login credential attacks, and are automated using scripts and/or bots. In this type of attack, bad actors use these automated tools to test large lists of stolen login credentials at known popular websites. It is common for these tools to rotate through proxy IP addresses in hopes of completing the attacks undetected.



So how do you protect against such sophisticated attacks? It takes a layered approach tailored to the specific needs of your business.

Second Layer of Defense:

Mobile app step-up authentication or OTP with SIM swap detection

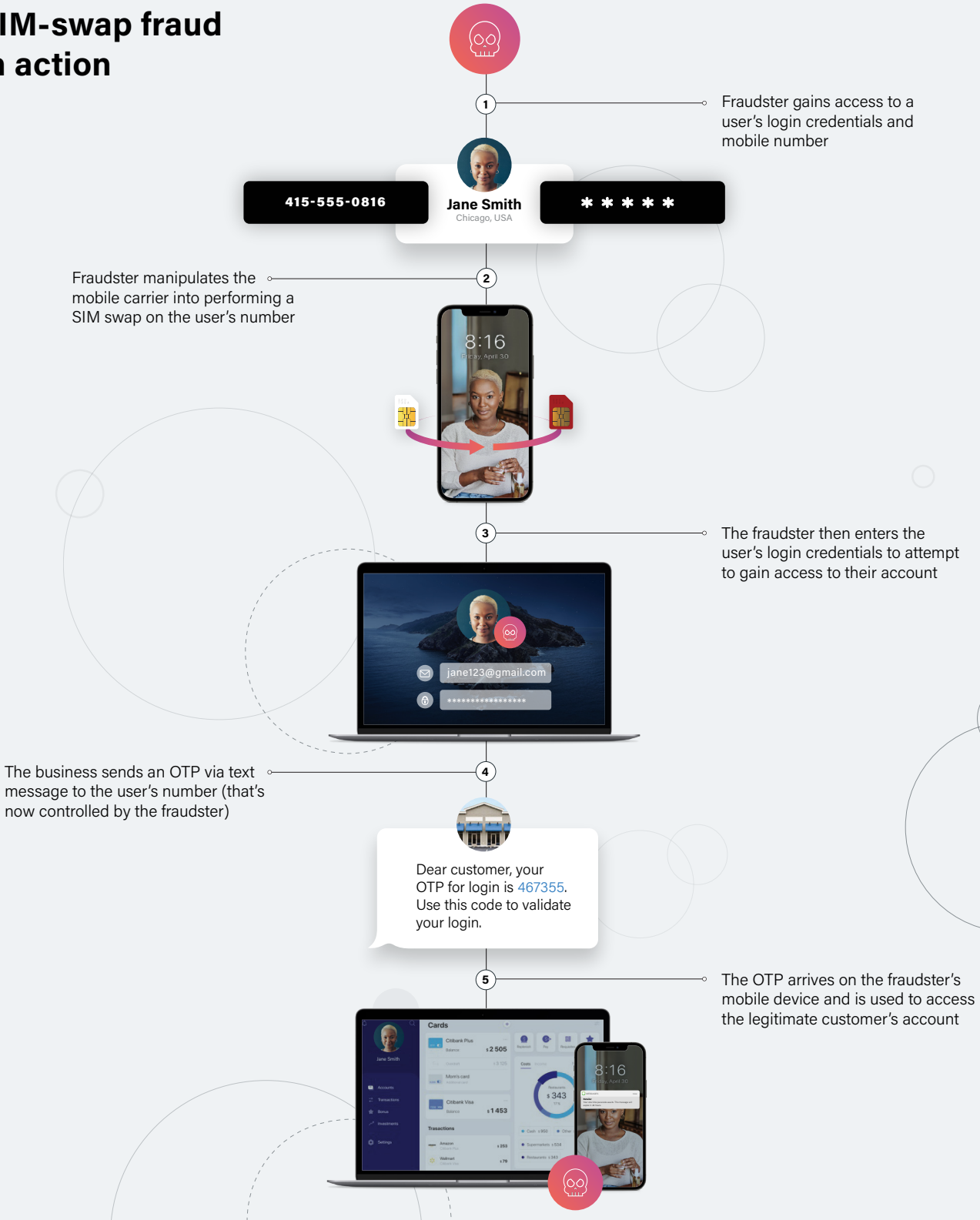


OTP intercept via SIM swap attack

One-time passcodes (OTPs) have become the most common authentication solution due to the scale of email and mobile phone adoption. The intention of authentication OTPs delivered via email and text is to rely on known contact details from the account to verify recent activity. The contact credentials on the account are trusted in theory because they're owned and accessed only by the user. Because OTPs are such a popular form of authentication, bad actors have developed multiple ways to intercept the codes before they reach the legitimate user. One common way to intercept OTPs sent via text message is through SIM swap attacks. This is where a fraudster temporarily gains access to a victim's phone number and receives calls and texts sent while they have control of the line. This is done by socially engineering the victim's mobile phone company and convincing them to transfer the line to a different SIM card. Once they have access, they can go through the standard password reset flow and receive the OTP before the victim realizes they have lost mobile service.

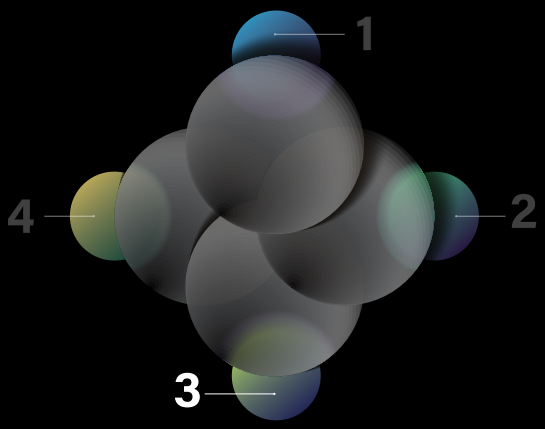
If fraudsters are intercepting OTPs meant for legitimate users, an alternative solution is to require users to authenticate themselves through a service's mobile application that leverages in-app authentication, e.g., logging into an account using a fingerprint. This can be done via biometrics or in-app, two-way communication. For consumers not willing to use a service's mobile application, the risk of OTPs can be minimized through SIM swap detection capabilities. These solutions query the user's mobile phone carrier for signals that indicate recent changes. When a high-risk change is detected, the OTP can be delivered via a tenured email address or the user can be encouraged to call in to authenticate with a service agent.

SIM-swap fraud in action



Third Layer of Defense:

High-risk activity monitoring

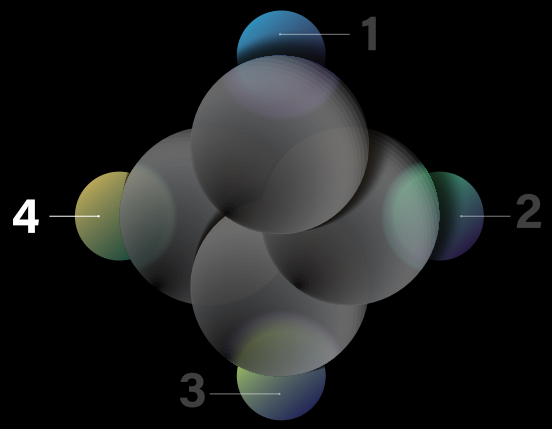


When a digital criminal gains access to your customers' accounts

In the event a cybercriminal defeats the first two layers of defense and makes it into a customer account, it's not too late to protect the account. Bad actors are aware the lifespan of stolen account credentials is finite, so they often try to monetize the account as quickly as possible. This may show up as atypical account activity, which can then be evaluated for risk. For example, if an email address and/or phone number is changed and then a high-risk activity—like a withdrawal or transfer—is performed immediately after the change, this can be a sign of an account takeover attempt. The trust and safety team can decide to restrict the account from performing high-risk activities until the account is confirmed as secured.

Fourth Layer of Defense:

Behavioral biometrics



Social Engineering: When the login is from the legitimate customer

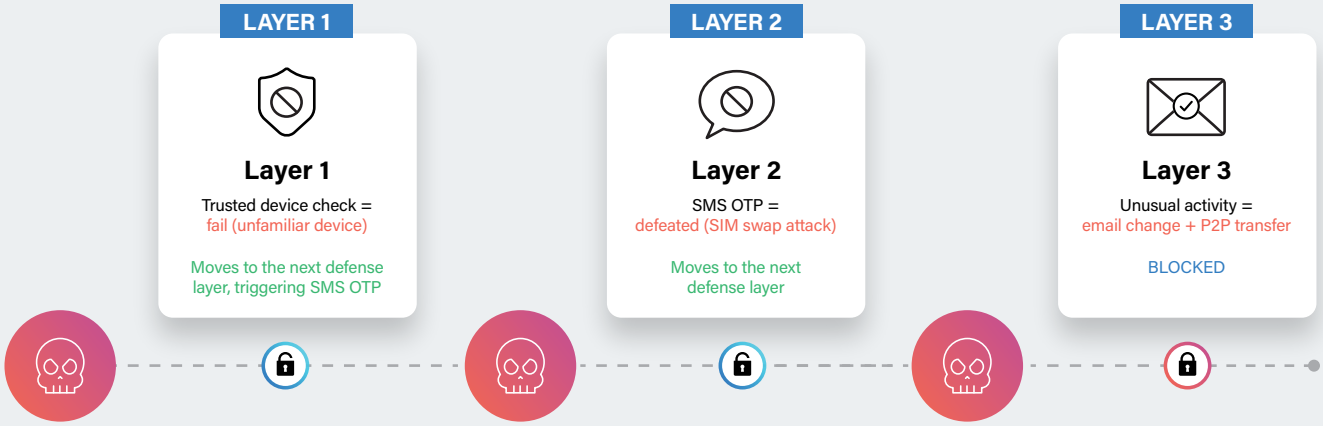
Ninety-eight percent **of cybercrime involves social engineering, with attacks becoming increasingly complex. In many social engineering attacks, the victim is being guided to perform multiple actions within their account.** During these attacks, the customer's behavior can signal they are using the service differently than is usual. While bad actors are instructing customers, there can be a delay or hesitation between actions taken by the victim. The victim may not understand what the fraudster is asking or they may probe for additional detail. While this is occurring, the account session may appear unusual by being longer, showing idle cursor behavior, or even aimless cursor movement to prevent page timeouts. The victim may be asked to transfer funds to a specific account or perform an activity they have not performed before. This increases the chance that mistakes, such as typos or clicking on the wrong section of a page, will occur. This can be captured and evaluated through a solution called behavior biometrics.

Another social engineering scam has the fraudster convincing the customer to allow remote access to their machine. This also can be detected with behavior solutions that monitor for evidence of a remote access connection. When an account is suspected as being involved in a social engineering scam, there's an opportunity to restrict and limit the account from further high-risk activities.

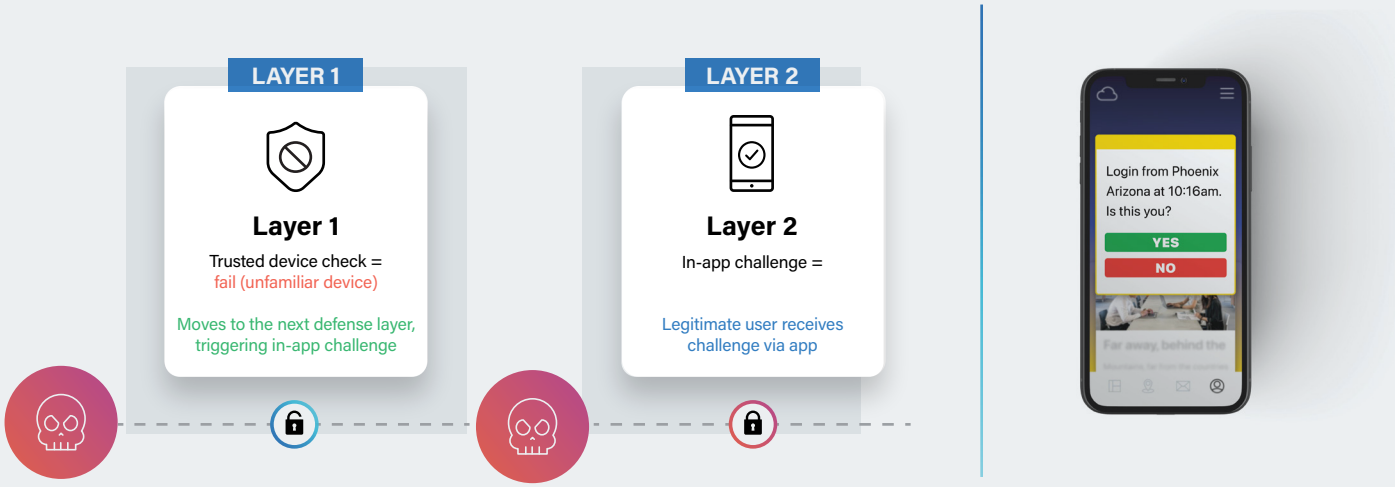
ATTACK	DEFENSE LAYER
Fraudster logs in with stolen credentials	Device intelligence detects unfamiliar device
Fraudster triggers password reset flow and intercepts OTP delivered via text message	• Replace OTP with in-app biometrics or in-app security challenge/question • SIM Swap detection on phone line prior to OTP
Social engineering	Behavior analysis detects anomalous account activity
Credential stuffing	Device intelligence detects scripted login attempts

Protecting accounts against these types of complex attacks requires access to, and analysis of, real-time data at multiple touch points. This includes second-level security considerations that trigger automatically, ensuring that trusted users aren't penalized for an atypical behavior or two—while fraud is pinpointed accurately and stopped swiftly, regardless of how quickly or broadly a business is targeted.

Dynamic Friction plays a critical role here, guiding users along whatever experience is appropriate for them on your site, and preventing cybercriminals from successfully mimicking trustworthy customers.



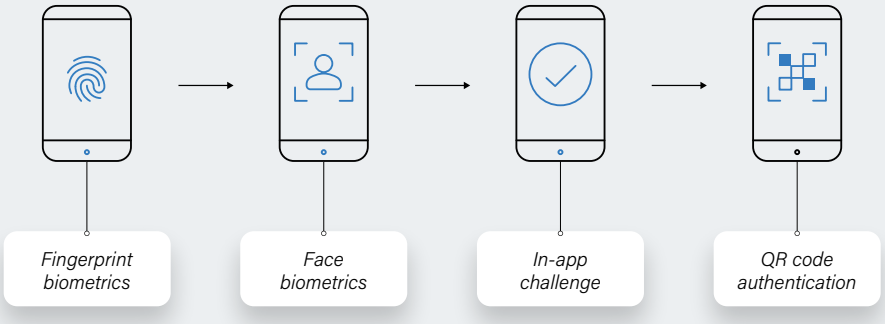
This illustration shows how a layered approach to account security works. If a fraudster is able to circumvent one layer, an additional layer of friction is required to prevent ATO.



This illustration shows how in-app challenges can improve account security. If a fraudster acquires login credentials and fails device identification, an in-app challenge can be an effective backup. The best solution to combating compromised passwords is to stop using passwords.

Outside of social engineering, the common theme between many ATO attack vectors is compromised usernames and passwords. And while there are many solutions to help mitigate the risks of stolen account credentials, the best solution is to eliminate passwords altogether.

Passwordless login



The image above shows common passwordless technologies that are available today to authenticate users. Many passwordless solutions rely on multi-factor authentication (MFA). But not all MFA solutions are created equal, so there's a lot to consider when selecting the right solution for your business.

- ☐ **Are you a mobile-first company?** Organizations leading with a mobile-first strategy may have the majority of their users utilizing their mobile application. This makes adopting authentication controls that are reliant on a native mobile app more realistic. A company that has minimal mobile application adoption may have to consider mobile authentication solutions as a partial account security strategy with other solutions for non-mobile app channels.

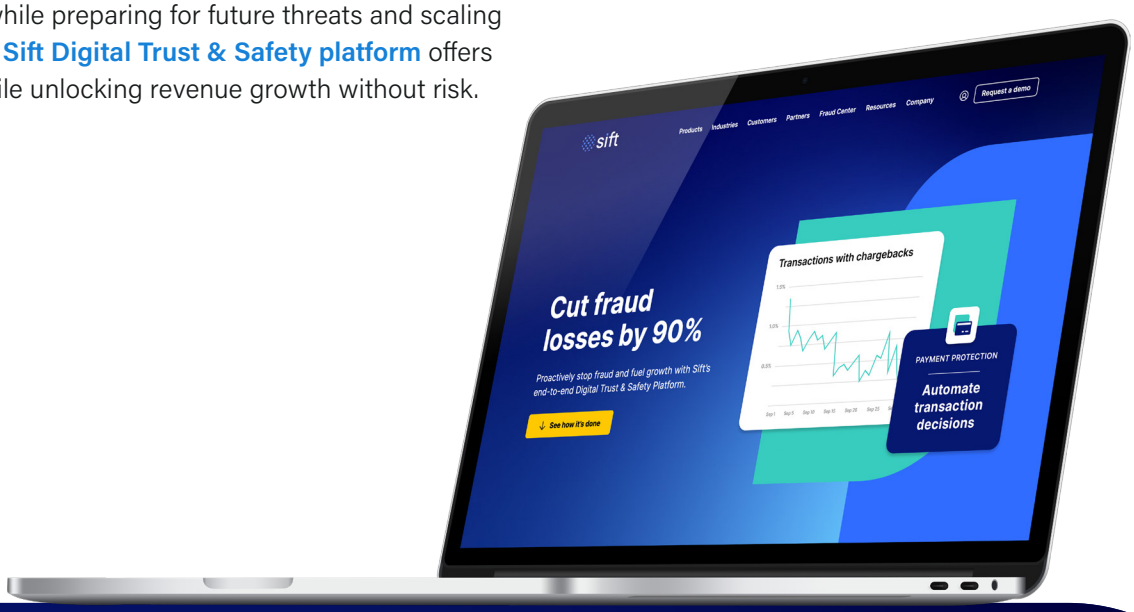
- ☐ **Do you have a backup strategy?** There will be scenarios in which users do not have access to their mobile app but need to use the service. For a financial services company, this means potentially limiting access to a user's money. For an online merchant, this means missing out on potential sales and lost revenue. OTPs are an example of a backup option.

- ☐ **For biometric solutions, how do the solutions keep users' data private?** Are there safeguards in place that encrypt biometric data? Does the solution have liveness detection, behavioral biometrics, or other means of ensuring accuracy?

Digital Trust & Safety for Account Security

ATO manifests in many different ways, with new attack vectors showing up every day. To be fully prepared for evolving threats, having the ability to choose from a variety of solutions and incorporate them into an account security strategy is critical. Additional layers of security do not automatically equate to a safer customer journey, unless those layers are applied within an overall framework that aims to balance both security and the user experience.

With Sift, businesses gain access to a platform that provides comprehensive protection to secure accounts, authenticate users, and fuel growth today while preparing for future threats and scaling with your business. The **Sift Digital Trust & Safety platform** offers unrivaled protection while unlocking revenue growth without risk.



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.