ATO

Attacks and Sophistication On the Rise

FORTER®

INTRODUCTION

Stolen Data, Compromised Accounts

Over 900 data breaches led to the compromise of well over 3 billion data records in the first half of 2018. That's compared to 1.2 billion in the first half of 2017, indicating an increase of 72%. In recent years, attacks have consistently been on the rise and have affected a wide range of industries. The Breach Level Index notes that of all of the incidents reported in the first half of 2018, there were only 21 where encryption was used, providing at least partial protection. In almost all cases, the data was unencrypted and, therefore, easy for criminals to use.

Hackers used to target valuable financial information, such as credit card numbers. But now they've broadened their scope. Relatively few people use their Facebook accounts to store credit card information, for example, but many people use their social accounts to login elsewhere. Access to a Facebook account means smooth, legitimate-looking access far more widely. A criminal can often do more damage — or, from their perspective, gain more profit — with stolen account credentials than with stolen credit card information. There's also the danger of phishing, where customers are tricked into entering their data into a fake version of a site or app. **The realization that an account has more value than a stolen credit card has been one of the main contributors to rising account takeover (ATO).**

Our online accounts have become part of our online identities — which are, at this point, an inextricable part of our identities in the real world as well. That makes accounts appealing to those who are always looking for new vulnerabilities to exploit. It is no surprise then that account takeovers have been increasing in popularity with fraudsters in recent years. Forter's Fifth Fraud Attack Index found a 31% increase in ATOs year over year, and that is a trend that shows no signs of abating.

> "Our online accounts have become part of our online identities — which are, at this point, an inextricable part of our identities in the real world as well.

This white paper explores the developing trends in ATO, particularly in the realm of e-commerce, and looks at how companies can protect themselves and their customers from this pernicious avenue of attack.

1 ATO Across the Board

Data breaches have affected a variety of organizations, from retailers and medical facilities to government and financial institutions. A recent Forter survey found that 25% of respondents were aware that their accounts had been hacked into on a retailer's website. **The reason that account information is so valuable is that it can be an easy way to enter so many facets of our lives.** Many people reuse passwords, despite repeated advice to the contrary. That means that account information in one place can often be leveraged elsewhere. Additionally, so much information is shared publicly, particularly on social networks, that social engineering has become easier than ever before, enabling an attacker to present themselves convincingly as their victims.

Because many merchants do not have effective protection against ATO, fraudsters are often able to change or add account details once an account has been compromised, allowing for further exploitation. Many companies fail to analyze the behavior of users changing their email addresses. This allows fraudsters to cover their tracks without any trouble, ensuring that their victim does not receive notifications of whatever actions they take using the account.

And the more services a company provides — for example, if they have an enticing loyalty program, or provide a white-glove checkout service or pickup options for valued customers — the more tempting they are to a fraudster looking to cash in. The same qualities that make them appealing to good customers make them especially enticing for bad actors as well.

1 in 4

● ○ ○ ○

survey respondents were aware that their accounts had been hacked into

2 Profile of an ATO Fraudster

This leads to an interesting characteristic of ATO fraudsters. In most cases, a fraudster will attempt an attack, capitalize on it and repeat it if successful. Criminals are practical people running a business: it's all about ROI. With ATO, the ROI works differently. A fraudster who has found a particular site which provides account features that make it a lucrative target will keep attacking.

In fact, Forter found that **more than 80% of ATO attacks are carried out by less than 10% of fraudsters** attacking the site. A relatively small group (within the context of a site's attackers) is responsible for the overwhelming majority of ATO attacks. They specialize. If your system doesn't excel at identifying returning actors, even when they're trying to hide, it will be a challenge to stop ATO.

This tenacity means that criminals are especially likely to be looking for ways around whatever safeguards have been put in place. For example, T-Mobile recently reported an uptick in instances of illegal number porting. If a fraudster can get a victim's number moved temporarily to a device they control, then when your site uses multi-factor authentication to send an SMS to the device, the victim won't receive a notification. The criminal, of course, can then use the information in the SMS to access the account or accounts.

> "
> Fraudsters who focus on ATO attacks become extremely proficient at them, and can mount attacks at scale.

Fraudsters who focus on ATO attacks become extremely proficient at them, and can mount attacks at scale. For example, entering stolen account information can be done quickly and efficiently by bots and trawling for information to outwit security questions is easy when using social networks and searching for keywords. Similarly, the success of scams like number porting can be leveraged across multiple accounts. ATO protection must similarly work at scale, or fail to stem the tide of criminals who are expert and determined to succeed in this particular method of attack.

SPOTLIGHT

Fraud Rings

Accounts can be leveraged for gain in so many ways that ATO is particularly likely to be perpetrated by fraud rings. Criminals working together can maximize the number of hits they attempt, share vulnerabilities they've found, or parcel out jobs among themselves to combine different kinds of expertise. For example, one member of the ring might specialize in acquiring data, another in automation, another in social engineering research, and so on.

Fraud prevention systems must be extremely sensitive to connections between users in order to spot these fraud rings at work — even when those concerned are doing their best to conceal their real devices, locations, and intentions.

Forter's research indicates that fraud rings are often responsible for 20-30% of ATO attacks against a site. They're fast, efficient, and frequently sophisticated.

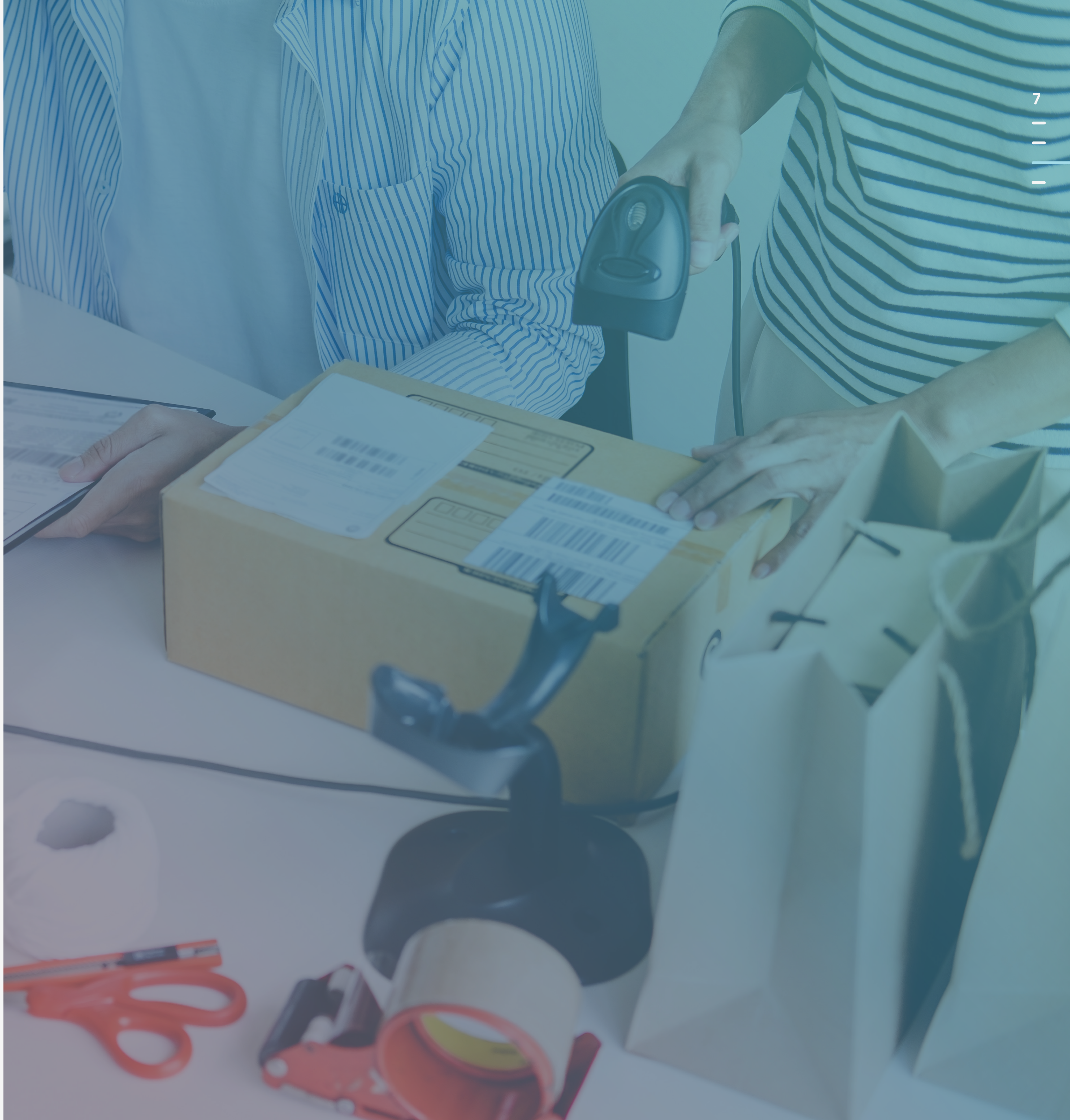
20% – 30%

of ATO attacks are by fraud rings

3 Methods of Monetization

Merchants have become aware of the increased dangers of ATO attacks in recent years, and guarding against losses from ATO have become part of the everyday job. However, the urgency of combating the risk itself, combined with the difficulties of adding new training necessary for manual reviewers, has meant that little analysis is generally performed on the nature of the attacks themselves.

“ATO” is typically used to refer to the type of attack where access is gained to an account in order to purchase items directly. This is an important and common form of ATO, but it is no longer the sole expression of account attacks, and for some businesses it is no longer even the primary form of attack. It is vital to understand the range of attacks and their natures in order to identify and guard against them.



SPOTLIGHT

Bots

The level of sophistication ATO fraudsters are willing to reach in order to exploit the benefits of hacked accounts makes these fraudsters especially likely to consider scaling their operations. In the most extreme cases, a fraudster (or sometimes a fraud ring) will write code to automate every step they need to take, streamlining and speeding up the process. They can automate everything from logging in, to changing the shipping or email address in an account, to purchasing goods or exploiting a loyalty program. Some highly sophisticated models even build in repeat visits to the account before purchase, acclimatizing the system to their presence.

Many fraud prevention systems are simply not able to identify this kind of sophisticated bot usage, making it harder to find and block these repeat attempts. That's a problem because fraudsters (or fraud rings) can perform more than 100 attacks per second.

100+
attacks per second

3 Ways Fraudsters Monetize E-Commerce ATO

CLASSIC ATO

This is what most people think of as ATO. The fraudster hacks into the account and uses the payment method attached to the account to make a purchase. In most cases the purchase will be sent to an address convenient to the fraudster, either directly to them or via a mule. The good reputation of the account will likely persuade most sites to either allow the purchase or be very careful before denying it, since no one wants to reject an order from a valued customer.

ADDED FINANCIALS ATO

This form of ATO is common but is discussed less often than the classic type of ATO. Here, the fraudster hacks into the account and adds new (stolen) financials which are then used to make purchases. This allows a criminal to leverage the reputation of accounts which do not have payment methods attached and can mean that the account is left open for exploitation for a relatively long period of time. Many sites do not have protections in place to identify fraudsters adding financials to an account.

LOYALTY ATO

This kind of ATO has emerged relatively recently and is gaining traction as companies build on their loyalty programs to attract valuable customers. Forter has observed a consistent pattern wherein merchants putting effort into improving their loyalty programs come under increased ATO attack — in some cases an increase as high as 200%. Customers are starting to feel it: a recent Forter survey **found that 22% of customers are aware that their loyalty points have been stolen at least once.**

Many loyalty programs allow customers to use their points for purchases, making them more and more compelling to fraudsters. Essentially, it's a form of free money for a criminal who has access to an account with points. Since customers rarely check their points in the way that they might check their bank balance or credit statements, this is an effective way to slip under the radar.

4 How to Block ATO

As ATO attacks continue to increase, merchants need to invest in identifying and stopping them. Failing to do so leaves them open to potentially serious losses, and also risks compromising precious customer trust.

Identification of ATO attacks must be performed with accuracy, however. It is tempting to respond to the threat by investigating any remotely suspicious activity, but such an approach is time-consuming for a fraud team and risks irritating and delaying good customers. Merchants should avoid adding friction to the shopping process out of a misguided attempt to protect accounts. As we have seen, multi-factor authentication such as SMS alerts is not foolproof, and rolling it out widely is likely to annoy your user base and make them less likely to complete a purchase. **In fact, according to a recent Forter survey, half of Americans agree they're less likely to buy something online if the entire checkout process takes longer than half a minute.**

The proliferation of false positives — good customers whose experience is negatively impacted by unnecessary extra checks or delays — is not ideal for a business. Wrongfully accusing a loyal customer of fraud could cause them to leave you for the competition. Accuracy, then, is the key. You need to be able to identify and block ATO attempts without disrupting the purchases made by good customers.

> Merchants should avoid adding friction to the shopping process out of a misguided attempt to protect accounts.

Evaluating the Entire Customer Journey

To achieve this, merchants need to stop focusing only on the point of transaction. This has traditionally been the part of a customer journey in which fraud teams were interested, since this is where monetary loss threatens. With ATO, on the other hand, looking at checkout already means you've missed the boat. You would be unaware of a fraudster who had been able to access the account for some time, exploring the victim's typical buying patterns and even changing details in the account. Fraudsters sometimes even visit an account a number of times to establish the legitimacy of their presence, making checkout easier when they attempt it. The inability to catch them early on allows an invasion of your customer's privacy which could cause you to to lose customer trust and makes financial loss at checkout more likely.

Customer journeys in today's world are often complex, made up of many visits with different purposes. One purchase might take five minutes to complete; another may be carried out over a period of days or weeks. A successful fraud system must analyze the entire customer journey in order to understand the behavioral patterns of each individual customer, and of your customer base as a whole.

Does the way this person is logging in match their typical login behavior? Do their product choices make sense with what we know about them? Is this one of the devices we have seen them use before? Are they exposing any hidden connections to fraudulent actors we've seen in the past?

All of this, and much more, needs to be answered during the customer journey, whether it ends in a purchase or not. And it needs occur in real-time.

Merchants need a system which can assess every action a user takes on their site and analyze it all within the context of their past behaviors and the behaviors of other customers, both good and bad. The system should be able to send decisions and notifications at any point in the customer journey, alerting retailers to ATO as soon as it has been identified, and protecting the account accordingly. Additionally, a system must constantly evaluate all of the activity on a site and watch out for the development of new trends in behavior between accounts which might be legitimate — or might not. For this to occur it is necessary to be able to identify connections between accounts and users, even when effort has been made to conceal any relationship and no overt data points are shared.

It's time to face up to the fact that ATO is not only increasing, but increasing in reach, impacting your user ecosystem long before the point of transaction. Merchants must protect their sites, their business, and their customers from exploitation by criminals who are becoming more sophisticated all the time.

"

A successful fraud system must analyze the entire customer journey in order to understand the behavioral patterns of each individual customer, and of your customer base as a whole.

About FORTER®

Forter is the leading e-commerce fraud prevention company that protects merchants during each stage of the customer lifecycle. The company's identity-based fraud prevention solution detects instances of fraud beyond the point of transaction in real-time, such as during attempts at account takeover and return abuse.

A team of world-class analysts constantly research new fraud trends and update Forter's machine learning solutions with cutting-edge insights, ensuring the proprietary algorithms adapt to the latest fraud strategies in real-time. As a result, Forter is trusted by Fortune 100 companies, online travel businesses, and fast-growing digital disrupters to deliver exceptional accuracy, a smoother user experience, and elevated sales at a much lower cost.

Where ATO attacks are referred to in this white paper, this reflects attempts at ATO and not successful ATO attacks.

Visit www.forter.com