



✓ riskified

The Login Dilemma: Shopping in the Age of Account Takeovers

Riskified's 2020 Account Security
Survey Results



* * * * *

Table of Contents

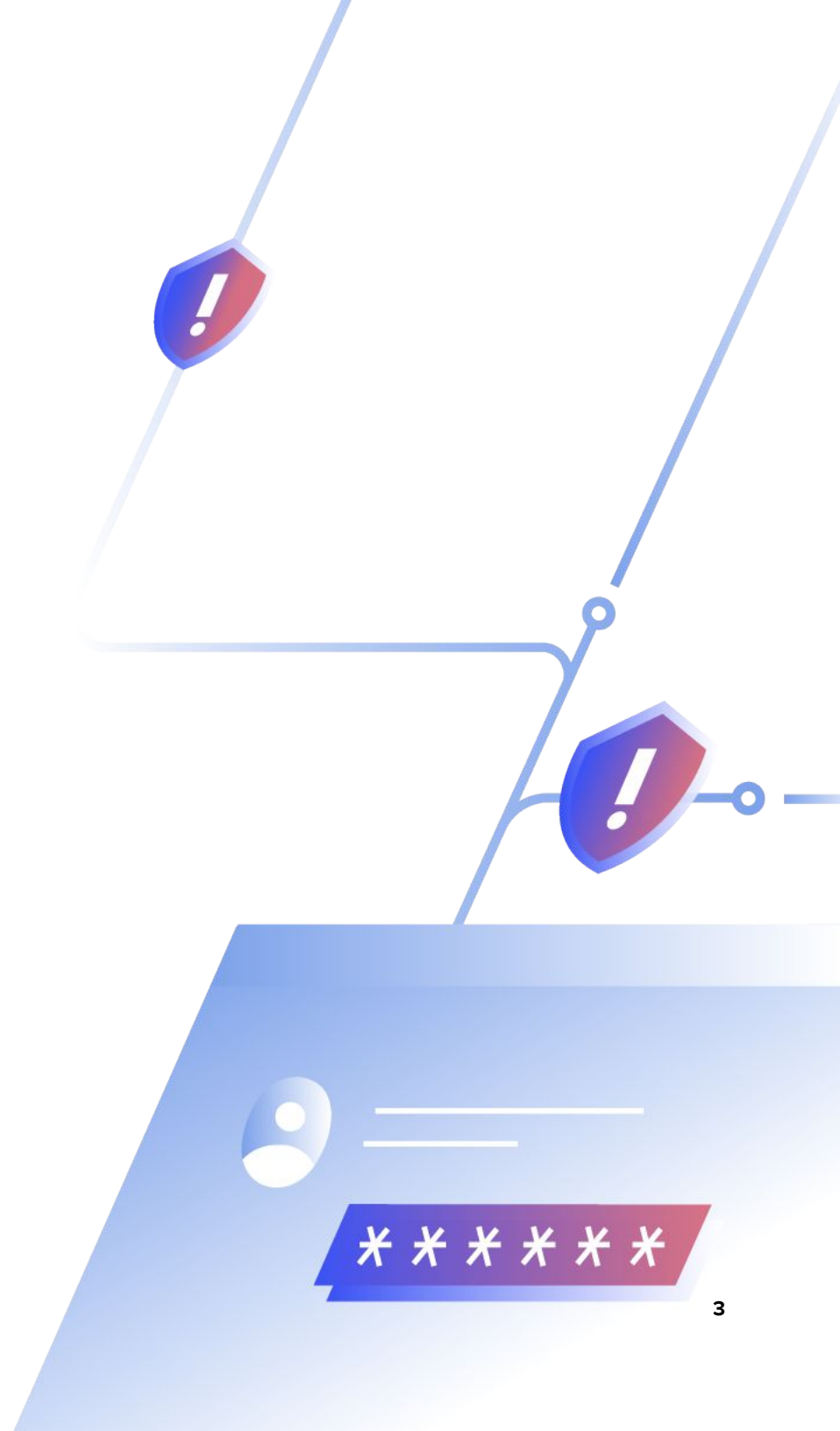
Executive summary	<u>3</u>
.....	
Introduction	<u>5</u>
.....	
01 What are ATOs and how do they happen?	<u>6</u>
.....	
02 Riskified's Account Security Survey	<u>13</u>
.....	
03 How to protect your store from ATO attacks	<u>26</u>
.....	
Conclusion	<u>29</u>
.....	

Executive Summary

Account takeover attacks (ATOs) are on the rise: fraudsters have learned that while they require a little more effort, they yield better rewards than basic CNP fraud. ATOs also cause a great deal more harm. To customers, they can feel like a personal attack, and the compromised information fraudsters obtain through ATOs can have a lasting impact. Merchants, on their end, may suffer residual damage to their bottom-line.

Earlier this year, Riskified conducted our most comprehensive survey to date on account security, participated by 4,000 online shoppers and 425 merchants. We learned why store accounts are so critical to shoppers and merchants, and saw how ATOs drive a wedge between them, damaging brands' hard-earned reputation.

This report explores how cybercriminals obtain legitimate login credentials, examines key MOs, and breaks down the variety of fraudulent schemes available to these bad actors once they breach an account. Read to discover actionable insights on customers' and retailers' attitudes towards account takeovers, and learn tips to detect a bad actor at the first point of contact: the login.



You'll find insights on:

01 What are ATOs and how do they happen?

ATO attacks are multi-layered acts of fraud. First, a bad actor must obtain the login credentials to a good customer's online store account. While the methods for doing that are typically more complex than simply buying stolen credit card details on the dark web—often involving advanced manipulation techniques and technological savvy—the effort is often worthwhile. Once a customer's account is breached, there is a smörgåsbord of fraud schemes to pursue. This chapter breaks down the methods fraudsters use to obtain login credentials and explores the main fraud tactics they employ once they gain account access.

02 Account Security Survey Results

How do customers and merchants feel about ATOs? Our 2020 Account Security Survey measured the pervasiveness and impact of ATO attacks. The majority of eCommerce transactions today happen via store accounts.

Shoppers have come to expect the frictionless experience these accounts facilitate, and the loyalty perks that come with them, and are much more likely to return to a store where they are account holders. That is why store accounts are central to merchant-consumer relationships and to a shopper's lifetime value. But how confident are your customers in their security, and what happens when these accounts are compromised? In this chapter, we share the most compelling and actionable insights we discovered.

03 How to protect your store from ATO attacks

The fundamental challenge in stopping ATOs is that merchants do not have enough data to work with at the point of login to make a reliable decision. What can merchants do to increase accuracy when making high-stakes approve or decline decisions? The answer lies in mixing the right "cocktail" of data points, including IP geo data, behavioral analytics, and spoofing detection, to name a few. In this chapter, we share tips on how merchants can obtain additional data points to aid in their decision.

Introduction

Account takeover (ATO) attacks are more devious than your standard CNP fraud. When fraudsters gain access to legitimate customers' store accounts, they obtain a wealth of high-value information. The fraudulent transactions that follow are harder to detect and stop because they look like they are made by known customers. ATOs are more costly, too: In addition to the lost revenue and the costs associated with chargebacks, these attacks have a devastating impact on brand reputation and the lifetime value of a customer.

A Riskified-commissioned survey of nearly 4500 participants provides insights into the negative impact ATOs have on both customers and merchants. Despite the increase in ATO attacks—more than one in three (35%) merchants reported that at least 10% of their accounts had been compromised in the last 12 months—many merchants do not have the necessary safety measures in place to fend off such attacks.

Customers, on their end, don't keep quiet when their accounts are breached. The majority of online account holders, 65%, said they would likely stop buying at the store, 54% said they would delete their account, and 30% said they would encourage friends to stop shopping with the merchant.

In this report, we examine ATO attacks and their consequences for merchants and customers. We also offer merchants tips on how to protect their brand and safeguard customer data.

01

What are ATOs and how do they happen?

Card Not Present (CNP) fraud happens when a fraudster buys stolen credit card details, usually on the dark web, and uses them to check out. Account Takeover (ATO) attacks add another layer: before committing the fraud, a bad actor gains access to a legitimate customer's eCommerce store account.

What is an ATO?

While ATOs are more complex, they are a lot more lucrative for fraudsters. Once a good customer's account is obtained, there is a smörgåsbord of fraud schemes they can attempt. They can make purchases with stored payment methods, expend loyalty points (think frequent flier miles), and steal valuable personal information to use and sell elsewhere. The types of personal data shoppers regularly store in their online account include their address, email, phone number, payment methods, and ID numbers, including passport numbers.

The tactics

The type of information typically stored in online accounts hints at the different vulnerabilities these accounts have. The ATOs we see on our network can be divided into three primary tactics: the login & checkout; data theft; and loyalty fraud.

The login & checkout

A bad actor logs into a store account and uses the stored credit card information to make a purchase. Since transactions by repeat customers are broadly recognized as 'safe,' merchants are less likely to question them. Even when merchants have a reason to doubt an account-associated transaction, our data show that they are often reluctant to decline it, not wanting to offend their loyal customer. Some merchants ask account holding customers to re-insert CVV codes. While this is good practice, it is far from foolproof.

Our data show that more than a third of merchants do not enforce regular CVV checks on stored payment methods with account-holding customers, often for technical or compliance-related reasons.

Even if you do not store payment methods in your online accounts, there are still vulnerabilities ripe for the picking. Fraudsters can use the account in conjunction with details of stolen credit cards unrelated to the account owner, taking advantage of the fact that loyal customers are more likely to have their orders approved. This may sound like a shopping pattern odd enough to raise red flags, but in fact, it is the most common ATO MO we see. When fraudsters check out from a known account, their orders are much harder to decline.



The tactics

Data theft

Not every successful account takeover concludes in a transaction. Fraudsters can cause a lot of damage by using the personal data stored in the account in other fraud MOs, including forms of identity theft. One scenario we have seen involves using PII stolen from one account to secure access to other store accounts owned by the same customer.

Loyalty fraud

This is any fraud that abuses a loyalty program, from using points or miles as currency, to transferring points to other accounts, in order to use them or sell them on the dark web.



The tactics

How do fraudsters get credentials?

The key ingredients of any ATO are a legitimate customer's username and password. Most of the time, login credentials are compromised through a phishing attack or a data breach.

Credential phishing is easy, cheap, and effective. Phishing specialists manipulate and trick account holders—or, in some cases, customer service representatives—into surrendering credentials. One scheme we've seen involves sending a legitimate customer an email prompting them to reset their store account password, then directing them to a mockup of the store's login page. Since the mockup looks identical to the original site, account holders can easily fall for such ploys, practically giving away their credentials. So-called phishing kits are available for sale on the dark web.

These types of phishing attacks are very common and highly effective: phishing emails enjoy a [30% open rate](#). Fraudsters are inundating the web with more and more 'traps': there are approximately [1.5M new phishing websites](#) published per month. [More than half \(56%\)](#) of mobile users received and clicked on phishing URLs in 2018.

30%

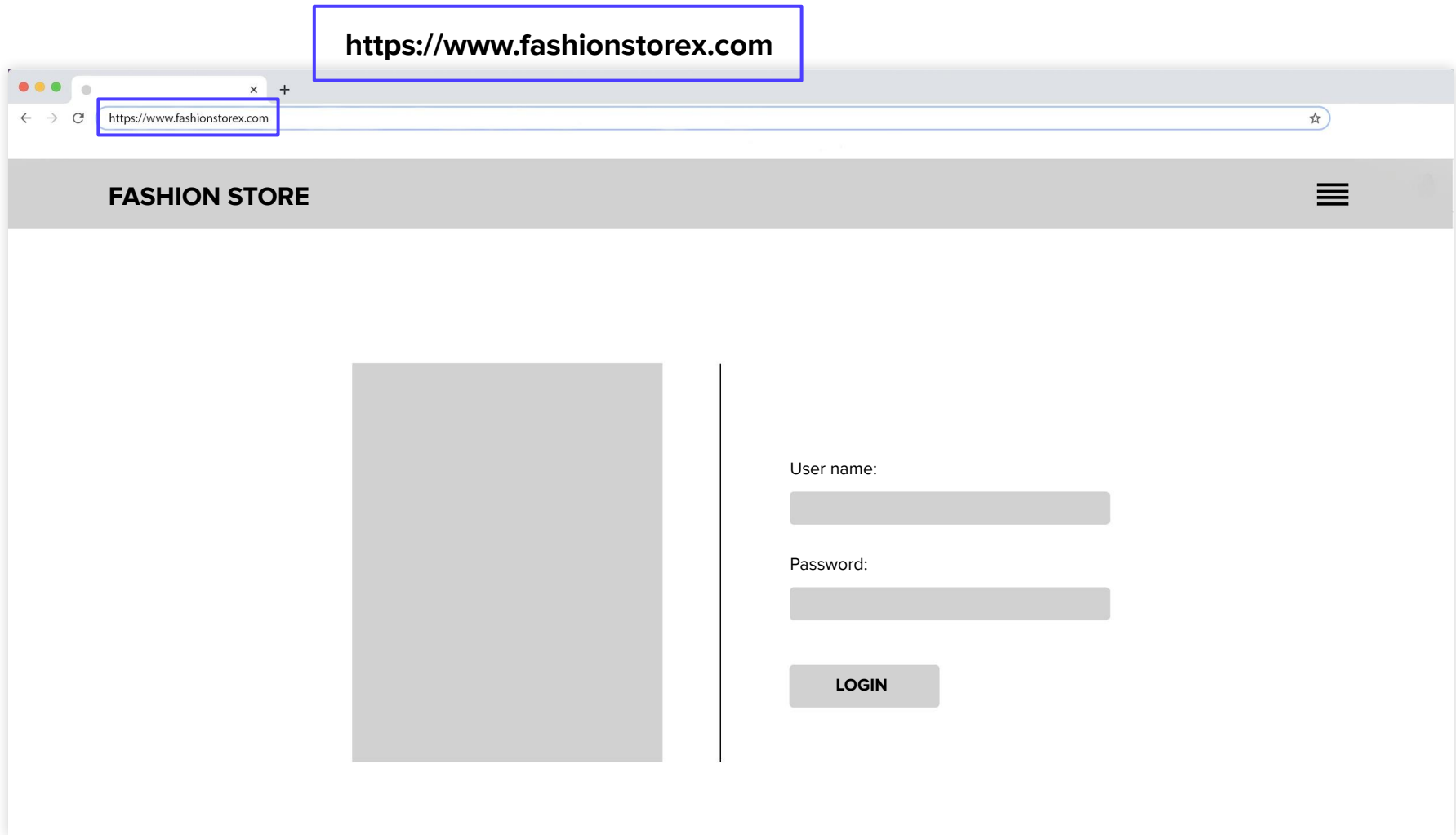
Open rate for phishing emails

1.5M

**New phishing websites published
each month**

56%

**User received and click phishing URL
on mobile in 2018**



The mockup looks exactly like the real site, except for a subtle change in the URL

A data breach is another common path to ATO. [Facebook, Yahoo, Twitter, LinkedIn, and Quora](#) have all fallen victim to breaches, leading to compromised personal information of billions of people.


One data element hackers get from these breaches is sets of credentials: usernames and password combinations.

Fraudsters can then use bots to test these credential sets at many different online stores. This process, called credential stuffing, is done en masse: hundreds and thousands of potential logins tested. When they detect a working set, hackers usually sell it on the dark web to other fraudsters who commit the actual ATO. In fact, a [report](#) by Swiss firm ImmuniWeb found there are more than 21 million stolen credentials for Fortune 500 companies for sale on the dark web. There are vast marketplace with a variety of products; fraudsters can buy validated credentials linked to accounts with guaranteed loyalty points or stored payment methods.

21M

Stolen credentials for Fortune 500 companies for sale on the dark web





with miles or point

Product example: Login: afmoo***84@gmail.com:!QA***r5 Available miles or point : 500

Sold by **cashboy** - 0 sold since March 21, 2019 **Vendor Level 4** **Trust level 4**

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: **USD 5.99**

Qty: **Buy Now** **Queue**

0.000676 BTC

Description

Feedback

Refund policy

with miles or point

Product example:

Login: afmoo***84@gmail.com:!QA***r5

Available miles or point : 500

Verified credentials are incredibly affordable on the dark web

02

Riskified's Account Security Survey

Earlier this year, Riskified commissioned a survey to measure the pervasiveness and impact of ATO attacks. A sample of over 4,000 US, UK, French, and German online customers and 425 eCommerce professionals participated.

This is the most comprehensive survey we have conducted to date on the issue of online store accounts: how central they are to merchant-consumer relationships, how critical they are to revenue growth, and how confident both consumers and retailers are in their security.

Here are some of the most compelling and actionable insights we found.



Most online shopping happens through store accounts

Offering secure store accounts is essential to both merchants and customers. Merchants say that account holders shop more often and spend more per purchase than other customers who check out as guests. 81% of customers said that more than half of their online transactions happen at stores where they hold accounts. Merchants reported that 64.4% of orders are made by customers who are logged in.

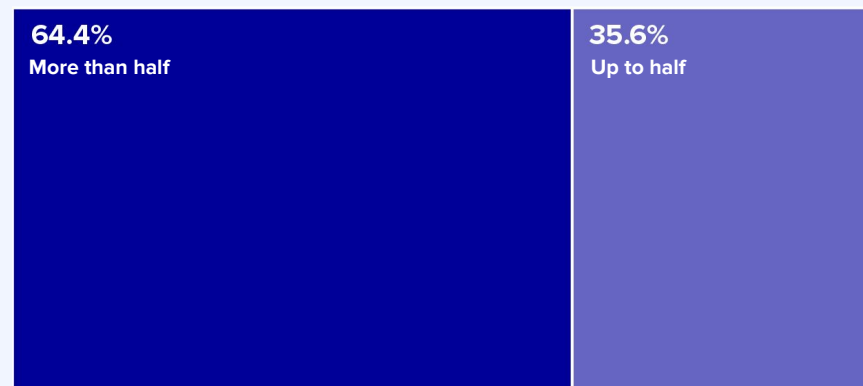
CUSTOMERS

What share of your online purchases are with business where you have an account?



MERCHANTS

What share of purchases at your store are made through store accounts?



○ Source: Riskified's Account Security Survey



Store accounts encourage higher-value carts, more shopping

The overwhelming response we received from merchants leaves no room for ambiguity. More than half reported that account holders shop more often, and check out higher-value carts. It really drives home this key point: store accounts are much more than a service to customers; they are assets. Every time a customer opens an account, their future expenditure prospect with the merchant increases, and their lifetime value can double or triple.

Merchants who say account holders shop more frequently (out of all the merchants who track these metrics)

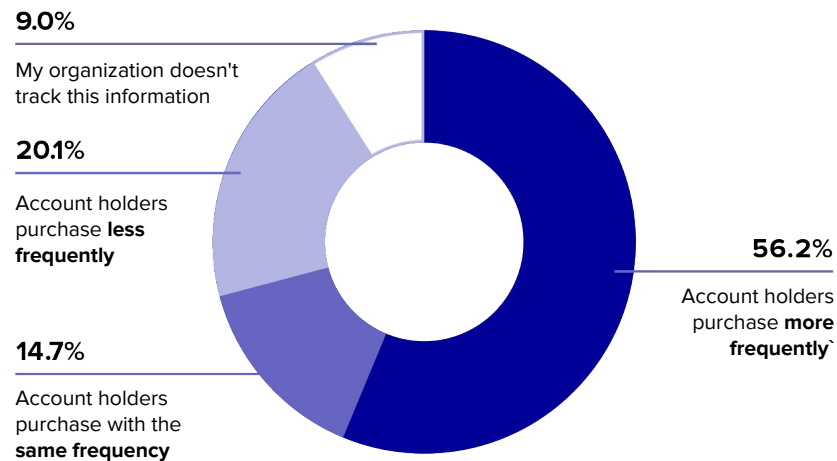
61.75%

Merchants who say account holders spend more per purchase (out of all the merchants who track these metrics)

54.8%

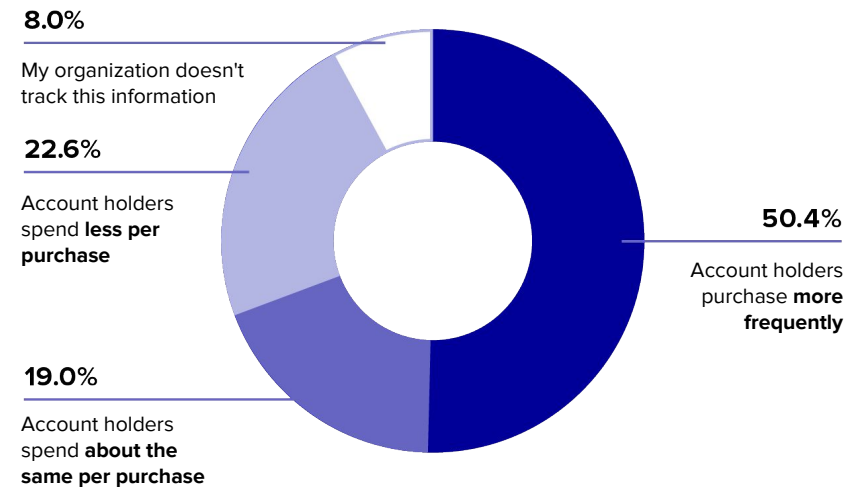
MERCHANTS

Which best describes cart *value* in account holders vs guest checkout?



MERCHANTS

Which best describes shopping *frequency* in account holders vs guest checkout?



○ Source: Riskified's Account Security Survey

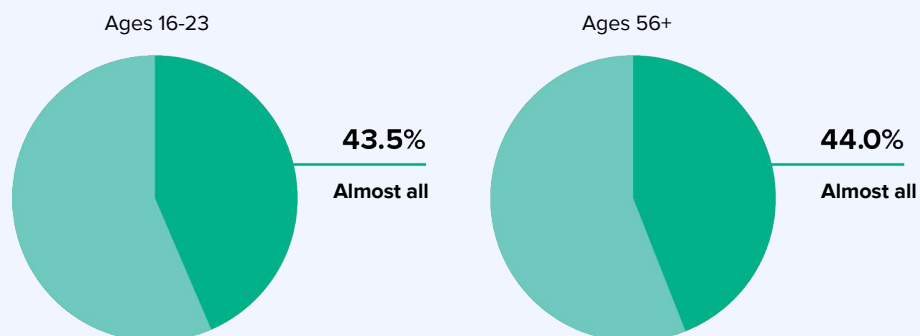


Store accounts are popular with everyone

Our survey shows that consumers of all ages shop more frequently at stores where they hold accounts. The majority of both laptop and mobile shoppers said that having a store account makes them buy more.

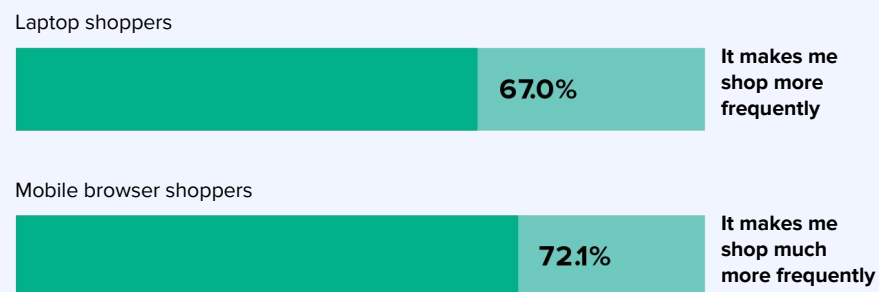
CUSTOMERS

What share of your online purchases are with business where you have an account?



CUSTOMERS

How does having a store account with a business impact your online shopping habits?



○ Source: Riskified's Account Security Survey



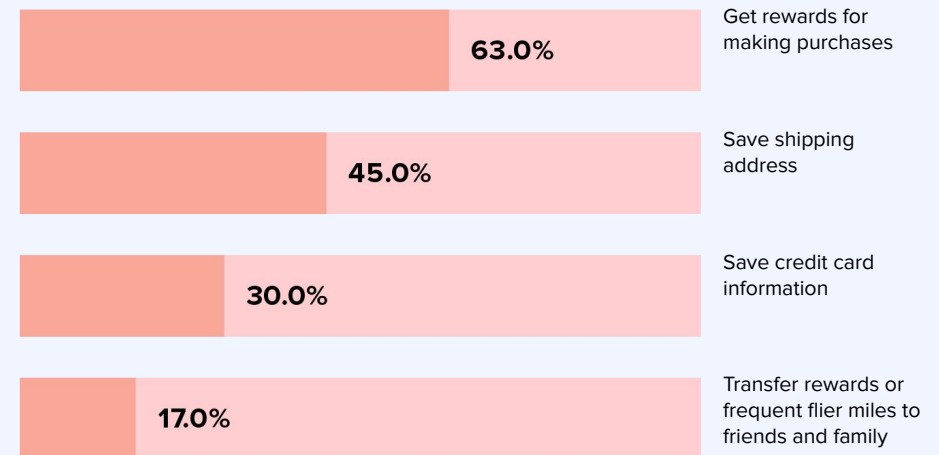
So how do you get users to subscribe?

Perks, the survey confirmed, are great motivators for people to open store accounts. It should come as no surprise that reward programs work: nearly two thirds of consumers said they would shop more with a business if they earned points.

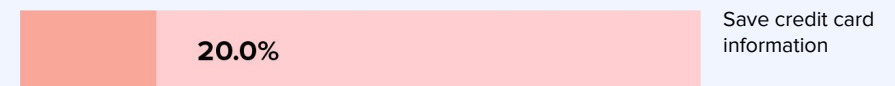
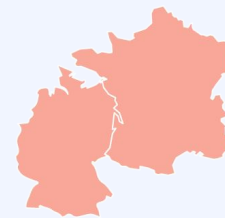
Perks, of course, go beyond accumulating points. Shoppers consider the option to securely store their personal information for future transactions a major perk. Nearly half of consumers said they would shop more frequently with a business that allows them to save their shipping address, and 30% also mentioned the ability to save their payment details as a motivator of future transactions. This demonstrates the importance consumers place on a smooth checkout process.

CUSTOMERS

Which of the following account perks would likely make you shop more frequently with a business?



In France and Germany, only about 20% of respondents said “save credit card information”



○ Source: Riskified’s Account Security Survey



The other side of the coin: how important is data security?

The challenge many merchants face is that every perk and service they offer creates a vulnerability that fraudsters can exploit. For example, many airlines and travel booking sites allow the transfer of points and miles between accounts. This practice is a boon for customers who want to combine their miles or share them with family, but it also makes it easy for fraudsters to whisk away precious loyalty rewards.

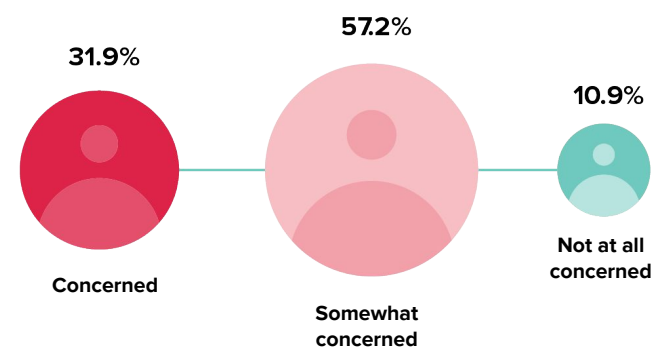
When it comes to account data, it is a balancing act. Allowing account holders to store personal information and payment methods can reduce friction. Merchants who add extra security steps at login, like two-factor authentication, re-introduce friction to the funnel and risk cart abandonment. Requiring complex passwords to boost security also packs on the friction. That said, the damages caused by ATOs can far surpass those related to friction. Customers seem to be very aware of this threat, with the majority saying they are somewhat or very concerned about having their accounts compromised. Nearly 20% of consumers said they've had accounts compromised within the past year.

Shoppers whose accounts had been compromised in the past year

20%

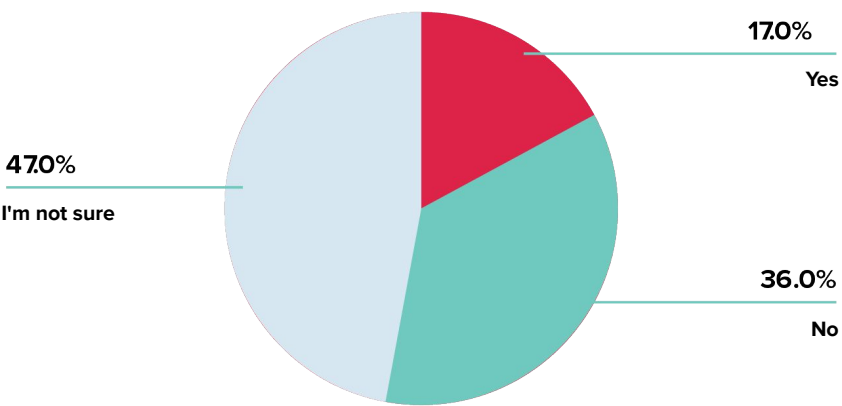
CUSTOMERS

How concerned are you about having one of your store accounts compromised?



CUSTOMERS

Over the last 12 months, did anyone gain access to any of your online shopping accounts without your permission?



○ Source: Riskified’s Account Security Survey

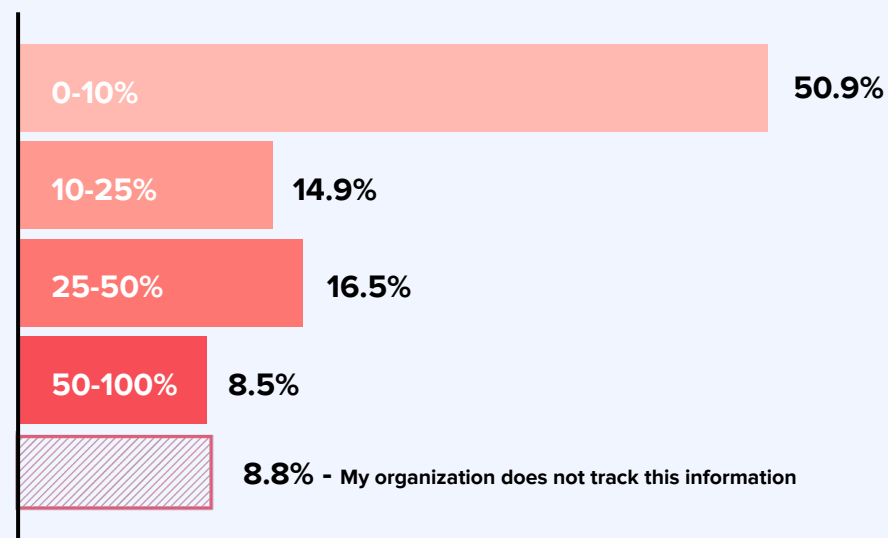


ATOs are pervasive

When we asked merchants about their experiences with ATO attacks, specifically how often their stores had been compromised in the past, the responses were dramatic. More than half of merchants reported having experienced ATO attacks within the last 12 months. Many saw a large percentage of their accounts compromised within this time frame, with 15% reporting 10-25% of their accounts had been breached, and 16.5% reporting breaches of 25-50% of their accounts. These numbers demonstrate just how widespread ATOs have become.

MERCHANTS

What share of accounts at your online store were compromised over the past 12 months?



● ATO rate

○ Source: Riskified's Account Security Survey



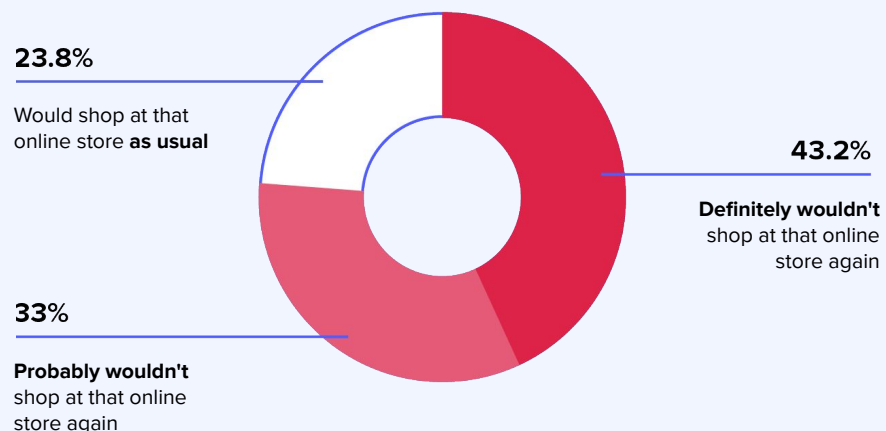
ATO recovery is no small feat

Not only are customers aware of the threat, they take breached accounts very seriously. In the aftermath of an ATO, customers typically have to spend hours fixing the damages caused: re-establishing their identity, resetting passwords, canceling credit cards and filing chargebacks. So, it's no surprise that most customers said they would be unlikely to shop online with a merchant again after an ATO. Additionally, many customers said they'd be vocal about the incident, posting about it on social media.

It is important to note that this type of brand-compromising response is unique to ATOs and is not typical to other types of CNP fraud. Conventional CNP fraud is a crime of opportunity, like having your wallet lifted in a packed subway car. An ATO attack can feel a lot more personal because it targets the victim's identity and private information. ATOs can feel analogous to having your home burglarized, with the merchant, who was entrusted with the keys, letting the perps stroll in the front door.

CUSTOMERS

Which would you likely do if your store account was compromised?

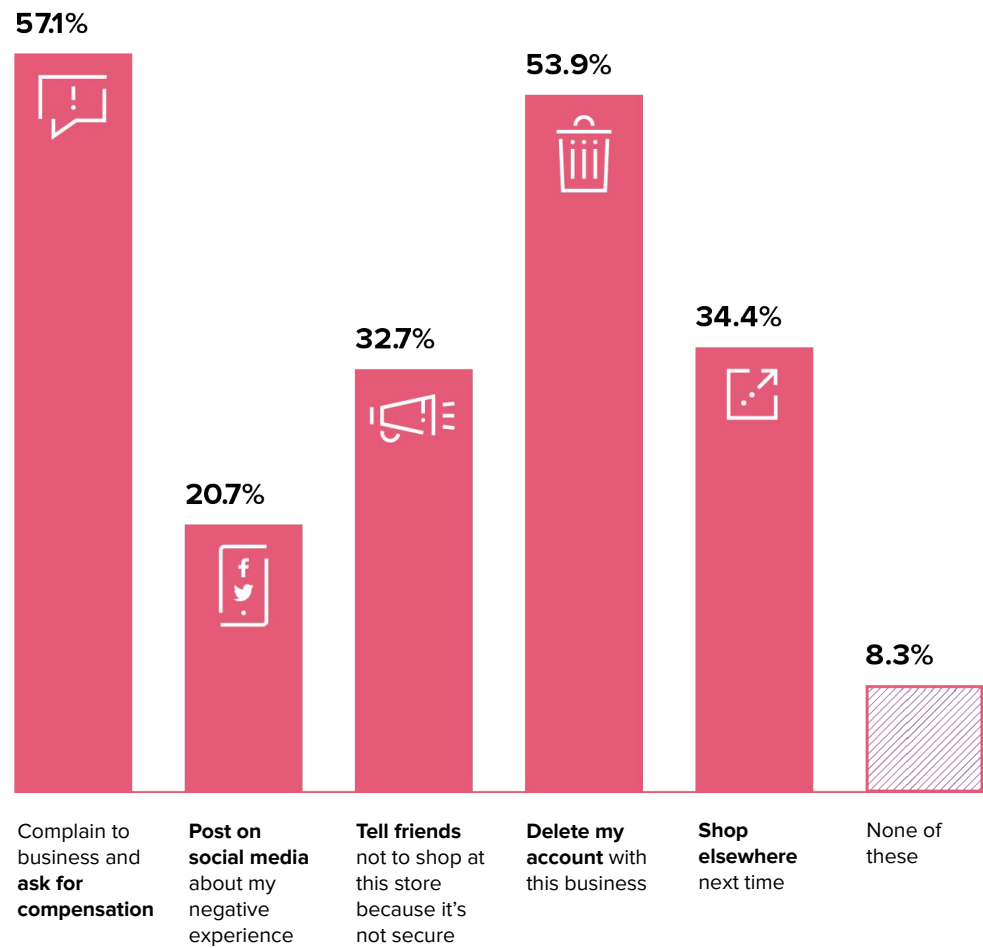


○ Source: Riskified's Account Security Survey

CUSTOMERS

How would having your online account compromised change how you would shop with that store?

○ Source: Riskified’s Account Security Survey





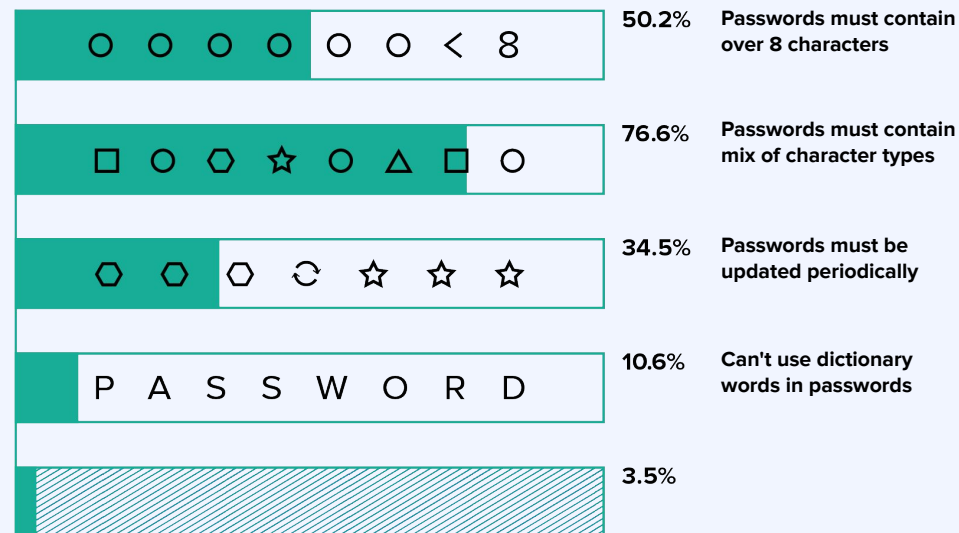
Passwords are a double-edged sword

Many merchants require that account passwords meet certain security guidelines. Indeed, long, complex passwords are more resistant to cracking attempts. But these guidelines can only protect against ATOs up to a point. Even though customers hold retailers entirely responsible in cases of account takeovers, customers themselves play a key role in securing the safety of their own accounts. Our survey showed that nearly half of customers use the same password for two or more online store accounts, leaving themselves vulnerable to credential stuffing.

Credential stuffing is effective because customers tend to reuse passwords. Much like our sugar intake, we know it's bad for us, but the temptation is simply too high.

MERCHANTS

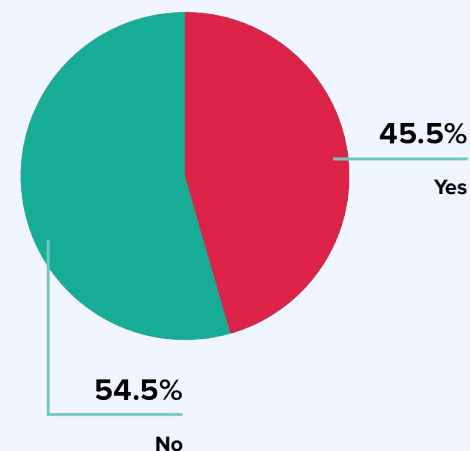
Which are password requirements for customers opening accounts at your store?



CUSTOMERS

Do you use the same password for two or more store accounts?

○ Source: Riskified's Account Security Survey





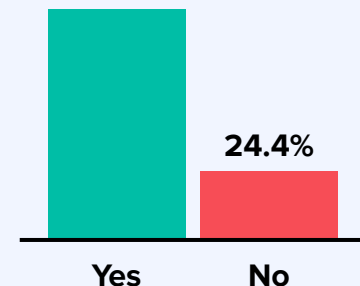
Fighting back: what are merchants doing, and how can they do more?

Merchants are taking measures to protect their customers' store accounts. More than 75% of the merchants we surveyed said they use at least one protection measure, from bot-detection technologies to two-factor login authentication and activity pattern review.

However, more than 82% of merchants saw up to 50% of their customers' accounts compromised in the past year, demonstrating that these measures are insufficient. Our analysts, who study cases where merchants use a standalone ATO solution in conjunction with our CNP fraud solution, detected a common theme: many solutions out there are only effective against one ATO modus, leaving accounts vulnerable to a variety of other attack tactics.

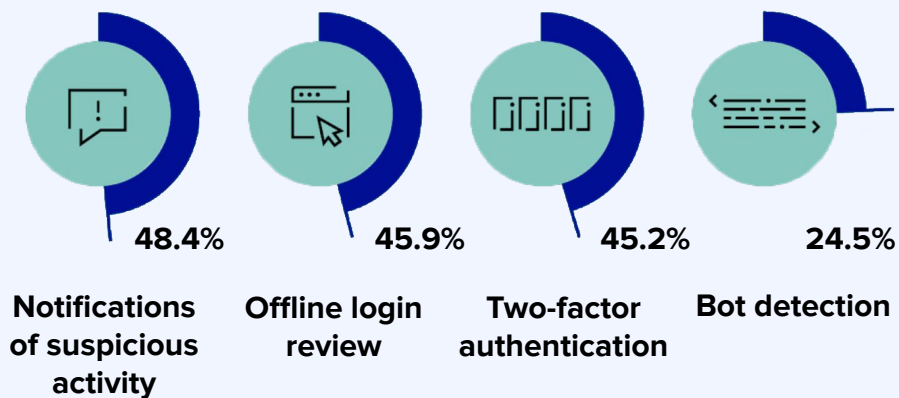
MERCHANTS

Are you taking any measures to protect customers' online accounts from ATO attacks?



MERCHANTS

What measures are you taking to protect customers' store accounts?



Source: Riskified's Account Security Survey

03

How to protect your store from ATO attacks

The fundamental challenge to stopping ATOs is clear: merchants do not have enough data to work with at the point of login. Comparing IP addresses and device fingerprints is nice, but not enough to make a reliable decision, because legitimate customers have an abundance of good reasons to login in from new devices and different parts of the world.

Not only is this a difficult call to make, it is also high-stakes. Be too soft and potentially enable an ATO that could cost you the lifetime value of a loyal customer. Be too strict, and you could end up denying access to good customers, sending them straight to the competition.

So what can merchants do? The most important thing to do is to obtain additional data points to aid in the decision.

There are a number of options. Here are some:



IP Geo delta



Transaction data



Browsing time before login



Spoofing detection



Password entry behavior



Sharing data with other merchants

01 IP Geo Delta

When it comes to IP comparison, merchants shouldn't simply ask if the login location has changed, but rather how different is it than usual? A repeat customer logging in from a location down the street from their usual address? Perhaps they are shopping from their neighborhood cafe. A customer suddenly logging in from the other hemisphere? A second look could be justifiable. For many merchants, most notably in the travel sector, customers logging in and making purchases as they travel internationally is very common practice.

02 Browsing time before login

A shopper's behavior can provide clues into the legitimacy of their activities. When people go online to shop, they usually browse for some time, typically logging in when it is time for them to complete their transaction. When fraudsters enter an online store, they typically attempt a login immediately to determine what they could gain from the account.

03 Password entry behavior

Most illegitimate users copy and paste login credentials, a practice that is rare among legitimate account owners.

04 Transaction data

Beyond a customer's past logins, a lot of insights can be gleaned from previous transactions. Where did they shop from and where did they ship the goods? This, for example, can help determine whether the IP at the login attempt matches, say, the shipping address or billing address from a previous transaction. This data could help tip the scale on an otherwise questionable-looking login attempt.

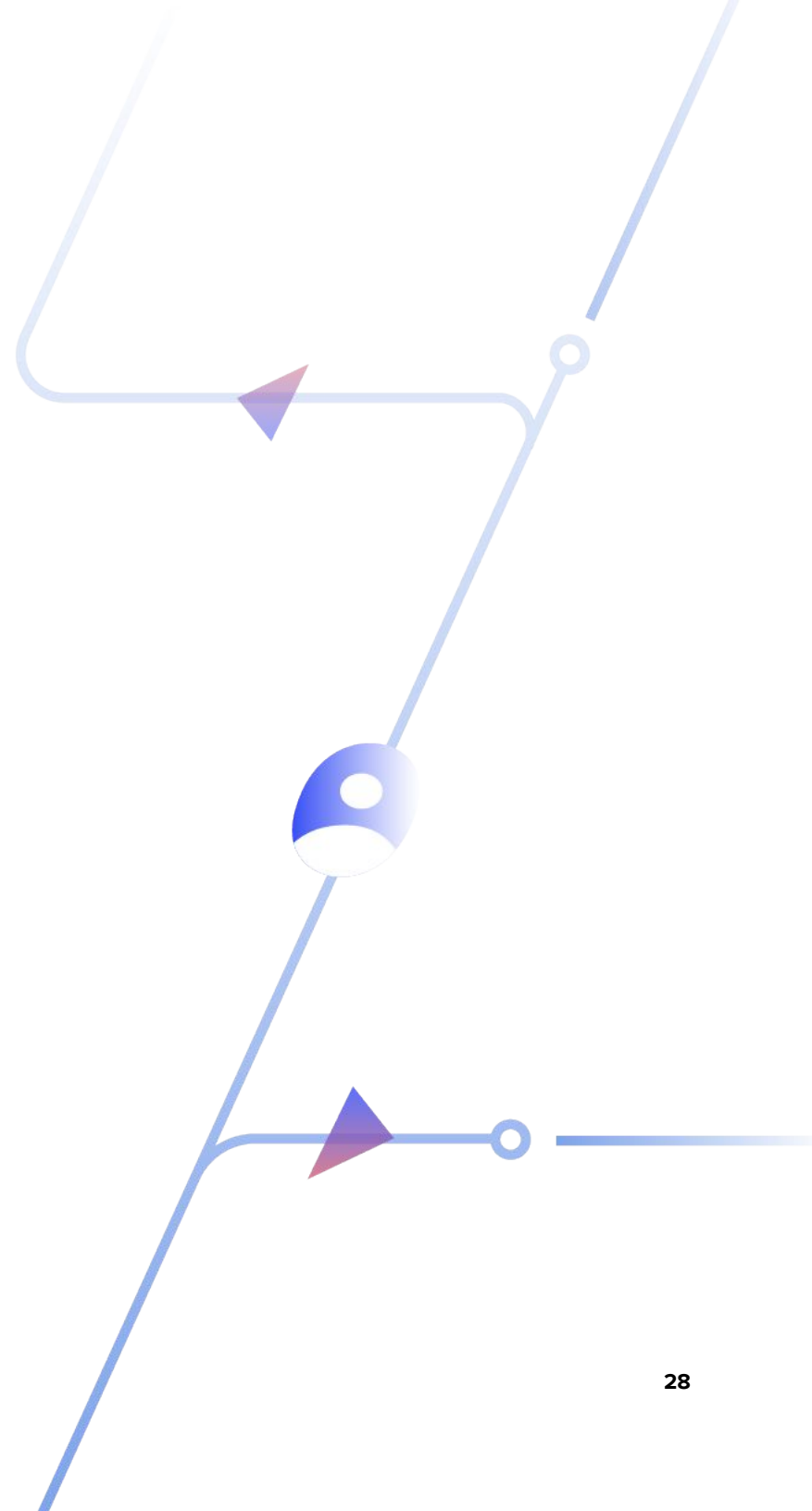


05 Spoofing detection

When fraudsters buy login credentials on the dark web, they often also buy information about the account owner's device: installed languages, time zone, and much more. They can then try and disguise themselves as the account owner's device. One of the powerful tools merchants can use is spoofing detection technology that indicates when a user is disguising their device.

06 Sharing data with other merchants

For merchants who partner with an ATO fraud solution, it is important to ensure that your provider aggregates data from different merchants. Strong data sharing networks can fill in the missing information you need and help you complete the narrative behind each login.



Conclusion

With the little extra effort it takes to obtain a set of login credentials, fraudsters can cause a lot more damage than standard CNP fraud. When store accounts are compromised, brand reputations are damaged, and merchants risk losing their most loyal customers. And these disastrous attacks are fast becoming the go-to fraud MO.

Many merchants believe they are taking action to protect their customers' data, but are they doing enough? Our survey shows that a lack of true understanding of the problem instills a false sense of security in many merchants.

A complex problem calls for a technologically-sophisticated approach. In the case of ATOs, merchants should ensure that their solution is using every available data point to keep accounts safe. These include IP geolocation and device fingerprinting, but also bot-detection, behavioral analysis, and drawing on a strong network of consumer data to inform their decisions.

More About Us

Merchants lose billions to underperforming legacy fraud solutions, payment failures and high-friction verification. Riskified uses powerful machine-learning algorithms to recognize good orders with a 100% guarantee against fraudulent chargebacks. We have an unparalleled ability to detect legitimate customers and keep them moving toward conversion. Merchants can safely approve more orders, expand internationally and ensure a seamless shopping journey without taking on new risk.

For more information, visit our [website](#) or contact us directly: at hello@riskified.com



About Riskified's ATO solution

Riskified's ATO prevention solution accurately identifies malicious login attempts, delivers actionable next steps, and minimizes friction for your customers. Our machine learning models, combined with digital fingerprinting and behavioral analytics, assess the risk of every login and resulting account event. We then provide a clear "allow," "block," or "verify" decision. When verification is required, our solution can deploy the identity challenge on the merchant's behalf.

By linking every account login and event to millions of previous shoppers and billions of transactions across Riskified's merchant network, our system differentiates legitimate customers from bad actors with a high level of confidence. Merchants who partner with Riskified benefit from best-in-class fraud detection technology and actionable decisions, and ensure that their good customers are never subjected to needless friction.

To consult about your organization's account security contact:

Alex Feldman, Product Manager, Customer Trust

alex.feldman@riskified.com

Ephraim Rinsky, PMM, Customer Trust

ephy.rinsky@riskified.com

Or sales@riskified.com



Written by

Amarelle Wenkert