Best Practices in Account Takeover

July 2013
# Table of Contents

Introduction 3

Account Takeover is Painful 4

Differences between Account Takeover and Account Compromise 4

Why Account Compromise Solutions Don’t Always Stop Account Takeover 5

What Does the Future Hold? 6

Account Takeover Requires a Comprehensive Solution 7

Why Industry Leading Organizations Use ID Score Account Takeover to Combat ATO 7

Conclusion 8
Introduction

A consumer’s email address, phone number and home address associated with their credit card account just changed in your processing system. Did the consumer initiate the request or did a criminal just take over their account?

Unfortunately, your organization may be the last to know. In the 2012 “Faces of Fraud” Survey conducted by Information Security Media Group, in 82% of cases involving identity fraud, the consumer uncovered the theft before the company. Not surprisingly, 26% of organizations surveyed reported losing consumers to competitors following a fraud incident.

In a 2011 study conducted by the Ponemon Institute, 56% of businesses reported experiencing fraud in the last 12 months, with 75% of those victims reporting account takeover fraud.

Account takeover fraud is not isolated to a single industry. The potential for account takeover exists whenever a company allows consumers to establish accounts that store any information of value. Account takeover can involve virtually any type of account including government benefit accounts, wireless phone contracts, checking, credit card, and e-commerce accounts.

This paper identifies gaps in the use of traditional controls currently employed to prevent account takeover fraud. It offers an alternative to access-focused solutions by discussing the benefits of a multi-channel, cross-industry solution focused on analyzing account management activities for indications of account takeover fraud.
Account Takeover is Painful

In an account takeover scheme, the fraudster uses data they have in their possession to take control of an account away from the legitimate account-holder for purposes of carrying out unauthorized transactions. While account takeover can take place via all channels, including face-to-face, the majority of account takeover attempts target the online and call-center channels.

In financial services, an account takeover scheme may involve a fraudster assuming control of a customer’s credit card account by adding themselves as an authorized user and immediately spending the remaining credit available. In eCommerce, cybercriminals may assume control of a consumer’s account, order physical goods using the debit card number on file, ship to an alternate address, and subsequently sell the stolen goods on another website and pocket the proceeds.

Fraudsters move quickly and often use the data gathered from one account takeover scheme or data breach to take over additional accounts at other companies. Even worse, criminals often collaborate and sell compromised identities to the highest bidder, resulting in further damage to the consumer’s account and identity.

In the aftermath of an account takeover scheme, the victim feels violated. Fair or not, consumers often view the organization that allowed the fraudster access to their account to be at fault. The loss of privacy and most importantly, control of their accounts is often too much to bear. Many account-holders will move their business to a competitor despite the best efforts by the company to repair the damage. Trust is intangible, but it is obvious when it has been lost.

Differences between Account Takeover and Account Compromise

Account takeover (a.k.a., account hijacking) is often described as synonymous with account compromise, but they are in fact, very different ways of committing fraud and violating a customer’s privacy.

While related to the account takeover problem, account compromise is a fraud scheme that focuses on obtaining access, as opposed to control, of an account through the online channel. Typically, account compromise, or “hacking”, occurs when a fraudster has obtained an account-holder’s login credentials and is able to access the account online. There are a multitude of technological resources devoted to addressing the many different ways that a person’s online account is subject to compromise, however many of these solutions target online threats.

An example involving “family fraud” illustrates the differences between account compromise and account takeover: John Doe Jr. lives with John Doe Sr. Jr. decides to log into Sr.’s checking account using Sr.’s computer and legitimate credentials (obtained surreptitiously).

Nothing appears out of the ordinary to the bank as it previously authenticated Sr.’s device, and the login credentials are legitimate. Consequently, there are no red flags associated with the account activity.

Jr. decides to change the email address on the account to his own, suppresses paper statements and requests electronic statements instead. He subsequently writes an unauthorized check to himself for $10,000.

The act of logging into John Doe Sr.’s account illegitimately represents account compromise whereas the subsequent actions by John Doe Jr. to suppress paper statements etc., signifies the act of account takeover.

Access-focused solutions looking to thwart malware or other sophisticated account compromise schemes would be ineffective in the example illustrated above.
Why Account Compromise Solutions Don’t Always Stop Account Takeover

Given the inherent differences between account takeover and account compromise, fraud detection tools typically cannot address both types of fraud. The following overview of traditional fraud detection and prevention tools details their inherent strengths and weaknesses, and consequently their ability to detect account takeover related activity.

Device Recognition

Companies with an online self-service channel often use device authentication solutions to compare a laptop, desktop or mobile phone’s electronic signature to a database of devices previously associated with online fraud.

In the event that the device matches a previously identified device with a negative history, the company can deny the transaction, challenge the user with a quiz, or flag the login for additional review. However, device recognition only works for online transactions and may not flag a device that is “clean” with no previous connections to online fraud. In the case of “family fraud”, where the fraudster has access to their family member’s internet-banking apparatus, device recognition has limitations in detecting fraudulent behavior.

Malware Recognition

Malware detection is another tool that attempts to prevent account compromise as well as account takeover fraud. In theory, devices attempting to log into an account are examined for the presence of malware which might indicate remote control of the device by criminals. However, malware prevention and virus detection solutions have a limited shelf-life as providers are in a never-ending race with cybercriminals to combat the latest threats.

Malware is most effective when the virus appears and is shared amongst members of the public. Distributing best practices and insights into emerging threats is a critical component of reacting to malware innovation. Malware detection will always play an important role in mitigating account compromise risk, but should be used in conjunction with other solutions.

Voice Recognition

Companies who offer account management services through call-centers are increasingly utilizing voice recognition solutions to assess the legitimacy of the caller. Voice recognition software attempts to study the conversation for signs of deceit as well as determine a match to a previously captured sample of the consumer’s voice.

Voice recognition software is an innovative and emerging way to mitigate call-center fraud. In most cases, it requires integration with a more comprehensive suite of fraud solutions. While these solutions can be effective on their own, companies often spend considerable resources to integrate them into the enterprise’s risk controls.

Another drawback to voice-based fraud solutions is that – much like device recognition – it applies to a single channel (e.g., call center, online). In addition, the solution focuses on preventing access to an account rather than evaluating account changes. Risk managers cannot ignore the value generated via voice recognition technology, but they will need to weigh investments required to integrate these solutions with the expected benefits.
Knowledge-Based Recognition

Knowledge-based authentication (KBA) requires consumers to provide answers to questions that, theoretically, only the actual customer knows the answers to, and is again focused on restricting unauthorized account access.

Unfortunately, criminals often use social media sites such as Twitter, Facebook or LinkedIn to gather “secret” data that they can use to access the consumer’s accounts. Similarly, public records-based quizzes are susceptible to the dedicated fraudster willing to do a little research.

With each additional layer of invasive security, consumers are more susceptible to frustration and likely to avoid self-service offerings. Risk managers are well aware of the limitations of KBA solutions, but the popularity of quizzes has far outpaced their effectiveness as a single form of consumer authentication.

Anomaly Recognition

Anomaly detection is a powerful way to use real-time analytics to detect potential account takeover activity. There are numerous anomaly detection solutions that target account takeover fraud. In general, anomaly detection software attempts to detect unusual activity in a sea of apparently “normal” transactions.

Anomaly detection solutions typically utilize sophisticated analytical techniques to establish a baseline of behavior for a customer, or a set of customers. The solution then compares the activities of an account-holder to that baseline for the purposes of detecting high-risk and suspicious activity. If the activity appears inconsistent, depending on the tolerances established by the software provider and/or the company, the system flags the activity for additional review. Anomaly detection solutions often focus on account takeover within and across different business units as an enterprise offering.

These solutions are often installed into the client’s environment and require a significant amount of integration and customization. However, the result of the customization is a solution that is optimized to the client’s risk tolerances and resources. In addition, much of the risk-mitigating value of these solutions occurs behind the scenes, creating very little friction for customers.

Some of the limitations of an installed anomaly detection solution include the lack of a cross-organization and cross-industry approach where a client can compare the consumer’s activity with other companies to the activity being tracked at the client. Even if the technology allows for cross-company comparisons, much of the information used in anomaly detection solutions is rendered anonymous, making it more difficult to track the same consumer across clients.

What Does the Future Hold?

Account takeover is expected to continue to grow due to increasingly frequent, massive data breaches, the proliferation of online “black markets” to trade illicit, private data, and the ever-increasing self-service options offered by companies to allow for convenient account management activities. In addition, the sophistication of malware continues to outpace the public’s ability to adopt effective defenses.

Moreover, the increased adoption of Europay, MasterCard and Visa (EMV, targeted for August, 2014) technologies intended to thwart card present fraud at point-of-sale is expected to actually accelerate the migration of fraud activities towards exploiting weaknesses associated with a company’s self-service offerings. With more fraudsters determined to commit account takeover, and a growing availability of sensitive data to perpetrate the crime, leading organizations are already looking for ways to shore up the gaps in their account takeover defenses.
Account Takeover Requires a Comprehensive Solution

Today, risk managers are cobbling together account takeover solutions by threat, by customer-care channel and by business area. Device recognition, virus detection and KBA quizzes can all play a role in preventing fraud, but none of these solutions can single-handedly prevent account takeover.

Combating account takeover starts with preventing unauthorized account access and subsequent malicious account changes. If access controls are defeated, however, the methods detailed above are limited in their ability to prevent unauthorized changes to account profile data. For that, companies must adopt a new approach.

Why Industry Leading Organizations Use ID Score Account Takeover to Combat ATO

What happens when the fraudster passes the authentication process and gains access to an account? What does account takeover activity “look” like and how do companies flag such activity effectively, in real-time, before losses occur?

An enterprise approach to combating account takeover fraud requires a comprehensive, real-time understanding of normal and abnormal account maintenance activity across the organization’s channels and product areas. Activities that carry a high-risk of account takeover fraud, such as changing the email and mailing address associated with an account, take place millions of times a day. How can companies stay ahead of fraudsters while minimizing customer friction on the millions of benign account management activities that occur daily?

ID Analytics designed ID Score® Account Takeover (IDS-ATO) to provide organizations with exactly this solution—an enterprise risk score focused on assessing the legitimacy of requested account changes through real-time, cross-industry data.

IDS-ATO assesses a requested account change in several ways, including:

- Has the account holder made similar changes at other organizations?
- Holistically, does the full set of requested account changes match a pattern of account takeover?
- For PII changes, does the new information being added to the account (ex. new address or phone) have a history of high risk behavior?
- For PII changes, does the comparison of old and new information reveal a high-risk behavior?
The IDS-ATO solution’s unique ability to accurately make these assessments comes from the rich and insightful data in the proprietary ID Network™ – one of the nation’s largest networks of cross-industry consumer behavioral data repository of identity information containing over 2 billion historic consumer events and over 3.3 million confirmed frauds. These events, such as credit applications and transactions, are sourced from a wide range of industries and updated in real-time, providing IDS-ATO with a comprehensive, up-to-the-minute view into the risk associated with a requested account change.

Unlike most prominent Account Compromise solutions, IDS-ATO is an enterprise solution, capable of analyzing consumer behavior across every channel in the organization. For example, if a consumer added him or herself as an authorized user online, and then called the bank to change the address and request a new card, IDS-ATO will observe and assess all of the cross-channel behaviors to deliver a score which accurately depicts the risk associated with the activity. Based on that score, the company can decide to approve the changes to the consumer’s record, or subject the account to additional manual review.

Since IDS-ATO focuses on changes made to the account itself, the solution complements the types of authentication and account compromise solutions mentioned above. There is no other solution leveraging a cross-industry, identity-based network of data to manage account takeover risk. Perhaps most importantly, the solution is flexible, able to accurately evaluate the risk level of any account management event for any account in any industry in the United States.
Conclusion

While today’s risk managers don’t lack for options in addressing account takeover, all too often these options focus strictly on restricting account access, are restricted by channel, and lack a cross-organization and cross-industry perspective. ID Analytics’ IDS-ATO solution is the only source of cross-industry PII-based insight into the fraud risk associated with changes to an existing account. In real-time, companies receive a three-digit risk-based score conveying the account takeover risk related to an account maintenance activity. This in turn allows the organization to automate approval of low risk account maintenance requests, reducing customer friction and operational expenses, while segregating high-risk accounts for additional review or scrutiny.

Given the damage that account takeover fraud can cause, and the likelihood these problems will continue to grow, investing in a targeted solution makes sense, especially one which can demonstrate a quick return on investment by avoiding losses associated with fraud and preventable customer attrition.

How do you evaluate whether ID Score Account Takeover is right for your organization? To discuss a complimentary evaluation test, contact ID Analytics today at 858-312-6200 or sales@idanalytics.com.

ID Analytics’ solutions protect you and your clients

Partner with an experienced, trusted firm. Since 2002, ID Analytics has been delivering a unique perspective of risk based on proprietary Advanced Analytics and the ID Network®, the nation’s only real-time, cross-industry compilation of identity information, data not available in consumer credit reports. For more information about ID Analytics contact us at marketinginfo@idanalytics.com or 866-248-7344 or visit www.idanalytics.com/solutions/enterprise.

ID Analytics is a registered trademark of ID Analytics, Inc. All other trademarks and registered trademarks are the property of their respective holders.