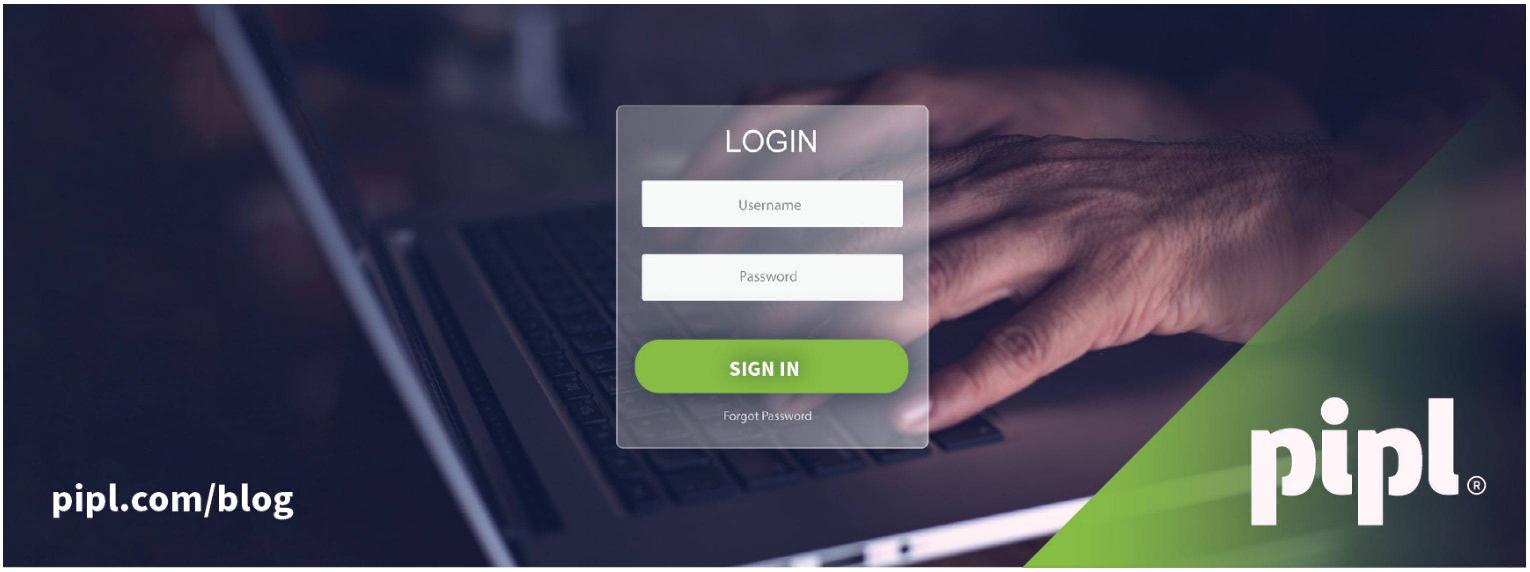

ATO: How Fraudsters Leverage Established Accounts to Commit Fraud

Editor's Note: This guest blog post is written by Alexander Hall, principal at Dispute Defense Consulting and a reformed fraudster.

The number of methods employed by fraudsters is indefinite and grows with each passing day. Credit card fraud leveraging dark web marketplaces, identity theft, phishing, generated card numbers, fraudulent checks, etc. Here, I'll explain the method known as account takeover (ATO), and what merchants can do to defend themselves against several iterations.

What Is ATO?

An account takeover is when cybercriminals use an established account that's been accessed by an unauthorized user. Typically this is done with the intention of committing fraud, and there's a variety of ways ATO happens.

Different industries offer perks to account holders in different ways. The value of these offerings is what fraudsters are after. Once an ATO exploit has proven successful, the method becomes a standard operation for identity criminals until it no longer works.

How Is It Done?

There are many ways for an account to be taken over. A few examples are:

Stealing Username/Password Combinations

In 2021, a hacker forum released a batch list of more than 3.2 billion stolen credentials (dubbed the Compilation of Many Breaches) that included data from companies such as Netflix, Linked In and others. Smaller lists have been in circulation for well over a decade now and such lists are commonly found for sale on dark web forum sites. This method is the least demanding and least successful, due in large part to the mass adoption of reset codes being sent to verified email addresses and phone numbers. This is where Phishing and SMShing come into play …

Phishing/SMShing

This method is intended to intercept a reset code, two-factor authentication (2FA) code or link for a password reset. When fraudsters are attempting an ATO for an account with stolen login credentials on a device unrecognized by the site/app/etc., a notification will be sent to the account holder via verified contact information. This is typically in the form of an email or a text to a registered device. The fraudster anticipates this, contacts the victim and employs social engineering tactics to access the link or code in order to gain access to the account.

Building a Minimum-Requirement Profile Via Social Engineering

Minimizing friction for customers has become more and more important over the past few years, and fraudsters know this. By building profiles and contacting the customer service teams of the companies the victims engage with, fraudsters are able to submit requests to make changes to accounts after successfully navigating the verification challenges. Updating contact information by claiming a stolen phone, adding authorized users and sending out replacement cards (which are to be pirated from mailboxes) are all examples of what can be done using this method. Next, I'll cover a few examples of what can be done once an account is taken over.

How Do Fraudsters Use a Compromised Account?

When pondering how a fraudster might leverage a stolen account: Depending on the success of the ATO (and the restrictions for an account following updated information) the fraudster can do anything that an authorized user can. If an authorized user can make large purchases on a billing cycle or deferred payment, so can the fraudster who accessed the account illegally. If an authorized user can rent a car, so can that fraudster. If an authorized user can enter a secondary phone number for verification purposes in the future, the fraudster now has that same power.

Successful fraudsters play both long and short games. They may use several quick turnover methods today, while working on chipping away at various systems over time to make an exploit work for a large profit. Additionally, effective fraudsters understand the value of escalations and combining several methods to remain undetected and still get what they seek.

Here are five methods centered around a successful ATO.

1. Hijack an account and use stored payment information to place orders

This is the most common example of ATO fraud. The fraudster logs into an account and places an order, using the stored payment info. Third-party payment apps are vulnerable along with merchants who do not hide the payment information from the user or do not verify with biometrics or security codes.

2. Hijack an account and use stolen information to place orders

This method is a combination of two methods. The first is buying stolen payment information. The second is the ATO. By leveraging a good payment history of the account, the fraudster then associates new (stolen) payment information with the intention of bypassing any escalations.

3. Hijack an account and associate an authorized user to a credit/debit card

This method applies to issuers, banks, fintech, credit unions, merchants with in-store credit cards and more. This method also requires more preparation by the fraudster. In order to access an account, any or all of the methods mentioned above would need to be used in unison. If successful, it results in the ability for the fraudster to associate a new address (business accounts are most vulnerable for this) and add an authorized user and secondary or replacement card.

4. Spend loyalty points/miles

With the spike in flight cancellations, hotel cancellations, etc. we've seen during the pandemic, and the resulting refunds being issued in credit/miles/points/etc., fraudsters have been working to capitalize on the large amounts of stored value in accounts associated with travel, hospitality and related industries.

5. Buy Now, Pay Later (BNPL)

Buy now, pay later isn't necessarily new. The system is essentially a credit line with more back-end processing and less liability for the merchant. Fraudsters that leverage identity can make it through the verification process of a merchant and use stolen information (or none at all) during the agreement with the BNPL service provider.

How Can Companies Identify ATOs in a System?

The most effective way to identify ATO attempts and successful ATO account conditioning is leveraging personal identifiable information (PII) data. In order to see why, it is important to understand what this set of information may have with it compared to other sets of information.

Let's take a look at a simple ATO attempt. This fraudster uses stolen login credentials to log into an account with the intent of using stored payment information to enact a transaction on the site or app.

To the fraudster, the process looks like this:

1. Access the Site/Application

When the fraudster first lands on the website or loads the app, device fingerprinting and IP geolocation can be used to begin identifying who is interacting with the site. Through the use of VPNs, proxies and other tech, the IP address might not represent where the fraudster is accessing the site. However, these data points can be used to check against the same data points of the authorized user. At this point, we do not know which account to associate these data points with, so we're just observing for now.

Next, we will simulate that the targeted system doesn't employ 2FA of any kind, and that the fraudster has illegally bought accurate login information for the account.

2. Successful Login

The fraudster successfully logs into the account by using the stolen login information. Ah! Now we have an account to cross reference.

Has this IP address or this device MAC address been used with this account before?

3. Build a Cart

As the fraudster navigates the site, they begin to build the cart and are providing more data, which support "behavioral analytics." Things like filtering by most expensive or targeting items with high resale value are indicators to watch for.

4. Checkout

Now the fraudster has built their cart and is ready to checkout. Unless they have proximal access to the shipping address used for previous orders and have someone that they can send to intercept the package, they will need to input a shipping address that hasn't been seen on this account before.

They input the new shipping address and complete checkout.

Now, the Prevention Strategy

From the moment this user interacts with the website or app, their IP address can be leveraged. The goal isn't to identify them as a fraudster, yet. The goal is to identify whether or not their access is suspicious. Once they log into the site, we now can see in the data that this account is being accessed by an IP (or device) that hasn't been seen before. This is the first red flag.

The second red flag comes in the form of their behavior and the contents of their cart. Obvious flags might include loading a cart quickly with expensive items or with items that are easily resold. For this step, leverage historical orders to see if these habits fit the spending habits of the account.

The nail in the coffin comes in the form of associating a new shipping address. On its own, this might not seem like a big deal. But remember that not only has the account been accessed by a new device, the items being purchased are suspicious when contrasted with past orders, and the items are also being sent to a new shipping address.

What's great about this approach is its simplicity. All of the information being leveraged in this strategy comes from the effective use of PII and historical in-house data. Think about ways your company can include these techniques in its fraud defenses and make any ATO attempts DOA.

In a world where everything's already been hacked, traditional fraud-prevention methods aren't enough anymore.

Merchants need a proactive, end-to-end strategy for account takeover defense.

Learn how our identity trust solutions can help.