Account Takeover: A U.S. Payments Forum Resource Brief

Introduction

Account Takeover (ATO)[1] is a type of fraud that occurs when a bad actor, or fraudster, gains control of a legitimate account. This could be any kind of account, from email accounts to an account on a merchant website to a bank or credit card account. Gaining control of a legitimate account depends on getting access to account holder information. Data breaches, phishing[2], and malware[3] are all means for getting such access.

One difficulty in combating **account takeover fraud** is detecting that it has occurred. Fraudsters are constantly looking for ways to take control of accounts without alerting the true account owner or the organization where the account resides that they now have access. In some cases, unauthorized access to or use of the account is obtained by a relative, employee, or other individual associated with the account holder without the account holder's knowledge or permission. This paper aims to provide guidance on how fraudsters gain access to accounts, typical behaviors to watch for, and preventative measures that can be taken to avoid **account takeover fraud**.

The Nature of Account Takeover

When organizations think about fraud in payments, the focus is typically at the transactional level. For many years, counterfeit and lost/stolen fraud have been a major source of fraud in the payments industry. When a transaction occurs on a counterfeit or stolen card, networks and issuers have techniques in place to identify and flag it as fraud and in many cases can take reactive measures such as deactivating the card, essentially removing the fraudster's ability to continue committing fraud.

[1] https://www.proofpoint.com/us/threat-reference/account-takeover-fraud#:~:text=Account%20takeover%20fraud%2C%20also%20known,control%20of%20a%20legitimate%20account.

[2] https://en.wikipedia.org/wiki/Phishing

[3] https://en.wikipedia.org/wiki/Malware

Account takeover fraud, however, can be difficult to detect as it does not occur at the transaction level but happens initially at the account level. Fraudsters eventually perform transactions, account transfers, or other actions on accounts that have been compromised. However, initially many fraudsters took steps to avoid detection by performing changes to the account such as altering contact information. If done correctly, activities on the account will appear legitimate while being controlled by an unauthorized individual. This is one aspect of account takeover that fraudsters find particularly attractive.

Phases of Account Takeover

To understand how account takeover occurs, it may be helpful to break it down into three phases: data gathering, account modification, and impacts.

Data gathering

Prior to taking over an account, fraudsters will need to gather or purchase information that can be utilized to gain access to or take control of accounts as if they were the actual account owners. Data sourced through multiple means can often be purchased with a relatively low barrier to entry, and can be used to attempt takeover of numerous accounts simultaneously, often through automated means. Here is a short (but not exhaustive) list of common methods used:

- Data Breach: A data breach occurs when sensitive information is exposed to unauthorized users in error or is accessed through nefarious means. This often occurs when there are gaps in an organization's security assessments or when software vulnerabilities are left unpatched. In some cases, social engineering is used to gain access to a network (see social engineering below). Data breaches are a desirable source of data for fraudsters as they can often gain access to consumer accounts using this method. Types of data usually targeted in a data breach include personal identifiable information (PII), usernames, passwords, email addresses, and financial account and/or card account information.
- Social Engineering: Social engineering is a technique used by fraudsters to mislead an individual or organization into believing they are someone or represent someone who they are not. This is often accomplished by performing phishing schemes involving SMS, phone call, and email methods, as well as other forms of spoofing someone's identity.

Account Testing and Modification

Once a set of possible credential matches have been collected, fraudsters will often employ automated or human means to test combinations until successful matches are discovered. Once discovered, the fraudster is ready to target certain aspects of the accounts.

After a fraudster has gained access, they often take additional measures before fully utilizing the account in an attempt to reduce the likelihood of being discovered. This typically involves changing key pieces of data pertaining to the true account holder, such as physical address, mailing address, email address, and phone number. Once the fraudster has modified the account to the point they feel comfortable attempting to further leverage the account without being discovered, they may move forward with utilizing the account as if they were the true owner.

Impacts of Account Takeover

The actions a fraudster takes often depend on the type of account compromised. Certain account types lend themselves to certain fraud campaigns more than others.

- Account takeover can potentially result in the loss of the following:
  - Reputation
  - Goods
  - Money
  - Future Orders
  - Other losses

Identifying ATO

Regardless of where the takeover is occurring, whether at the merchant level, credit card account level, etc., it is often extremely difficult to detect. While it is important to monitor for red flags, such as multiple pieces of personal information being changed at once, fraudsters may make subtle changes over time in order to prevent the takeover from being as noticeable. Another challenge for businesses is the balance of customer experience vs. preventing fraudulent activity; therefore, it is important to develop internal strategies to ensure that the actual account holder is the one requesting the changes.

Prevention and Mitigation

While this brief has highlighted that detecting account takeover fraud can be difficult, there are ways to help mitigate its effects should it occur for an organization. If followed, the below best practices should help with prevention and mitigation.

- Prevention of data loss for organizations:
  Protecting customer and account related data is central to preventing ATO fraud. Fraud actors rely heavily upon the discovery of mass exposed or breached account details. Following industry standards as well as staying up to date with current practices reduces the risk of data loss.

- Identification of transaction patterns:
  When successful, account takeover typically results in a series of transactions (payment or data-based) that do not fit with expected patterns for a given customer. It is strongly recommended that baseline patterns are established, monitored, and updated to ensure that out of pattern transactions are more readily identifiable. Such transactions can then be examined and appropriate actions can be taken.

- Login pattern monitoring:
  The way in which a user logs in to their account is typically predictable and can be tied to a combination of data points, for example, device, IP, geography, frequency, time of day, and certain behaviors that can be tracked and established as a normal pattern for a user. When a fraud actor is attempting a takeover, the login patterns rarely align with expected patterns for a given user.

  It is important to note that should a login be successful and fall out of expected patterns, it is recommended that the account owner is notified of the login, provided some identifying details such as location, device, and time, and is given the option to flag as potentially fraudulent activity should the login be unrecognized by the user. Organizations may want to consider implementing additional verification requirements for questionable login activity.

Prevention and Mitigation Toolbox

The list below should serve as basic guidance on tools and techniques that may help in preventing and mitigating the effects of ATO fraud. It should be noted that the list is not exhaustive but represents common approaches that can serve as a starting point.

- Behavioral Analytics:
  - Monitoring the typical behavior (i.e. login velocity, transaction pattern, etc.) of account users allows for anomalous activity to be detected and mitigated quicker.
- Two Factor Authentication:
  - Requiring a secondary login credential (e.g. One Time Passcode) adds an additional layer of security and makes it more difficult for fraudsters to gain access at the login phase of an account or during first time set up of a device.
- Account Monitoring:
  - Monitoring activity taking place on a given account including login methods and related data, changes to account holder information, and actions atypical for a given user enables organizations to more easily detect if an account has been compromised.
- Consumer Device / Mobile Device Authentication:
  - Leveraging authentication techniques native to the user's device for the account login process (i.e., device passcode, fingerprint, and "Face ID") allows for a built-in layer of security in the two factor authentication.

- Account Information Reset Confirmation:
    - For example, when an account has contact information reset, an automated email confirmation should be sent to the older contact information (i.e. email reset sends confirmation to the old email address).

Conclusion

Account Take Over (ATO) is an eminent problem that has spread across industries and impacts customers at all levels. Having control over your account during the customer experience is expected and when a fraudster can receive control of a customer's account, they can do serious damage. The fraudster's ability to manipulate the account details and make fraudulent purchases will damage the customer's experience at that retailer, jeopardize their PII, and potentially cause financial loss in the process. Big box retailers, fast food chains, and energy companies are just a few of the many industries that have had targeted ATO campaigns against them. It is impossible to avoid ATO completely, but there are ways for your company to respond, prevent, and mitigate the risk, whether it is utilizing a third-party solution or developing in-house monitoring through transaction patterns to effectively combat ATO.

Developing a balanced relationship between a frictionless and secure customer experience is a top priority. Enabling the necessary policy and security rules to prevent fraudsters is needed to combat ATO and other threats to customers. As the industry plays the game of cat and mouse with various fraudsters on ATO, it is important to note that each time a new mitigation technique emerges, organization should review not only through the lens of security but policy as well. These changes will help make the customers safer and reduce risk for any potential parties involved.

About this Brief

The U.S Payments Forum Payments Fraud Working Committee is publishing an ongoing series of short summaries and primers on trending topics related to fraud in the industry. Account takeover fraud is the second publication in this series.