WHITE PAPER

Socure

Preventing Account Takeover with Identity Verification

The Definitive Guide

Executive Summary

Managing risk and protecting customers have become top priorities for enterprises as the world becomes more reliant on digital services for all aspects of personal and professional life. Achieving these risk-related goals becomes more challenging as fraud continuously evolves in complexity and brazenness. Account takeover (ATO), a form of third party fraud, is one of the more common types of threats, and among the more dangerous, but it can be addressed effectively as part of an organization's overall identity management and fraud prevention approach.

According to the 2020 Javelin Research study, Identity Fraud Report, incidents of ATO increased 72% in the preceding year, and it continues to grow and inflict harm. The challenge for modern organizations is complex, as they do not want to introduce any fraud prevention methods that might detract from the customer experience. At the same time, they must eliminate fraud in order to provide an optimal customer experience.

Let's look at how mitigating account takeover with a layered approach that includes Socure identity verification can control the ATO problem without negatively impacting customers.

> "Sophisticated fraudulent attacks can circumvent many of the legacy tools used to identify unusual activity. At the same time, the behavior of many legitimate consumers is becoming more fluid between devices and geographies and more privacy focused. This makes legacy device fingerprinting and IP address policies ineffective."

Gartner

"Don't Treat Your Customer Like a Criminal"

July 2021

Account Takeover Explained

ATO is an attempt to gain unauthorized account access in a digital environment using the following steps:

1 A fraudster gains access to victims' account(s)

2 That fraudster then makes non-monetary changes to account details, like:

a. Modifying personally identifiable information (PII)

b. Requesting a new card

c. Adding an authorized user

d. Changing the password

3 From there, the fraudster carries out unauthorized transactions resulting in a financial loss

Additionally, there is the risk to the business in the form of brand damage, which happens through the potential loss of the victim's customer relationship between the business and the consumer.

Countering ATO fraud while minimizing consumer experience friction poses an ongoing challenge for financial services, fintechs, and other digital enterprises. It's critical to stop the bad actors while not inconveniencing or frustrating good customers. This is where a fraud risk score provides a valuable tool to passively control ATO without interference in the customer experience.

Account Takeover Countermeasures

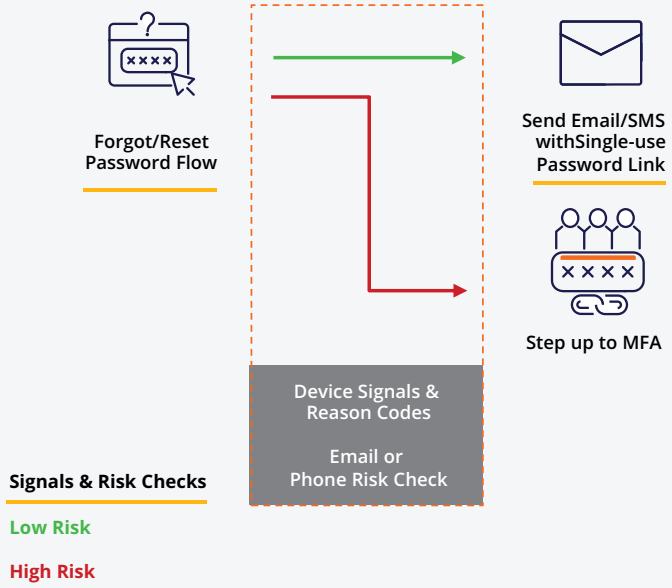
Enterprises typically have controls in place to mitigate ATO attacks. These include bot mitigation, behavioral biometrics, device telemetry, and transaction/event monitoring. Each of these controls help stop ATO, but none by itself solves the problem. There is no "silver bullet" technology that completely eliminates the ATO problem. An optimal approach layers ATO mitigation solutions to control the issue.

Fraud Dynamics in ATO

Fraudsters frequently need to modify account profiles in order to execute their nefarious activities, and that means changing an account email address or phone number. The bad actor can then navigate step-up controls when the organization might send a one-time passcode to the dubious email address or phone number. Once the fraudster has redirected the account, they can take full control and make unauthorized transitions to make an illicit profit.

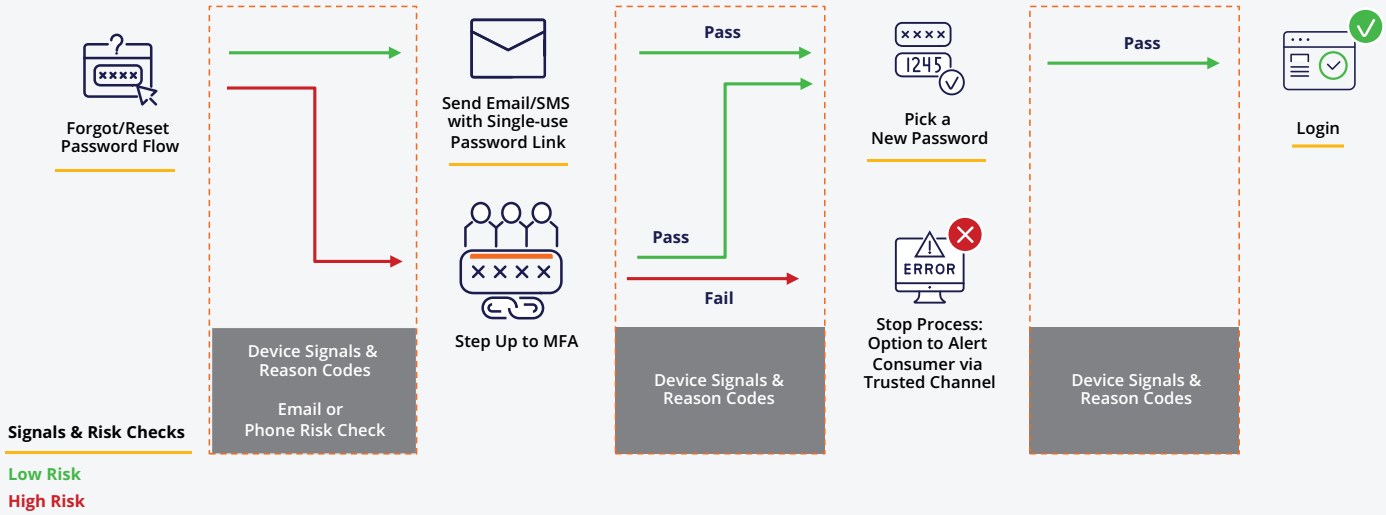
An underutilized control point is when those account profile changes are made – specifically, the modifying of an email address, phone number, or physical address on file. Before making a requested change, enterprises can validate the riskiness of that email, phone number, or address, and check the device signals, while also checking on how closely correlated these various presented digital identity elements are with the user itself (see Figure 1).

FIGURE 1: MULTICHANNEL RISK & ATO: ADDED PROTECTION FOR CRITICAL FLOWS



Moving beyond the profile change process, device risk can help control risk at every point of interaction including login, profile page, account updates, high-value and risky transactions, and more (see Figure 2).

FIGURE 2: DEVICE RISK & ATO: EXTENDED PROTECTION FOR CRITICAL PROCESS FLOWS



Comparing Effectiveness in Countering ATO: Socure vs Alternatives

Effectively countering ATO requires validating identity elements such as email addresses, phone numbers, and physical addresses. Socure's graph-defined machine learning provides unique insights into these and other dimensions of a consumer's identity. Socure customers regularly perform comparisons to understand the effectiveness of Socure solutions against legacy and internally-developed solutions to validate email addresses or phone numbers. The charts on this page summarize one recent example of a major U.S. financial institution validating the performance of its existing solution from a top provider for phone intelligence against the Socure Phone RiskScore.

Socure Phone RiskScore effectiveness, as measured by the statistical Area Under Curve (AUC) for new account labels, is vastly better than another top provider based on ID fraud feedback data when predicting fraud at time of origination (see Table 1), an effectiveness that is also found at profile changes or when sending one-time passcodes. The table below compares AUC, fraud capture, and good-to-bad ratio (number of "good" identities flagged for every "bad" identity) for phone risk score results from Socure and an industry top provider.

The Socure Phone RiskScore offering provided consistently higher fraud capture with fewer false positives as represented by the good-to-bad ratio. This greater precision translates into stopping more ATO attempts while also providing consumers a better experience with less friction through a dramatically lower false positive rate.

The institution providing the test data also found that Socure Name-Phone Correlation has ~5% greater match on first name and ~3% greater match over the competitive product on last name based on production data for new accounts (see Table 2). A better name-phone correlation and coverage percentage results in a smoother customer experience with more accurate decision making.

TABLE 1: PHONE RISK SCORE COMPARISON

	Socure	Top Provider
Performance (AUC*)	**0.9058**	**0.6433**
Fraud Capture		
1.00%	**39.03% / 2:1**	1.79% / 55:1
2.00%	**50.75% / 3:1**	8.56% / 22:1
3.00%	**56.99% / 4:1**	9.90% / 29:1
4.00%	**61.87% / 5:1**	11.44% / 34:1
5.00%	**65.26% / 7:1**	20.85% / 23:1
10.00%	**75.51% / 12:1**	32.00% / 30:1

*AUC=Area Under Curve. Area Under the Curve (AUC) is the measure of the ability of a classifier to distinguish between classes and is used as a summary of the ROC curve. The higher the AUC, the better the performance of the model at distinguishing between the positive and negative classes. When AUC = 1, then the classifier is able to perfectly distinguish between all the positive and the negative class points correctly.

TABLE 2: NAME-PHONE CORRELATION COMPARISON

Name-to-Phone Comparison	Socure	Top Provider
FirstName Correlated with Phone	89.60%	84.61%
LastName Correlated with Phone	91.28%	88.02%
Overall Phone Coverage	96.29%	95.44%

Holistic Identity Analysis Improves Precision

Socure's Sigma models deliver superior accuracy by analyzing every dimension of consumer identity including name, email, phone, address, date of birth, SSN, IP, device, velocity, network and behavioral intelligence, and more. All of this is delivered in a single machine learning-based model.

Socure's fraud solutions take advantage of however much information a customer can provide. The Socure risk scores become progressively more accurate as more dimensions of a consumer identity are provided. Organizations can evaluate device signals with Sigma Device, a phone number with Phone RiskScore, an email address with Email RiskScore, or a complete identity with Sigma Identity Fraud and Sigma Synthetic Fraud, which leverage name, email, phone, address, date of birth, SSN, IP, device, velocity, network and behavioral intelligence to determine third-party and synthetic identity fraud.

Mitigating ATO with Socure: Use Cases

A key element of Socure's defense in depth is deflecting fraudsters at account opening and then validating profile changes or high-value transactions during the account lifecycle. The Socure ID+ family in general, with Socure Sigma Device combined with the Socure Phone RiskScore, Email RiskScore and Address RiskScore offerings in particular, are essential tools in your kit of ATO countermeasures to passively stop fraud and maintain an optimal customer experience. Below are some of the more common customer use cases.

ACCOUNT PROFILE CHANGES

Customers regularly change phone numbers and email addresses, but fraudsters can compromise credentials and redirect traffic to their own email or phone destination. Before accepting a change, many organizations validate the risk of the phone number, email address, or mailing address, as well as checking that the data is correlated with the presented identity. This validates the identity to stop potential ATO attacks.

VALIDATING OTP DESTINATIONS

One Time Passcodes (OTPs) are codes that are valid for only one login session or transaction. An OTP is usually sent via SMS to a mobile phone or to a destination email address, and they are frequently used as part of two-factor authentication (2FA). Validating the risk of the email or phone number destination along with correlating that it corresponds to the expected consumer can mitigate against ATO attempts.

ADDRESS VALIDATION FOR MAILING CREDIT CARDS

Financial institutions (FIs) operate in the digital world, but also in the physical world. FIs send credit cards and debit cards via the postal service to reach consumers, and fraud rings try to redirect those mailings. Before they put the envelope with the new card in the mail, most FIs validate the risk of the destination email address and check that it correlates with the expected consumer identity. Such checks can validate that the destination is a residential address rather than a commercial address or a jail and can also correlate that the destination physical address correlates with the consumer identity.

ADDRESS VALIDATION FOR HIGH-VALUE GOODS SHIPMENTS

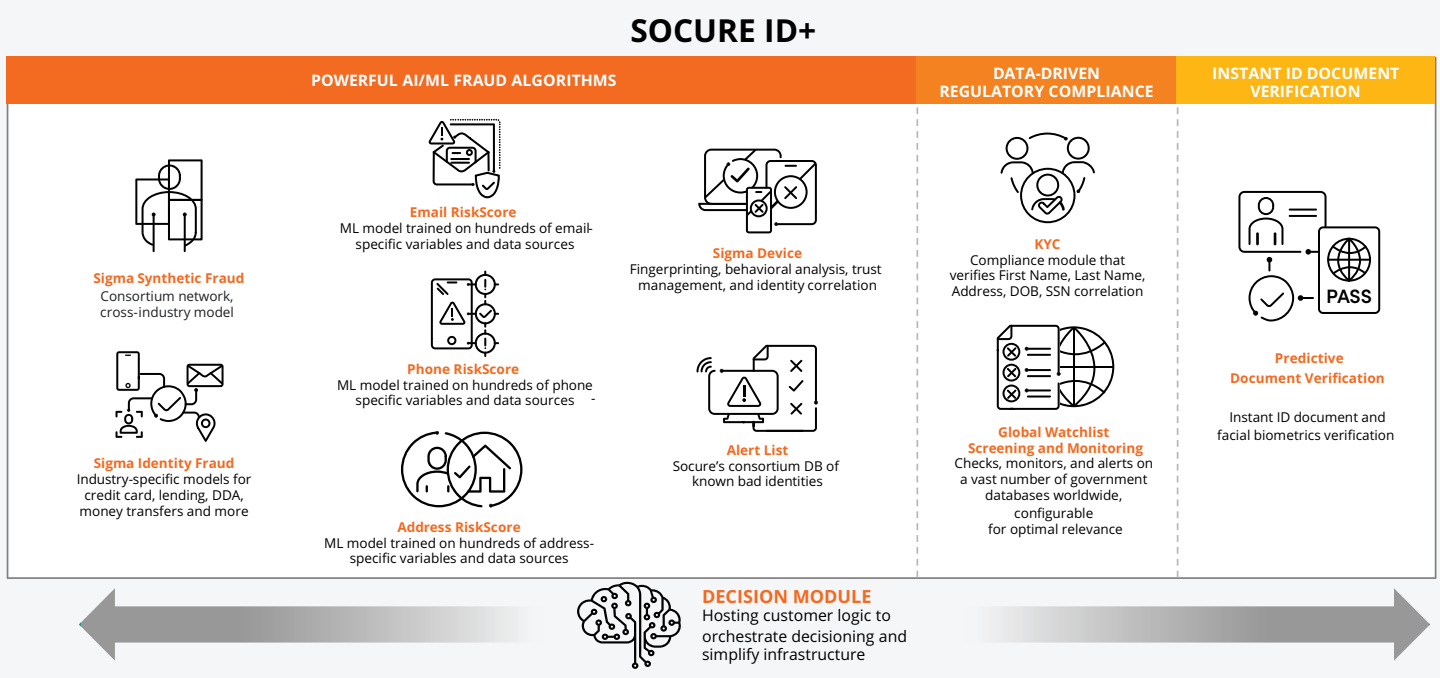
Fraudsters follow the Willie Sutton strategy. Willie Sutton, a notorious bank robber, was reputedly asked why he robbed banks, and responded, "Because that is where the money is." Fraud rings trying to make a buck frequently focus on high-value goods. E-commerce merchants and marketplaces countering fraud in high-value transactions can validate the risk of physical delivery addresses along with the correlation between that address and the consumer identity to minimize the possibility of fraud.

LOYALTY FRAUD & REWARDS POINTS REDEMPTION

Rewards points redemptions happen in diverse industries from airlines to hotels to retail. Loyalty fraud occurs when a person exploits or abuses your program for personal gain or criminal activity. A Gartner research analyst in 2018 reported that 48 trillion points are unspent globally with a value of $100 billion in the U.S. alone. Organizations can validate point redemptions/transfers by calling call risk services to validate that PII and device data is consistent with a good transaction prior to an account payout.

Solving ATO with Socure

Socure Sigma Device along with Socure Email, Phone, and Address RiskScore offerings can protect against ATO while maintaining the optimal customer experience by passively evaluating risk and correlation associated with identity elements like email addresses, phone numbers, and physical addresses.



To learn how Sigma Identity Fraud, Sigma Synthetic Fraud, Sigma Device along with Email, Phone, and Address RiskScores can boost the effectiveness of your identity verification, and control ATO, schedule a demo today or get in touch at salesinfo@socure.com.