KNOW IDENTITY

Mitigating the Mobile Account Takeover Epidemic

WHITEPAPER

July 2021

ONE WORLD IDENTITY

TMTANALYSIS

TABLE OF CONTENTS

INTRODUCTION

The COVID-19 pandemic has been instrumental in forcing businesses and consumers alike to seek new means of transacting via remote digital channels. This advancement of digital transformation may well have moved industries forward by months or even years, but there has been a cost associated with the uptick in fraud, with criminals taking advantage of naive users, weaknesses in traditional ID verification and the ability to hide in plain sight given the sheer volume of users moving en masse to digital channels.

The Achilles heel for much of this fraud has been mobile devices — as an always-on, always present technology, today's smartphones are inextricably linked to our daily lives, providing the connective tissue between digital and physical domains. While these attributes have been immensely enabling, there is a downside — these same attributes are also accessible to fraudsters, facilitating the ability to commit large-scale fraud anywhere on the globe, with smartphones at the epicenter of enabling these schemes. The eye of the storm is mobile account takeover (ATO) fraud, which enables not just the exploitation of the device and its installed apps, but also online accounts where technology such as SMS is used for access using out of band one time passcodes (OTPs).

The statistics outlined in this report speak for themselves — ATO fraud grew over 650% in 2020. While some of this could be chalked down to newly digital users and something of a pandemic "fog of war", 2021 may not be much better since fraudsters may be more focused on business as usual now that COVID19 related schemes are drying up.

> **There is a silver lining, however. Fraud mitigation technologies such as AI and ML continue to evolve, enabling fraud to be detected and stopped sooner than ever, and ever more ingenious means of proving true identity through behavioral biometrics bring the best of both worlds — robust verification and authentication, with minimal, if any, user friction. As well as mitigating fraud, the introduction of technology to what have historically been manual and labor intensive processes can have significant cost benefits. For instance, by incorporating digital identity within the verification process, AML and KYC costs can be reduced by up to 70%.[1]**

Finally, none of these solutions is suggested as a binary response to fraud — solutions can be built in layers, adding necessary verification steps as and when the risk profile warrants their requirement.

Read on to learn more about the current state of mobile account takeover fraud and best practices for risk mitigation.

ACCOUNT TAKEOVER FRAUD — EXPONENTIAL GROWTH FOR PANDEMIC OPPORTUNISTS

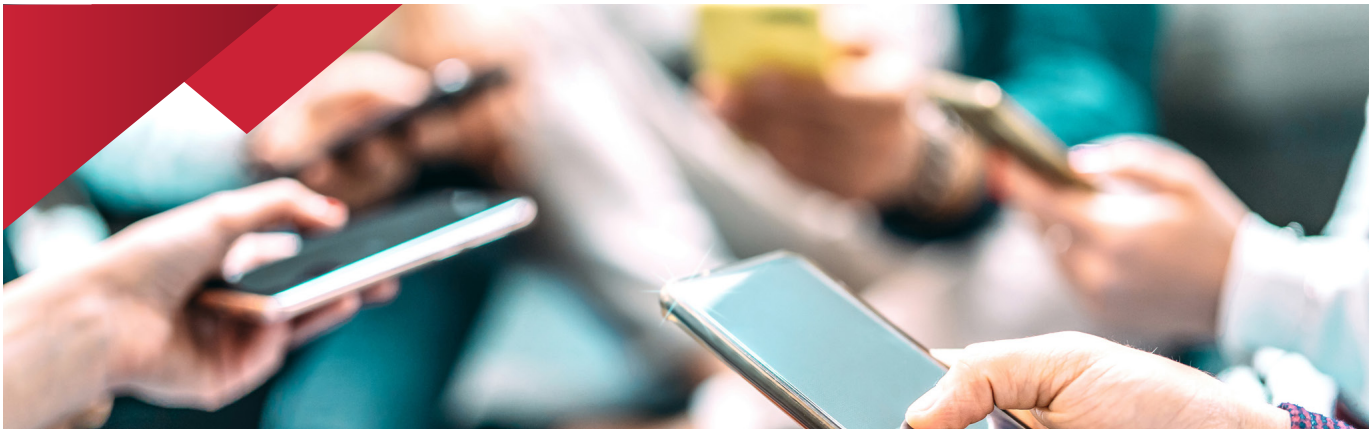
Mobile account takeover has been one of the most devastating means of perpetrating fraud in recent times given how pervasive mobile devices are in our everyday lives and the degree to which consumer accounts are reliant on mobile-based authentication for access. However, mobile is a subset of overall account takeover (ATO) fraud — a crime that has grown significantly in recent years.

Leading into the pandemic, ATO fraud had one of the highest rates of growth among fraud schemes, with a 70% increase in the U.S. in 2019.[2] That trend continued into 2020 — between the second quarter of 2019 to the second quarter of 2020, ATO fraud grew by 282%.[3] This occurred for two reasons:

1. **The rise of digital usage in 2020 increased at a level few expected.** Due to the pandemic, the time people spent on digital devices to bank, socialize, or shop increased by 215%.[4] Increased usage of digital tools also expanded the attack vectors that fraud organizations used to breach an organization or individual, with criminals often able to hide in plain sight due to the sheer volume of new users accessing digital channels.

2. **The increased data available on the dark web.** The amount of records exposed on the dark web and available for use by fraud groups willing to conduct ATO fraud grew 652% in 2020, compared to the year prior.[5] With more data available, fraud organizations have a greater ability to attack and steal more credentials.

Due to these trends, ATO fraud has become the most popular way that fraud organizations conduct financial crime, accounting for 42% of all fraud attempts against banks.[6]



Certain sectors face increased risk from an ATO attack

Social Media **36%**

Digital eCommerce **36%**

Financial Services **35%**

Physical eCommerce **25%**

Online Dating **22%**

Travel **19%**

On Demand + Delivery Services **12%**

Work apps/sites **7%**

Source: Sift

Consumers have become aware of the prevalence of this fraud, due to personal experience. Thirty-eight percent of consumers say they have been the victim of ATO fraud in just the past two years.[7] Further, 41% said it had occurred to them up to five times.

The Most Common Types of ATO Fraud Tactics

SIM Swapping: SIM swapping is an activity that consumers perform when they need to replace a SIM card or switch mobile carriers. SIM swapping fraud takes advantage of this process when a fraudster convinces a mobile phone agent with the help of stolen PII to switch a phone number from the consumer's SIM card to a fraudulent one. By doing so, the fraudster takes over a customer's number and, with control of the phone number, can often verify access to online accounts.

Phishing: Phishing remains one of the oldest and most effective tools in a fraudster's toolbox, using basic social engineering to trick the victim into believing that the inbound message is legitimately a request from the purported sender. The tactic preys on peoples' trust through email, text, or social media, encouraging users to hand over sensitive personal identifiable information (PII).

Malware: Malware can be sent via a phishing effort, or designed within an application. When a consumer downloads the infected app or attachment, it adds malware to the consumer device. Some malware can track the typing of the consumer, capturing the bank login.

Credential Stuffing: Often through the help of bots, a fraud group will attack a company using hundreds to thousands of accounts and passwords (sold from the dark web) in an effort to find holes within a fraud system. Fraudsters use the same account data against multiple organizations since consumers will often use the same password and login combinations.

Mobile Banking Trojans: An infected phone in a mobile banking trojan attack will have an overlay on top of a regular banking application screen. With the overlay, the user logins without realizing the overlay is in place; malware then tracks the keystrokes.

Man-in-the-Middle Attacks: As the name suggests, the bad actor sits between the user and the financial institution. The one conducting the attack can then view the keystrokes or data that the consumer provides at login. Often this occurs via a malicious Wi-Fi hotspot, where the user logs in without realizing a fraud group or individual runs the hotspot.

THE DANGER OF MOBILE ACCOUNT TAKEOVER

Mobile account takeover is a particularly pernicious subset of ATO fraud. Take, for instance, a victim of a SIM card swap. One minute the user has control of the phone. The next minute, it's disabled, unable to access online accounts. Then, when the user tries to access the accounts via a computer, they no longer can since the criminal has changed all of the account settings. The fraudster can then use the data and access to the phone number to lock the user out of other accounts, drain said accounts, and create new accounts, all using the personal profile verified by the phone number. They can achieve this level of theft because they use the institutions' reliance on the phone as a primary source of verification. It may not look like mobile ATO fraud from the institution's point of view, but the SIM card swap allowed for the fraud activity to unfold.

In such a scenario, a fraudster has multiple attack vectors in which to conduct the mobile ATO, including:

- **The SIM Card:** Criminals can link a phone number to a new device under their control through the SIM.
- **Port Out:** The process to move an account to a competing carrier can be used by a fraud group to switch a victim's number to the new carrier, with a device under the fraudster's control.
- **Call Forwarding:** A person's calls are forwarded to the fraudster, without the user's knowledge, resulting in the ability to confirm actions such as fraudulent mobile payments.

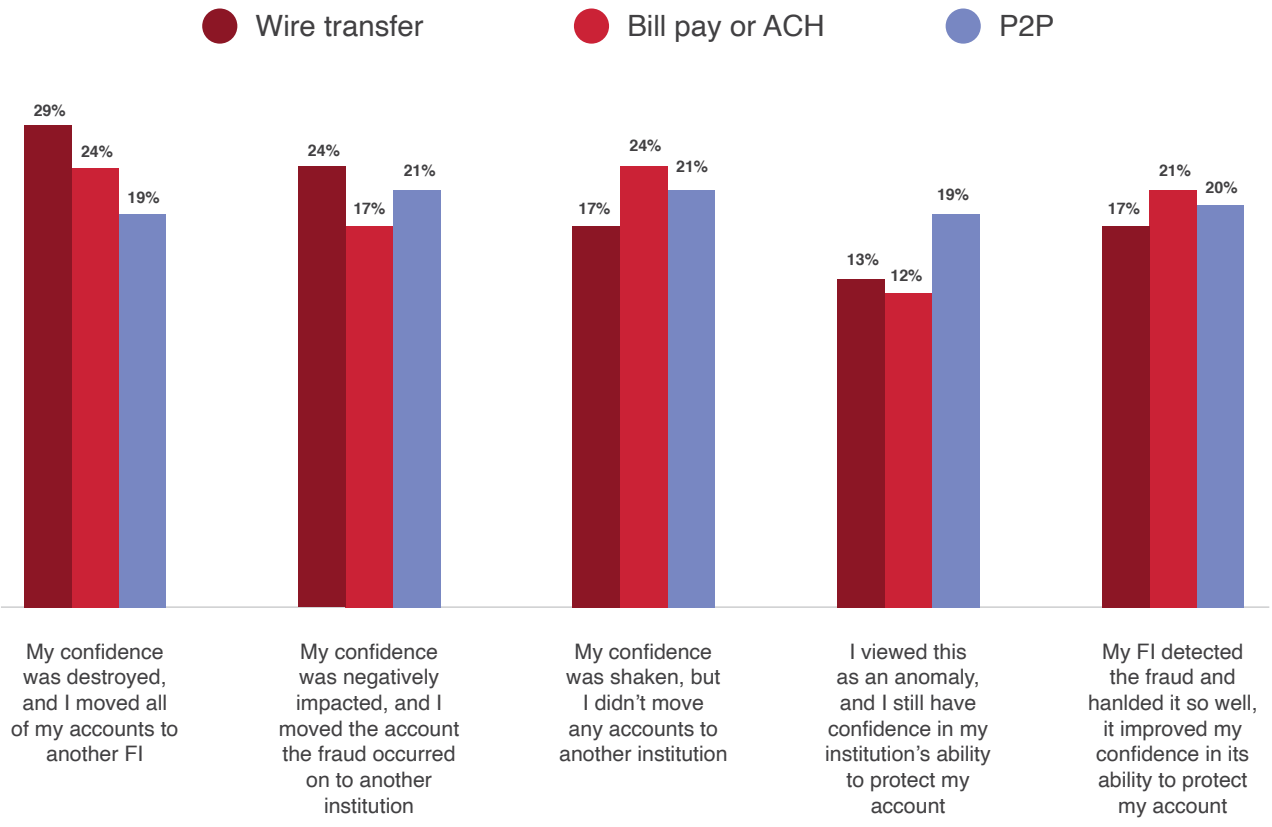
Fraud Finds Scale

While the image of a hacker in a dark basement may have permeated through pop culture, in reality when it comes to fraud attacks, companies must realize they face an enemy that is structured more like an organization. A recent such fraud ring used more than 20 mobile emulators and 16,000 devices to spoof account holders and steal access to their smartphones. They used scripts to automate the process, stealing from thousands of users. It's an effort that required funding and a network of criminals to pull off.[8] These groups invest in the latest technology, including AI and ML, to better circumvent financial institutions' protections and attack a larger group of people. It also means that companies face potentially significant losses when targeted by a fraud ring.

TIME TO DETECTION CHALLENGES

One of the main reasons for ATO fraud's success — the crime can remain hidden undetected for long periods of time. In cases where wire transfers were used during an ATO attack to steal funds, 39% of people learned about the attack on their account from a credit monitoring service or a collections agency. But when people do learn of the attack, they blame the organization for allowing it to occur. For those that faced an attack that impacted an account at a financial institution, 53% of users moved all their money to another organization once they learned of the breach.[9]

Impact of ATO on Customer Confidence in Their Financial Institution



Source: Giact

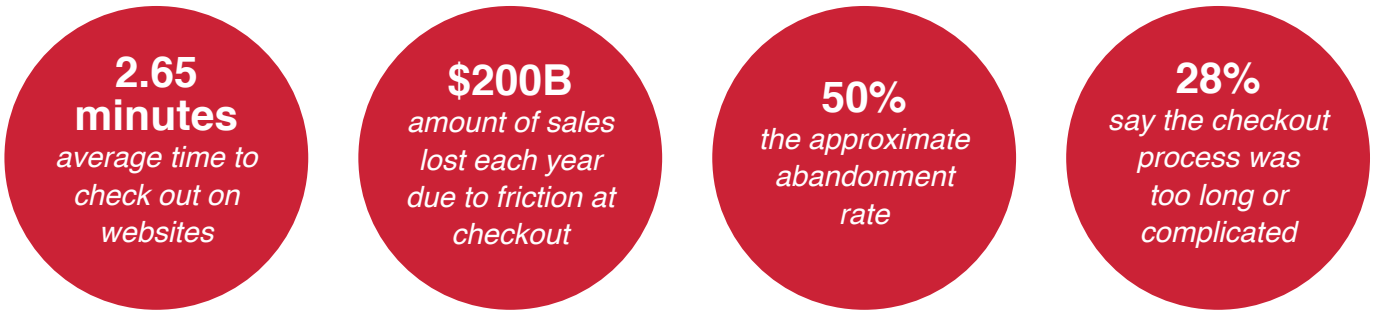
The indirect costs are also staggering. With increased ATO attacks, retailers face the likelihood of more chargebacks. In 2019, 30% of customers filed a chargeback due to a purchase made with a stolen credit or payment card. And, after an ATO attack occurs, 12% of customers do not change account information, allowing the bad actor to continue to attack the customer and the organization.[10] Having the tools in place to detect and prevent such attacks is vital to ensure that the ongoing rise in mobile ATOs will have limited impact on the company and its customers.

BUILDING UP COUNTERMEASURES

The key to preventing mobile ATO attacks resides in electronic identity verification (eIDV) and ongoing end user authentication tools. It is important that these measures don't just ensure robust proof that the individual is the legitimate claimant of the identity, but that these tools are not so onerous as to impede the end user's digital experience. Finding this sweet spot is a balancing act and highly subjective based on the risk tolerance of an organization.

This section outlines some of the best practices in countermeasures today, as well as outlining why a layered approach to fraud mitigation is required.

The cost of friction remains a vital part of the security puzzle



Source: Retail Dive

Mobile ID Verification Solutions

Mobile ID verification, from the consumer perspective, often looks similar to protections that they may find through any other device. But subtle differences exist. Like many services, mobile operators will provide users with a six to 15-digit pin, which serves as, essentially, a password to unlock or move services. This has benefits since users understand how to utilize such a code. It, however, can also be stolen similar to any other piece of PII or password. Organizations often give users the ability to incorporate two-factor authentication as well, which adds another form of protection.

But organizations face two issues when adding more protections. 1) They do not want to add so much protection that it becomes onerous on the user. Too much friction and consumers will not want to use the protection or the service. 2) Adding protections through the mobile device has the potential to fall into the fraudster's hands, if they end up controlling the SIM card or phone number. In fact, the verification method through the device, in such a situation, further protects the fraudster and harms the victim (once the bad actor takes control of the device). Instead, it requires the right type of mobile protections, which also take into account the user's

digital identity. Often such tools can work in the background, requiring little to no interaction by the user.

Mobile Network Operators (MNOs) have become a powerful source of data. Thirty providers have a network that spans the globe, and will cover six billion subscribers by 2025.[11] Using MNOs, organizations have access to location, biometric, and usage data, among other resources. Using this MNO data in the mobile ID verification can provide a clear picture of the user. By incorporating the data within your security layers, it allows an organization to recognize when roaming signals indicate that a user is in a location the company would not expect, based on previous activity. This becomes a sign of potential fraud. Or it can capture any increase in call forwarding, which could signal call forwarding fraud. And it can also see whether the SIM recently changed, flagging certain activity, like account withdrawals, as potential fraud.

Other protections, like SIM checks, will recognize when SIM cards have recently changed, flagging potential efforts to circumvent text message confirmations. This strengthens protections beyond the simple pin code, since the tool can recognize when a potential SMS confirmation may actually be an effort by a fraudster to take over a device.

Artificial Intelligence and Machine Learning

Fraud organizations adapt with the times, utilizing new technologies as soon as they can afford them. The reason they often seem one step ahead is that they do not have to worry much about process or organizational impact when incorporating the technology. Instead, if they can use it to better infiltrate a system, then they will. As the attackers, they also benefit from first-mover advantages. This leaves organizations playing catch-up to attacks. For combatting mobile ATOs, where often users and institutions do not even recognize an attack occurred, it is vital to have measures in place to prevent the attack before — or right as — it begins. That has become the potential of machine learning (ML) and artificial intelligence (AI). These tools can allow organizations to stop an ATO attack in real time, as opposed to responding to the attack after it has already taken place.

Take, for instance, a user asks to change the user name and password linked to a bank account. Sure, this activity can happen with a regular customer. But it also is a tactic that fraudsters will use to take over an account. How does the organization determine whether this request came from a user or not? This shows the potential of ML and AI. Using technologies such as behavioral biometrics and user and entity behavior analytics (UEBA), organizations can determine whether such requests made sense based on how the individual typed the information, when it occurred, where, or on what device. The ML component can subtly determine an unlikely shift in regular behavior. These tools provide frictionless ways to detect such devious activity before it has a chance to take over an account. And, in the case of bots, it can do so with each individual instance, keeping up with the thousands of requests a bot might try to make.

Layered Technologies

To protect against mobile ATO attacks, no one solution will provide the answer. Instead, fraud management requires a layered approach, in which many technologies support the fraud detection efforts. With the right solutions, this does not necessarily introduce increased friction. Instead, many of the solutions work in the background, providing constant security and flagging when increased verification is required. This enhances security from a simple deterministic approach such as passwords or PINs, providing many layers of verification in the identification process. This also goes beyond standard multi-factor authentication (MFA), which uses tactics like SMS messaging to confirm identity through the same device that the person committing fraud is trying to commandeer. Instead, a strong MFA layer will include attributes unrelated to the single device in question and more difficult to impersonate, like biometric identification through a fingerprint scan or facial recognition.

The reason using SMS texts or clicking on links sent to a smartphone does not provide a secure layer of protection is because those committing fraud can easily pretend that they are the account owner by swapping SIMs or using the account owner's PII. Instead, moving identification efforts to different devices and networks allow for further protection "out of band". If a user needs to access an account on a laptop, for instance, they will identify themselves both on the laptop and another device, like a smartphone. This improves protection through the requirement for multiple device confirmations, but also multiple networks, since the verification goes through, say, the Internet at home and the mobile network linked to the smartphone. This, as an example, reduces the potential for man-in-the-middle attacks.[12]

The layered approach also allows for protections the consumer never sees, like behavioral biometrics or UEBA support. As the action in the account unfolds, the technology compares the action and activity to the historical data for the customer — like time spent on each page, the angle the smartphone is being held, analysis of the user's walking gait, and more.

With a layered approach, institutions can increase the number of steps a user must pass through in order to gain access to an account when the tools signal the potential for fraud.

With the implementation of 3D Secure 2.0 authentication protocol for merchants, this layered approach to preventing mobile ATO becomes more viable. The original protocol did not take mobile into account when incorporating credit card authentication. Instead, it increased friction at the sales level and, because it didn't incorporate into mobile channels well, it often looked like it might have been a tool to attempt fraud. Now, with 3DS2, retailers can integrate the authentication into mobile applications, it only requires authentication in high risk cases, biometric verification will be seamlessly incorporated, and much of the authentication efforts are hidden from the user.[13] Visa found that 95% of transactions will be approved immediately through this protocol while reducing fraud by 40%.[14]

THE UPSIDES TO LAYERED ID VERIFICATION

By incorporating a layered ID verification approach, companies gain benefits beyond the simple act of stopping mobile ATO fraud. They can reduce the friction customers face when accessing accounts, reduce the cost of fraud prevention, and prepare for any future trends within the mobile fraud space.

Reducing Friction While Increasing ROI

Companies and financial institutions have, historically speaking, had to view fighting fraud, particularly ATO and mobile ATO fraud, as an if-or decision because of the potential for increased friction. For retailers and social media firms, the desire to ensure a frictionless experience won out, which had the potential to drastically increase the amount of attacks. They did this because any type of friction could ruin a sale or signup. The fear that false declines within fraud systems would turn away reliable customers also played an important part in discussions. Financial institutions, insurance agencies, and health care organizations, on the other hand, had to weigh security against all other needs. This drastically increased the amount of friction users could expect to experience.

By incorporating an eIDV process, through layers that support a mobile experience allows for a drastic reduction in both friction and attacks. This ensures that organizations do not have to look at the two interests with a competitive framework. The incorporation of eIDV, for instance, has resulted in drastic reductions in the onboarding process for highly secure institutions.

> **Investor onboarding at financial institutions went from a few days to under five minutes**
>
> **Online registration at healthcare organizations reduced time from up to 28 days to under 10 minutes**
>
> **Insurance company signup fell from four days to 30 seconds**[15]

This does not increase the potential for fraud. Organizations can use ID verification to meet regulatory Know Your Customer (KYC) concerns. They achieve this because the digital identity has been developed and accessed without the need for customer input. This ensures the individual's identity and prevents fraudsters from circumventing the system. Therefore, the risk of fraud declines. The layered identification approach provides the potential for continuous monitoring, or the ability to have a clear picture of the user throughout the customer lifecycle from account opening through purchase and ongoing support. It makes it more difficult for a fraudster to circumvent, since it requires retaining the original account owner's cadence, typing

rate, and style of access throughout the entire visit. Any red flag that rises will result in additional layers of verification. Among those financial institutions and technology companies that have incorporated a layered approach using AI and ML, 40% say it further increases value in the investment, due to the ability for continuous monitoring to fight fraud.[16]

In the long-run, it also proves to reduce costs. Traditional anti-money laundering (AML) and KYC efforts at financial institutions cost approximately $2.50 for a basic check, but that rises to $10 to $150 due to the staff required for more intensive investigations. By incorporating digital identity within the verification process, AML and KYC costs can be reduced by up to 70%.[17]

The Future State

While utilizing a holistic approach can aid organizations in their efforts to fight fraud, there remains significant trends that companies must keep an eye out to prepare in case fraudsters switch efforts or if new security tactics come to the fore, which may provide further protection. Within the mobile ATO space, three specific trends are worth watching in order to adjust fraud-fighting efforts. The layered approach allows the ability to adapt as norms, tactics, or fraudulent activity shifts.

The Debate Over eSIM continues

Mobile carriers face an increasingly loud chorus of industry players calling for the development of eSIM within smartphones. The introduction of eSIM would make the replaceable SIM card obsolete. Instead of users switching SIM cards whenever they change carriers, the eSIM would allow carriers to switch the phone without changing out the internal card. Software makers want this because it would provide more room for other features, like increased battery life.[18] It would also help prevent SIM swap. Critics argue, however, that fraudsters would use other tactics at the carrier level to conduct the fraud. Within such a framework, it further encourages the recognition of the user, no matter where they access the account or service, achieved through eID verification. financial institutions that fall for the tricks.

Fraud Worsens, Post-COVID

The rate of fraud showed significant growth prior to the pandemic. Globally, nearly half (47%) of companies had reported a case of fraud over the past two years, prior to the onset of COVID.[19] While the rate of fraud growth during COVID highlights the potential that those conducting the crimes saw in the confusion around the pandemic, it also provided an indication of what occurs when more business moves to digital. This digital shift will not end, post-COVID. Banking customers have essentially adopted digital as their primary way to contact a bank with 71% of customers using digital banking tools weekly.[20] Such online presences mixed with a growing level of expertise and technological sophistication from fraudsters leads to the expectation of ongoing growth in fraud rates.

Back To Normal For Fraud Businesses

During COVID, fraudsters moved to try and attack systems that were built in effort to ease the pain of the pandemic or to provide aid. This resulted in a heavy focus from fraudsters trying to steal benefits, such as stimulus checks, loans from the Payment Protection Program, or the Economic Injury Disaster Loan Program in the US. Fraud groups also pretended to provide aid to circumvent systems, by acting as mask suppliers, used fake vaccination scams, or targeted healthcare organizations. This focus on COVID related scams will dissipate along with the threat of the pandemic. In response, fraud organizations will return to common low-hanging fruit targets once again using phishing tactics, synthetic fraud, or other common tools, targeting those at organizations or financial institutions that fall for the tricks.

The way fraud shapes the rest of the year may look more like 2019 (pre-COVID), returning to more traditional types of attacks. But the rate of attempts, victims, and losses will certainly rise, as will the use of the smartphone as a way into an attack. Having protections in place that can secure the organization through a multi-layered approach prevents any shifts in tactics from leaving the business insecure.

CONCLUSION

Stopping mobile ATO fraud has become a vital way to prevent larger attacks on organizations. Through the proliferation of smartphones and the use of the devices to verify individuals by financial institutions, retailers, and other firms, those conducting mobile ATOs can infiltrate accounts and implement destructive fraud tactics. It makes for more important financial implications for organizations seeking to prevent fraud. Also, due to the impact ATO fraud can have on customers when it does occur, consumers blame the institution. This results in moving business to a competitor. The fraud not only saps the organization of funds, but leaves them with fewer customers as well. The institutions that take this threat seriously will become the ones that consumers turn to as threats rise.

With so much of verification centering around the smartphone, it makes it possible for those conducting fraud to use the verification methods to steal a phone number and access a person's swath of accounts located on or authenticated by the phone. By investing in technology that can move the verification process to a multi-factor method, as well as providing layers of opportunities to secure a digital identity, then the verification becomes an ongoing process. While the phone may be used within this process, so will other protective layers, including biometrics, other devices, and backend data through AI or ML, resulting in a more holistic view of the user. This reduces a fraud group's ability to conduct fraud through any single method, like SIM swap.

By understanding this value, organizations can take the steps necessary to protect users, creating an advantage over competitors as more customers seek safety.

ABOUT

ONE WORLD IDENTITY

One World Identity (OWI) is a market intelligence and strategy firm focused on identity, trust, and the data economy. We help businesses build solutions, execute upon strategies, make informed investment decisions, and connect with key decision-makers. Since 2016, we've advised many of the world's most innovative business leaders, investors, and government officials on building, buying, and investing in the next generation of integrated digital identity platforms and technologies. We recognize that identity, trust, and the data economy transcend industry verticals and are at a critical tipping point. Our goal is not just to help our clients respond to the market; we help them define it.

To learn more please visit **www.oneworldidentity.com**

KNOW IDENTITY

KNOW Identity is a community of thought leaders, executives, investors, policymakers, builders, and rising startups that are reimagining the way we implement digital identity solutions at scale. KNOW Identity's uniquely differentiated media and immersive events are where the leading edge of digital identity gets sharper. Our mission is to facilitate thoughtful conversation, enable cross-industry collaboration, and discover actionable solutions for the data economy. Learn from industry experts, develop your personal network, forge new partnerships, and contribute to a global conversation.

To learn more please visit **www.knowidentity.com**

TMT ANALYSIS

TMT Analysis is the leading provider of global mobile numbering intelligence. Mobile number data intelligence can help strengthen and validate the user verification process, reduce fake accounts, improve conversions with customers and even determine the optimal channel for message delivery.

Our data powers many of the world's leading identity providers, A2P SMS Messaging companies and financial services organisations, delivering actionable insights that enhance and protect every stage of the customer experience.

To learn more please visit **tmtanalysis.com**

ENDNOTES

1. “Mobile Identity Enabling The Digital World,” GSMA, https://www.gsma.com/identity/wp-content/uploads/2020/07/Mobile-Identity-enabling-the-digital-world-report-Final-1.pdf
2. Javelin, 2020: https://www.fisglobal.com/en/insights/what-we-think/2020/april/2020-javelin-id-fraud-study-points-to-dramatic-rise-in-real-time-p2p-fraud
3. Sift, 2021: https://pages.sift.com/rs/526-PCC-974/images/ebook-digital-trust-and-safety-q32020-account-takeover-fraud.pdf
4. Experian, 2020: https://www.experian.com/content/dam/marketing/na/assets/im/decision-analytics/infographics/account-takeover-fraud-2020-infographic.pdf
5. Experian, 2020: https://www.experian.com/content/dam/marketing/na/assets/im/decision-analytics/infographics/account-takeover-fraud-2020-infographic.pdf
6. Feedzai, 2020: https://thepaypers.com/digital-identity-security-online-fraud/fraud-rises-by-159-yoy-feedzai-report-shows--1249412
7. “Identity Theft Impacts Nearly Half of U.S. Consumers, Aite Group Report Finds,” Giact, https://www.giact.com/identity-theft-impacts-nearly-half-of-u-s-consumers-aite-group-report-finds/
8. “IBM Trusteer, 2020: https://securityintelligence.com/posts/massive-fraud-operation-evil-mobile-emulator-farms/
9. Aite Group, 2021: https://www.giact.com/identity-theft-impacts-nearly-half-of-u-s-consumers-aite-group-report-finds/
10. Sift, 2020: https://pages.sift.com/rs/526-PCC-974/images/ebook-digital-trust-and-safety-q32020-account-takeover-fraud.pdf
11. “Why mobile network operators are key to the success of a trusted digital identity, Idemia, https://www.idemia.com/news/why-mobile-network-operators-are-key-success-trusted-digital-identity-2020-07-17
12. “Out-of-Band Authentication,” Onespan, https://www.onespan.com/topics/out-of-band-authentication
13. “Early Days Authentication Did Not Have Mobile Payments In Mind,” 3DSecure2, https://3dsecure2.com/
14. “The Dawn of a New Era in eCommerce Authentication,” GPayments, https://www.gpayments.com/about/3d-secure-2.0/
15. “Digital Onboarding and KYC Report 2020,” The Paypers, https://thepaypers.com/reports/digital-onboarding-and-kyc-report-2020/r1240850
16. “Mobile Identity Enabling The Digital World,” GSMA, https://www.gsma.com/identity/wp-content/uploads/2020/07/Mobile-Identity-enabling-the-digital-world-report-Final-1.pdf
17. “Mobile Identity Enabling The Digital World,” GSMA, https://www.gsma.com/identity/wp-content/uploads/2020/07/Mobile-Identity-enabling-the-digital-world-report-Final-1.pdf
18. “Could eSIM technology make your smartphone less secure?,” Fierce Wireless, https://www.fiercewireless.com/tech/could-esim-technology-make-your-smartphone-less-secure
19. “Financial fraud is a global issue and it’s getting worse says PwC,” Wealth Professional, https://www.wealthprofessional.ca/news/industry-news/financial-fraud-is-a-global-issue-and-its-getting-worse-says-pwc/327030
20. “How banking will change after COVID-19,” HSBC, https://www.hsbc.com/insight/topics/how-banking-will-change-after-covid-19