DATAVISOR

The Dummy Handbook on ACCOUNT PROTECTION

Online accounts used to be just for identifying email users and granting them access to their inboxes, but nowadays they have become such an integral part of modern life that it is hard to think about a world without them. Today, the average person is said to have more than 100 online accounts that unlock access to a plethora of services, including social media, ecommerce sites, news subscriptions, ridesharing services, cloud storage, financial services, and an ever-expanding et cetera.

The fact that virtually every online service requires the creation and use of an account or profile by each of its customers makes account protection a priority for modern financial institutions and ecommerce firms. In fact, account fraud can affect a very wide variety of businesses, including financial institutions, retailers, social media networks, review platforms, and even government agencies. It is also often only the beginning of a series of criminal activities, as fraudsters may use these accounts for different purposes depending on the service they are attacking and other relevant factors.

This condensed handbook provides an overview of the different types of account fraud, the techniques used by criminals to perpetrate them, and some action items that companies can take to protect their customers' accounts and their own bottom lines.

ACCOUNT OPENING FRAUD

Account opening fraud can be defined as any attack or criminal activity that targets the customer onboarding process with the purpose of creating fraudulent or false accounts. In what is also known as account onboarding fraud, criminals will use stolen, false, or synthetic identities to gain an entry point and pose as a business' legitimate customers.

These are a few of the ways in which criminals use false accounts at different types of services:

DID YOU KNOW?

took down **1.3 BILLION** fake accounts in 2021

found **95 MILLION** fake accounts in 2021

dealt with **20 MILLION** fake accounts in 2021

Bots and Mass Registrations

As is the case with other forms of fraud, criminal groups often use bots and other advanced technological means in their activities. In this specific case, these techniques are used to mass register accounts and exponentialize the size of the damage they inflict.

For example, fintech companies offering new account creation incentives or promotions with the intention of attracting new customers who will then contribute to their revenue might be wasting valuable resources. Fraudsters often use bots and false or stolen identities purchased in batches by the thousands to mass register accounts, obtain the promotional bonuses, and then abandon the accounts.

Dormant Accounts and Money Mules

These so-called dormant accounts are a widespread issue because they could also be used for money laundering and muling. Since they are highly regulated businesses, this is especially troublesome for financial services firms such as banks and brokerage firms.

According to the FBI, money mules are people who transfer illegally acquired money on behalf of someone else. Criminals recruit money mules and use false accounts to help launder proceeds derived from online scams and frauds or crimes like human trafficking and drug trade. Money mules add layers of distance between crime victims and criminals to make it harder for law enforcement to accurately trace money trails.

Anti money laundering and counter terrorism financing laws and regulations worldwide carry severe penalties and fines and they should be taken seriously.

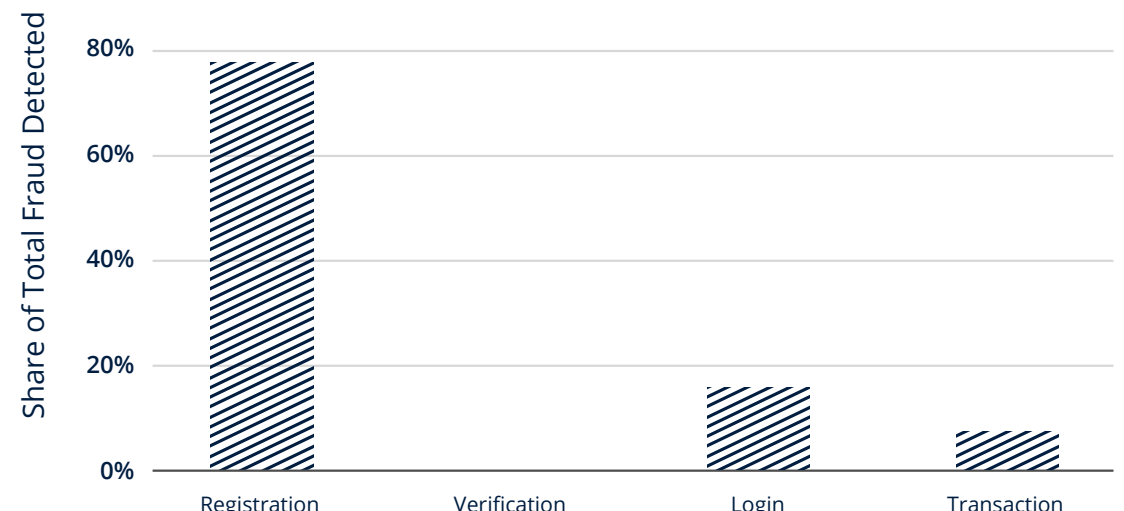
Fighting Account Opening Fraud

The first step towards a robust account opening protection strategy is to recognize that identity validation measures are not enough to solve such a complex problem. When an account opening is authorized solely based on whether or not the applicant has provided an identity (i.e. an SSN) that can be validated with a trusted third party (i.e. a credit bureau), companies might be taking fraudsters' words at face value and neglecting to use evidence to truly single them out from good customers.

Fortunately for everyone (but criminals, of course), technology has come a long way and advanced fraud prevention strategies allow businesses to spot fake accounts and block them before they inflict any damage.

Early detection Is critical, and DataVisor's solutions detect fraudulent activity in real time, the moment an account opens, stopping the process before any damage occurs. They leverage UML to holistically analyze digital fingerprints, metadata and more, and enable accurate decision-making, even with limited information.

Not only does DataVisor capture up to 99% of fraud attempts, but it also does so fast and early. DataVisor stops the vast majority of fraud at the registration point to prevent downstream damage and delivers continuous protection throughout the account lifecycle:



Read this success story about a leading fintech that left behind ACH Fraud, ATOs, Fake Accounts, and Policy Abuse to focus on its mission with serious results, including 92% of fraudulent account openings detected before the disbursement of promotions.

DataVisor's solutions deliver immediate ROI because they don't rely on historical data or labels. Using linkage analysis, they can detect groups of fake accounts simultaneously, enabling fraud and risk teams to make bulk decisions to thwart coordinated, large-scale attacks.

Source:
https://www.cbs17.com/news/investigators/be-aware-of-fake-social-media-accounts-more-than-1-billion-were-ousted-in-2021/

ACCOUNT TAKEOVER FRAUD

Often referred to simply as ATO, this form of fraud is perpetrated by criminals who gain illicit access to existing users' accounts. Like in the case of false accounts, the form of crime committed once accounts are taken over depends on the entity being targeted.

Below are a few of the ways in which criminals use stolen accounts at different types of services:

Credential Theft

This type of cybercrime occurs when someone steals the customers' login information (username and password) to sell them or use them to commit fraud.

Criminals often deploy social engineering attacks to steal their victims' credentials. These include phishing strategies where they send emails, calls or other messages pretending to be legitimate businesses or authorities in order to induce individuals to reveal their personal information such as passwords and credit card numbers.

In other instances, criminals attack the data repositories that keep user credentials at specific companies. This instance of cybercrime is called a data leak and can be used to steal from accounts at the affected companies and at others since users often repeat usernames and passwords for different sites and accounts. In fact:

44% of individuals use just two to five passwords for all their accounts, meaning they all may be compromised in the event of a data breach. In addition, 37% of Americans share their passwords with others, creating another massive opportunity for data theft.

Since data leaks often contain millions of account login details, criminals employ a tactic called credential stuffing where they inject stolen usernames/passwords in website forms using standard web automation tools like Selenium.

Credential cracking attacks, on the other hand, employ brute force to guess an account's password once the login username is discovered. This attack exploits what is often referred to as the weakest link in account protection: users' bad password habits.

Credential theft is also perpetrated by criminals who deploy malicious code on their victims' computers. These attacks include **keylogging**, where an attacker can track what users type and wait until they reveal their login credentials to steal them, and **man-in-the-browser** or MITB threats where browsers are infected to modify web page content, often to manipulate financial transactions in internet banking.

Session hijacking, which can also be called **cookie hijacking**, is an attack where a computer session key is attacked to gain unauthorized access to information. Cookies can be stolen to authenticate users on a remote server.

Regardless of how credentials are compromised or stolen by fraudsters, they are then used to commit fraud attacks which vary depending on the respective type of account. Another relevant aspect of account takeover attacks is that there is often a very long lead time between the moment where the credentials are compromised and when the actual attack is perpetrated, thus consummating the criminal activity.

Stopping Account Takeover Attacks

True ATO prevention requires a holistic approach where users and companies cooperate to promote account safety.

Companies should promote password best practices to make things harder for fraudsters. Such efforts should include deploying strong password requirements and sharing information with users about the importance of good password hygiene. This implies changing passwords regularly, not recycling passwords (especially with the same username in different sites), not sharing passwords with others, and not writing down passwords.

Multi-factor authentication can be an effective tool, but it has important drawbacks that need to be considered before implementing. Specifically, multi-factor authentication measures introduce a substantial degree of friction to customer experiences, which can lead to issues like user attrition and shopping cart abandonment. Given these considerations, companies should look carefully before implementing two-factor authentication measures and consider only requiring them for certain events (i.e. very large transactions) or for situations where an account takeover attack is suspected (i.e. after several failed login attempts).

Thankfully, other options exist. Machine learning is especially useful to detect and stop account takeover attempts before their effects materialize. Instead of using high-friction authentication measures to stop ATO attempts, DataVisor uses artificial intelligence to analyze web session logs, cross-account linkages, digital fingerprints, profile details, and account behaviors to surface even the most stealthy fraud patterns without damaging the UX for good customers.

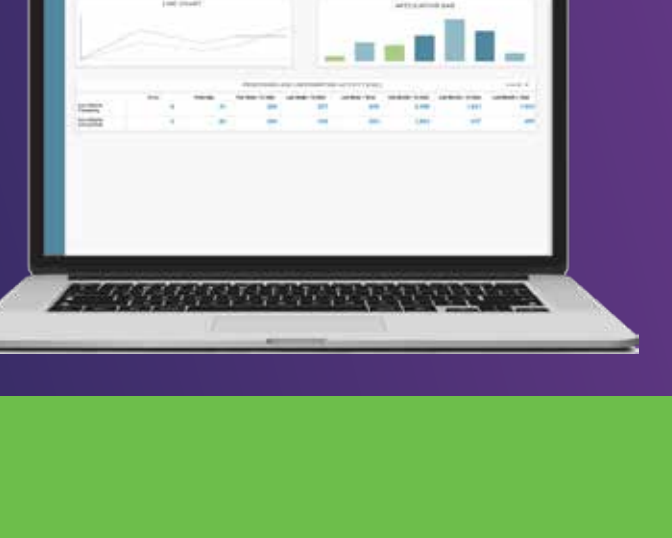
Digital businesses should make sure that their fraud teams are armed with tools that allow them to leverage their users' **behavioral information** to fight account takeovers. It is possible to uncover suspicious accounts and coordinated fraudulent registrations early in the incubation stage by spotting similar attributes and behaviors across accounts without requiring prior labels on the data.

An additional level of account protection can be achieved by employing continuous customer event monitoring techniques. Companies should keep track of logins, transactions, password changes, and other customer interactions to effectively detect anomalous or suspicious activity and act on ATO attempts before they result in financial and reputational damages.

Source:
https://www.pymnts.com/authentication/2022/how-behavioral-analytics-can-prevent-new-account-fraud/

Are you curious about how you can improve account security at your organization? A fraud specialist can answer any questions you may have in a no-pressure environment.

Schedule a free consultation session here!



About DataVisor

DataVisor is the world's leading AI-powered Fraud and Risk Platform that delivers the best overall detection coverage in industry. With an open SaaS platform that supports easy consolidation and enrichment of any data, DataVisor's solution scales infinitely, enabling organizations to act on fast-evolving fraud and money laundering activities as they happen in real time. Its patented unsupervised machine learning technology, combined with its advanced device intelligence, powerful decision engine and investigation tools, provides guaranteed performance lift from day one.

For more information on DataVisor:

info@datavisor.com

www.datavisor.com

967 N. Shoreline Blvd. | Mountain View | CA 94043

DATAVISOR