Aite PARTNER. ADVISOR. CATALYST.

Trends in Account Takeover Fraud for 2020 and Beyond

JANUARY 2020

Prepared for:

NuData Security

mastercard

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

- This paper will examine the evolution of account takeover (ATO) tactics over time. It emphasizes the factors that have contributed to the most recent attack patterns, which have proved to be a particularly troublesome challenge for some financial institutions (FIs).

- Early ATO attack patterns and their negative impacts were limited in scope because the information required to provision the crime was expensive, and the resources required to commission the crime were challenging to orchestrate relative to payment-instrument fraud, such as card and check fraud.

- Chief among the catalysts of changing ATO tactics were the EMV chips designed to thwart one of the most popular forms of payment-instrument fraud: counterfeit card fraud.

- A series of events, including the disruption of the increasingly sophisticated value chain that fraudsters use to mine and enrich the information they require to commission their trade, transpired to transform their tactics in such a way that would make ATO fraud an easier and more cost-effective crime to commit.

- Another of the events that helped to transform changes to ATO tactics was the trend among banks to aggressively expand digital sales and service platforms as well as innovations in person-to-person (P2P) payment services that created more appealing targets for fraudsters’ more sophisticated and automated attacks.

- The most recent evolution of ATO attack patterns suggests that fraudsters are shifting their tactics to rely on more sophisticated automation tools that have enabled them to significantly increase the volume of attacks on victim accounts and also on the creation and usage of mule accounts. The industrial scale of these tactics has recently proved to be a particularly challenging problem for FIs that are not adequately prepared.

- Among the lessons learned from the most recent trends in ATO is the value of fortifying authentication controls, automating claim intake and case management processes, stress-testing staffing models, engaging proactively with clients about security hygiene, and reexamining payment monitoring controls at the network layer and for those banks on the receiving end of the payment.

INTRODUCTION

ATO fraud has been a growing concern among many fraud leaders across the industry for the past few years, and for good reason. It is a peculiar and particularly unsettling form of attack, and one that has evaded a standardized definition. It is, thus, poorly measured. It almost has a mythical quality about it. It’s a boogeyman that inspires a kind of irrational fear, mainly because it’s become increasingly clear just how difficult it is to accurately detect and prevent these attacks. This is especially true when FIs’ adversaries have so many resources at their disposal to overcome the fragmented and disconnected identity-proofing controls most FIs rely on as countermeasures. This disconnection of the tools used by FIs helps perpetuate the problem.

This white paper traces the trajectory of ATO tactics from their origins to their most recent manifestation and places an emphasis on the characteristics and implications of the latest trends in attack patterns observed in the U.S.

METHODOLOGY

This white paper is based on the author’s past experiences as a fraud strategist for a top 20 U.S. bank and as a member of banking industry working groups on fraud. It is also based on interviews with fraud executives from U.S. banks conducted in April and October of 2019 as well as forensic analysis of attack patterns made available by NuData Security in December 2019. It does not contain any confidential information about impacted banks, networks, or related organizations.

THE MARKET

Various characteristics of ATO tactics have evolved over time, but none more so in recent months than the scale and scope of attack patterns. These changes in tactics have the potential to shift the distribution of fraud activity (and losses) across the industry as fraudsters innovate their methods for automating their attacks through expanded use of more sophisticated bots to aid them in their efforts to compromise the security of victim accounts and to facilitate the creation of mule accounts. FIs must work to diagnose and remediate gaps in their control frameworks to counter both these trends and those that they foreshadow as faster payments continue to evolve, or they will be more likely to suffer increased fraud loss, increased attrition and erosion of market share, and increased mule activity leading to reputational risk (Table A).

Table A: The Market

Market trends	Market implications
Fraudsters' greater reliance on tools that automatically penetrate authentication controls to grant them access to a victim's account as well as on the information and tools used to mass-produce mule accounts is impacting how banks control identity authentication and verification.	Additional layers of defense are required to provide more sophisticated methods for authenticating and verifying the identity of account access and account creation. Those FIs that fail to keep their identity authentication and identity verification controls up to date and capable of leveraging the latest countermeasures, such as device profiling, mobile network operator (MNO) matching, and behavioral analytics, are likely to suffer disproportionately in terms of attack rates and losses.
The scope and scale of ATO attacks are growing significantly.	FIs that lack automated claim intake and case management processes as well as those that have not stress-tested and hardened their staffing models and quality control processes will risk increased fraud losses, increases in attrition, and increased reputational risk.
The surplus of personally identifiable information (PII) has enabled fraudsters to build large inventories of drop accounts.	The inability to move large quantities of stolen money from victim accounts to accounts that are controlled by fraudsters (drop accounts or mule accounts) no longer represents a bottleneck in fraudsters' ability to scale up their operations.
The automated tools that fraudsters use to penetrate victim accounts are enabling this growth.	FIs that are not aware of gaps in their authentication control framework and that fail to remediate them are at high risk of suffering increases in ATO attack rates.
Large ATO attacks can be exceptionally disruptive to operational efficiency and client experience.	Stress-testing and automating fraud claim intake and case management processes as well as proactively engaging with clients to more deliberately control high-risk behaviors can be effective ways to mitigate or attenuate the negative impacts of significant increases in ATO attacks.

Market trends	Market implications
Industrial-scale ATO attack patterns challenge the conventional wisdom that more sophisticated payment monitoring controls at the network layer or at the receiving bank are not required.	While neither the network nor the receiving bank will suffer from changes to the risk of liability for financial loss resulting from a disputed transaction, the increases in frequency and severity of fraudulent payments from ATO attacks place the network and the receiving bank at increased risk of reputational damage or the erosion of market share due to increases in attrition.

Source: Aite Group

EARLY DAYS: A COTTAGE INDUSTRY

While ATO fraud was still a spooky thing in the early days of its evolution, it was, thankfully, well contained relative to card and check fraud. The primary reason for this was economic. The raw material required to commit card fraud or check fraud was plentiful and, therefore, inexpensive, whereas the supply of a full (or even partial) identity package was relatively limited. Perhaps more importantly, the cost, effort, and risk required to acquire control of an account prior to the expansion of digital services in the early 2000s was substantial compared, again, to the effort required to purchase and use a counterfeit card or check.

A typical attack required a great deal of planning and, prior to the widespread deployment of online banking, a lot of social engineering typically targeting the call center or branch. Compared to card or check fraud, it was labor intensive and required substantial resources to coordinate, especially when it came time to cash out. Setting up a mule account for capturing and distributing the stolen funds wasn’t unheard of in those days, nor was it as common as it is today, thanks largely to the relative dearth of raw material required to commission identity fraud. When an attack did occur, however, it was difficult to detect and prevent. If they weren’t detected early, ATO attacks usually resulted in larger dollar losses than card and check fraud.

From a client experience perspective, ATO fraud more frequently results in a customer either diminishing the banking relationship (e.g., maintaining a mortgage account but moving deposits elsewhere) or terminating it than do other types of fraud. The root cause of this has yet to be empirically proved, but intuitively, consumers may be less likely to hold their bank accountable for data breaches that occurred at a merchant that they shopped with because the numbers of third-party breach announcements made in the media over the past decade have desensitized them to the risks of payment-instrument fraud. Conversely, if a customer’s bank account was compromised (even if it was the result of the customer’s own poor security practices, such as using the same username and password as for other, less-sensitive sites) and a fraudulent payment was made from the compromised account, the consumer may perceive that the bank failed to adequately secure the account.

THE VALUE CHAIN OF FRAUD INC.

In the early 2000s, more and more elements of consumers' identities began to populate the vulnerable databases of the rapidly expanding commercial interests on and off the web. It didn't happen overnight, but increasing numbers of companies were demonstrating that consumers' static and digital identity data was emerging as an exceptionally valuable and quantifiable asset. And yet fraudsters seemed slow to adopt ATO fraud as a preferred tactic, at least in such a way that reflected a wholesale shift in their attack patterns.

Most fraudsters remained loyal to conventional forms of payment-instrument fraud. **Error! Reference source not found.** illustrates the economics at work from the fraudster's perspective as well as how these dynamics influenced trends in their attack patterns—a conceptual model of the fraud value chain. The barriers to entry and the costs of commission for conventional instrument takeover fraud (notably card and check fraud) were still small and, thanks to a process for mining raw material that was reaching industrial proportions, were getting smaller, especially compared to the relatively time-consuming and labor-intensive work still required for ATO. The distribution capabilities of Fraud Inc. were geared for mass production of instrument fraud, and there was still a lot of room for expansion. That was, of course, until EMV came along.

Figure 1: Fraud Inc. Value Chain

Mining raw material

- Instrument data (e.g., card numbers, account/routing numbers)
- Credentials (e.g. username and passwords)
- PII (e.g., name, address, phone numbers)

Manufacturing and distribution

- Aggregation of data elements from multiple breaches and data sources
- Augmentation and enrichment from social media and public documents
- Online marketplaces with competitive product management

Compromise and theft

- Account takeover (e.g., P2P, online/ACH, card and check intercepts)
- Fraudulent account application (application fraud)
- Instrument fraud (e.g., card fraud, check fraud)
- Scams (e.g., business email compromise, romance, lottery)

Money movement and cash out

- Mule/drop account application and funding from compromised or confederate accounts
- Electronic funds transfers via ACH, wire, or RTP
- Payments via debit card, ATM, over-the-counter, checks, or payment service (e.g., P2P payment systems)

Source: Aite Group

EMV CATALYZED THE FIRST SHIFT

The deployment of EMV was, in the opinion of many fraud executives, one of the most significant catalysts to trigger a shift in fraudsters' tactics because it threatened to virtually eliminate a significant chunk of revenue generated by counterfeiting cards.[1] This disruption to the value chain was significant enough to motivate some criminals to consider alternative tactics.

Check fraud certainly enjoyed a renaissance during this time, as some fraudsters migrated from one type of instrument fraud to another. This shift from card to check fraud disrupted the

[1] See Aite Group's report *EMV: Issuance Trajectory and Impact on Account Takeover and CNP*, May 2016.

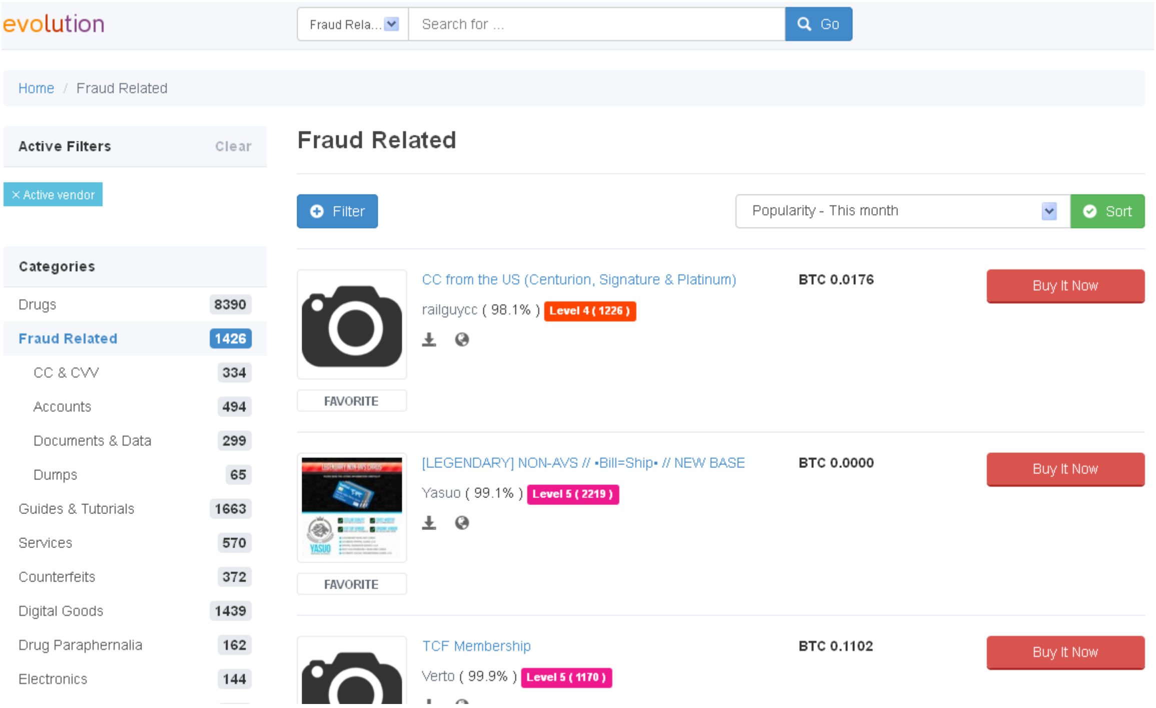
economic model by sparking an increase in demand for identity data that, for first-party check fraud, was required to defeat identity verification controls for new deposit accounts and, for third-party check fraud, was required to defeat identity authentication controls for check cashing. The challenge facing fraudsters looking to commit both first-party and third-party check fraud was scalability. At this point, the supply of identity packages was still relatively small and unsophisticated, which made mule accounts expensive and rare relative to today's costs and inventories.

First-party check fraudsters had the added challenge posed by the growth in the adoption of risk models used to automate the application of funds availability policies between 2010 and 2015. Regardless, the shift in tactics from card counterfeiting to check fraud was driving an increase in demand for the raw material necessary to defeat the banks' identity verification and authentication controls.

THE UNHAPPY COINCIDENCE OF AN INCREASE IN SUPPLY

The many online marketplaces that traded in stolen instrument data had also enjoyed an epic windfall of what was, until this time, thought of as more of a byproduct of the industrial-scale card data mining process: PII. It didn't take long for fraudsters' marketplaces on the dark web to ramp up production of "fullz," a slang term for a complete package of all the information about an identity that a fraudster would need to open a fraudulent account or to begin a campaign to compromise an existing account. Prior to being shut down in 2015, Evolution was one of many examples of online marketplaces on the dark web that traded in the raw materials required for committing fraud (Figure 2).

Figure 2: Dark Web Marketplaces



Categories	
Drugs	8390
Fraud Related	1426
CC & CVV	334
Accounts	494
Documents & Data	299
Dumps	65
Guides & Tutorials	1663
Services	570
Counterfeits	372
Digital Goods	1439
Drug Paraphernalia	162
Electronics	144

Fraud Related

CC from the US (Centurion, Signature & Platinum)
railguycc (98.1%) Level 4 (1226)
BTC 0.0176
Buy It Now
FAVORITE

[LEGENDARY] NON-AVS // •Bill=Ship• // NEW BASE
Yasuo (99.1%) Level 5 (2219)
BTC 0.0000
Buy It Now
FAVORITE

TCF Membership
Verto (99.9%) Level 5 (1170)
BTC 0.1102
Buy It Now

Source: Krebs on Security

Perhaps more consequentially, those same marketplaces also began to introduce innovations and value-added services. The information contained in the initial breach may have been limited to core data elements of the identity, such as name, address, and phone number. As this information was necessary but not sufficient for fraudsters to open a fraudulent account, many enterprising marketplaces began to assemble and aggregate elements of the identity from a wider variety of sources, including other breaches as well as social media and public documents. In doing so, they would enable the fraudster to have a relatively turnkey product that made compromising an existing account or opening a new fraudulent account easier.

THE ERA OF THE INDUSTRIAL-SCALE ATO ATTACK

While the fraudsters were amassing inventories of consumer identity data and credentials, ATO tactics during the late 2000s were predominantly focused on leveraging malware and phishing attacks to expose credentials and other useful information needed to compromise corporate and business accounts. The use of malware and phishing techniques (to say nothing of the ever-present use of social engineering techniques) exposed gaps in the authentication and transaction monitoring control frameworks that were (and in some cases continue to be) divided between wholesale, wealth, and consumer service delivery channels. It was a useful, if costly, period for absorbing lessons in how to control threats such as Zeus (a wildly popular malware application) with solutions such as endpoint malware detection and blocking controls on digital wholesale banking portals.

While many of the controls that were particularly effective at combatting these attacks have not only persisted but also migrated across channels and lines of business, FIs continue to underutilize some others, such as more proactively and deliberately engaging with clients on adopting better security practices as well as multifactor authentication. Nowhere is this more evident than with the significant growth in scam tactics, such as business email compromise (a particularly pernicious form of ATO).

By 2015, check and deposit fraud was resurgent, and ATO fraud, while still relatively rare in terms of incident rates compared to card and check fraud, was gaining in frequency and severity. While ATO fraud takes many forms and definitions from institution to institution, the form that most fraud executives agree was the most notable in terms of its surge in frequency immediately after online banking services proliferated was “online fraud.” An entire report could be dedicated to the topic of fraud event taxonomy (or even ATO fraud taxonomy), but for the sake of brevity, this paper will summarize online fraud as any fraud event that resulted from unauthorized access to an online banking profile.

The increase in online fraud was driven (as it continues to be today) by a mandate to better meet the substantial transformation of client expectations following the rise of online banking services. Deploying innovative digital services continues to be a top priority among banks that seek to compete with other banks and with emerging fintech challengers in the marketplace. Innovations in P2P payment services, though thoughtfully controlled by the networks, have played a significant role in the changes to ATO tactics as well as the amplification of ATO attack rates. Though the vulnerabilities to these innovations are largely the result of gaps among the member banks on the network, it is, nonetheless, an excellent illustration of how innovations that are meant to transform the client experience are altering the risk landscape by introducing incentives (in this case, easier and faster money movement tied directly to a deposit account) for fraudsters to challenge and overcome ATO controls.

Fraudsters’ targeting of P2P payment services marked the first milestone in what might be called the era of the industrial-scale ATO attack. As discussed earlier, early ATO attacks (primarily in the form of online fraud) were relatively tightly scoped in terms of the number of victim accounts that were targeted. The convenience of being able to move money directly from the victim’s deposit account and to do it quickly were significant factors in expanding the scale of attacks. Perhaps the most significant driver, though, was the growing ubiquity of P2P payment services.

The ease and availability of so many services that made it easier and more expeditious for fraudsters to move stolen funds from the victim's account to a safe location where they could reliably cash out proved to be appealing to fraudsters. The operating theory is that the fraudsters had prepared for and timed their ATO attacks by stockpiling an inventory of the credentials or identity packages necessary to fuel automated attempts to probe and then penetrate the online or mobile accounts of victim clients, and that they coordinated their attacks to route the fraudulent payments to a large inventory of mule accounts that were similarly planned and accumulated.

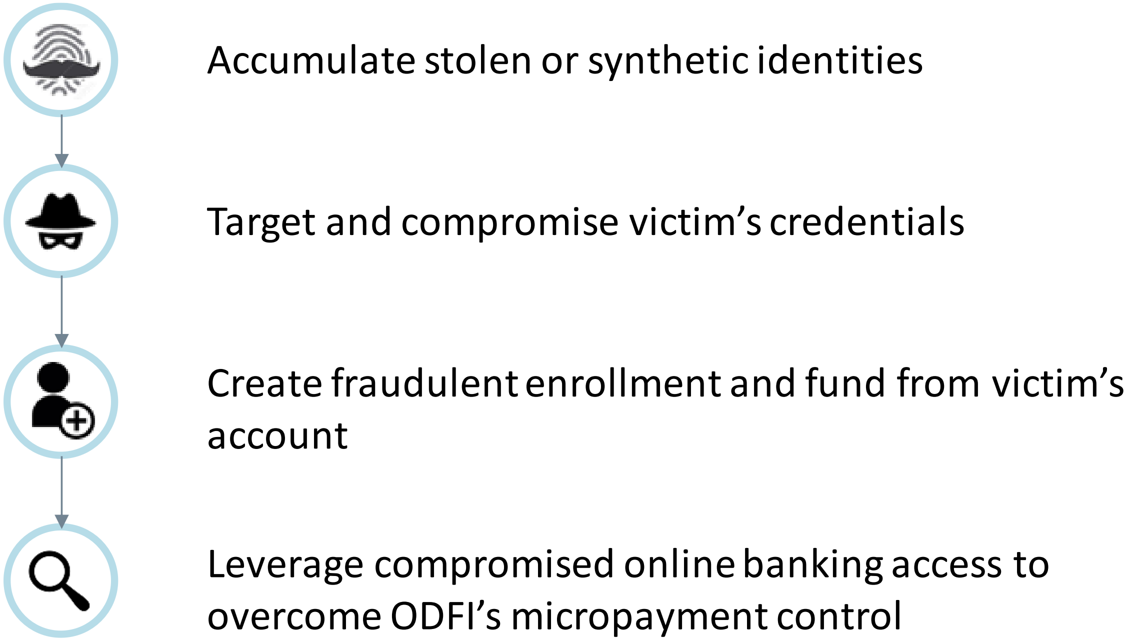
Considering the amount of coordination to orchestrate the many moving parts of multiple waves of fraud attacks across the growing number of banks on emerging P2P networks, it came as little surprise to many fraud executives that most of the fraudulent activity could be traced back to rings operating out of Nigeria and Eastern Europe. The similarity of tactics and the scale of the attacks reflected a much more organized and well-prepared operation than could be said of thousands of unconnected individuals acting independently. It was this characteristic that marks the next big shift in ATO tactics: the emergence of organized, well-prepared ATO attacks across a much broader scale of victims, coupled with similarly large-scale money movement and cash-out tactics.

APPLYING INDUSTRIAL SCALE TO CONVENTIONAL TACTICS

By mid-year 2019, most large banks were hard at work to compensate for the increased ATO activity resulting from the proliferation of P2P payments. While most have made the necessary adjustments to their control frameworks and are well on their way to compensating for the increased activity, there is evidence that the fraud rings have adapted the tactics that worked so well on P2P payments to ACH payments. Starting in October 2018, a handful of U.S. banks began to see significant increases in online fraud claimants reporting that sizeable portions of their deposit accounts had been lost to unauthorized ACH payments. Around the same time, a subset of a broader range of FIs, payments services such as PayPal and Venmo, and merchants began noticing an unusually high volume of ACH returns from what was, at first, only a few banks.

Each side of the disputed ACH payment (the originating depository financial institution, or ODFI, and the receiving depository financial institution, or RDFI) began conducting forensic examinations of some of the fraudulent payments to diagnose the root cause of the spike in activity. The results among some of the impacted banks revealed that the attackers were using conventional ATO tactics that were similar to garden-variety online fraud attack patterns (Figure 3) except in one important regard: the scale of attack volume. The attack patterns resembled the scale of attack volume seen on P2P payments, but instead of seeking to make one or two fraudulent P2P payments, they were taking larger dollar amounts. In some cases, if external transfer limits allowed it, the fraudsters were able to drain the account to the penny.

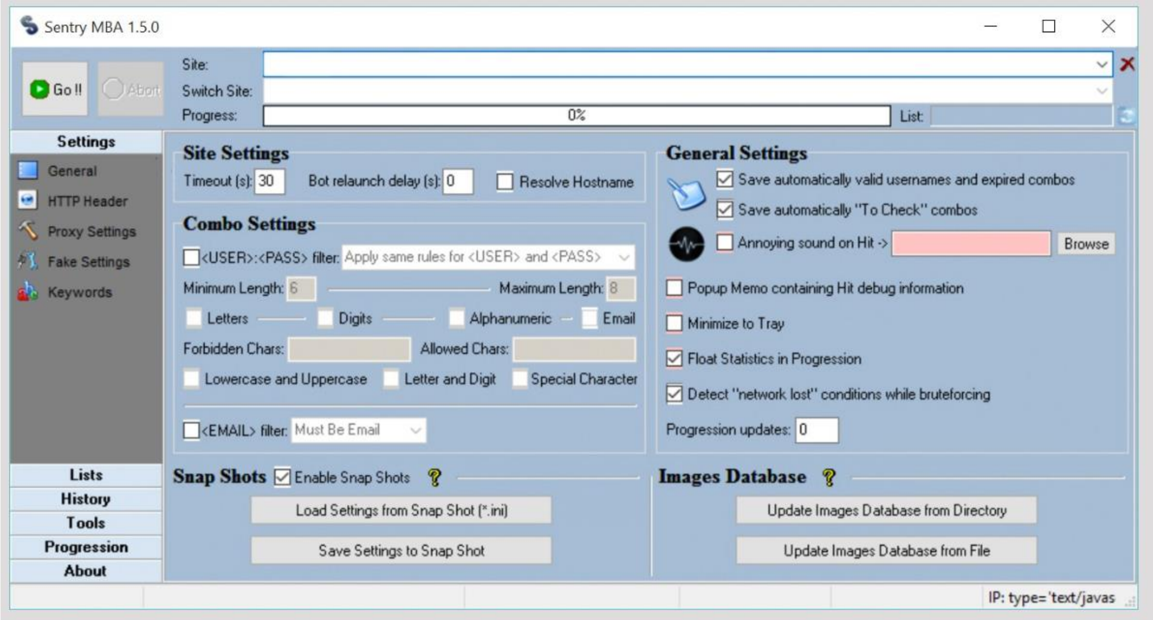
Figure 3: A Garden-Variety Online ATO Fraud Attack


Accumulate stolen or synthetic identities
Target and compromise victim's credentials
Create fraudulent enrollment and fund from victim's account
Leverage compromised online banking access to overcome ODFI's micropayment control

Source: Aite Group

Prior to this spike in activity in late 2018 and early 2019, these kinds of ATO attacks were relatively isolated and came at predictable rates. As discussed earlier, this was predominantly because scaling up this kind of activity required a level of organization and coordination that didn't exist prior to the P2P attacks. Specifically, the ring would have to make preparations for both sides of the payment. On the victim side, the fraudsters would need the credentials and an automated means of first probing and then compromising the victim's account, such as a credential stuffing tool like Sentry MBA (Figure 4). Credential stuffing is a technique that fraudsters use to automate login attempts to a website using long lists of compromised username and password combinations, usually purchased from dark-web marketplaces.

Figure 4: A Common Credential Stuffing Tool—Sentry MBA



Site Settings

Timeout (s): 30 Bot relaunch delay (s): 0 □ Resolve Hostname

Combo Settings

□ <USER>:<PASS> filter: Apply same rules for <USER> and <PASS>

Minimum Length: 6 Maximum Length: 8

□ Letters □ Digits □ Alphanumeric □ Email

Forbidden Chars: Allowed Chars:

□ Lowercase and Uppercase □ Letter and Digit □ Special Character

□ <EMAIL> filter: Must Be Email

General Settings

☑ Save automatically valid usernames and expired combos

☑ Save automatically "To Check" combos

□ Annoying sound on Hit -> Browse

□ Popup Memo containing Hit debug information

□ Minimize to Tray

☑ Float Statistics in Progression

☑ Detect "network lost" conditions while bruteforcing

Progression updates: 0

Snap Shots ☑ Enable Snap Shots

Images Database

Source: Shape Security

On the mule side, they would need to ensure that they had a reliable and robust inventory of drop accounts to receive the stolen funds, and then they'd require a way to quickly and effectively cash out those funds without raising suspicion.

ESSENTIAL CONTROLS TO DEFEAT ATO

There is little doubt that the role of automation tools such as Sentry MBA have made a profound impact on fraudsters' ability to scale up their attacks on victims' accounts as well as on their ability to open up a large-scale inventory of mule accounts used to support the movement of unauthorized payments, regardless of whether they're riding on P2P or conventional payment rails such as ACH or even wire. There is also consensus that the policy of "defense in depth" remains the dominant philosophy guiding most FIs' fraud strategy. The question comes down to whether the FI has added the layers of defense necessary to plug gaps in its control framework that fraudsters are exploiting to gain unauthorized control of victims' accounts on the RDFI's side and to create mule accounts on the ODFI's side.

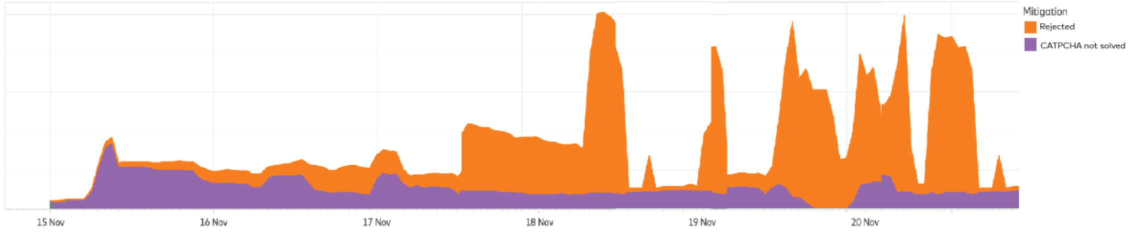
A more detailed examination of recent trends in attack patterns reveals that having the right controls that are capable of accumulating, parsing, and assessing the risk of a broad spectrum of signals in digital traffic can go a long way in boosting the effectiveness and accuracy of ATO detection. The attack patterns also reveal just how sophisticated the attackers have become in terms of masking their activity and making the adjustments necessary to dynamically probe defenses for the purposes of finding and exploiting vulnerabilities. So while it's necessary to have the capability to accumulate the signals and to take action on them based on a single attack pattern profile, it's not sufficient to keep pace with the rate of change in attack patterns. In order to do that, it's also necessary to be aware of subtle but significant shifts in how they're seeking to circumvent detection logic and to have the capacity to rapidly make adjustments to detection logic.

Recent analysis of ATO attack patterns reveals that fraudsters have been adjusting the configuration of the tools they use to automate attempts to create mule accounts. These are known by fraud executives as “bot attacks,” for which the term “bot” refers to the automated tool that fraudsters use to fill out account-opening web forms as a robot, or “bot” for short. Basic bot attacks are relatively easily discovered by behavioral biometric detection solutions. The solution analyzes the signals that exist within the stream of data captured by the server that manages the web traffic on the FI’s website. Specifically, the solution looks for factors such as the rate at which users type their information—e.g., name, address, and phone number—into the FI’s web-based account application form. Basic bot attacks are easy to spot because they usually don’t bother to try to emulate human behavior. The basic bot pastes data from a database of compromised identities into the corresponding form fields in an exceptionally rapid sequence of events that easily shows up in the web server’s logs.

More sophisticated bots deploy java script code that seeks to emulate a human—typing the information into the form fields as opposed to pasting it into the fields in rapid succession. While tools that have this capacity to emulate human behavior are useful in fooling more basic behavioral biometric fraud detection solutions that only measure the overall time to complete the task of filling out a web form, they don’t fare so well against more sophisticated behavioral biometric solutions like NuData that examine the cadence of typing to determine if it’s expected or not, for example. The fraudsters have responded to these more sophisticated behavioral biometric solutions by enhancing their tools, such as the Sentry MBA tool mentioned earlier, with the means to configure the java script code to introduce randomness into the cadence of “typing.” In their response to the fraudster’s escalation, behavioral biometric solution providers have responded by applying sophisticated analytical techniques, such as machine learning, to continuously analyze web logs from across the spectrum of their clients for the purpose of isolating subtle commonalities among behavioral characteristics that either result in fraud or that suggest inconsistencies with legitimate behavior. They employ teams of statistical and subject-matter experts in fraud detection to examine the results of what their risk models flag as potentially “out of pattern” to determine whether the anomalies justify a deeper analysis or testing.

Such was the case in November 2019, when NuData Security machine learning models flagged a variety of subtle but significant shifts in tactics. Further analysis revealed that a high rate of “input anomalies”—a term used to categorize anomalies in how a user inputs data into a web form—emerged rather rapidly within a subset of the population (Figure 5). The subtle changes in the events, including the behavior, pointed at a bot as the source of the flagged traffic. The model found these anomalies across a variety of indicators, such as the frequency or “velocity” of the attempts, the failure rate of attempts, the language settings of the device used, and the geolocation of the IP address of the device. These values combined created a user profile highly inconsistent with behaviors among legitimate traffic. Instead, these attempts were correlated with high risk activity, and the company was able to mitigate the attack. After NuData’s data scientists researched the anomalies with their clients they confirmed that the anomalies were highly correlated with fraudulent outcomes and they worked collaboratively with the clients who were impacted by these attacks to enable them to mitigate the attacks.

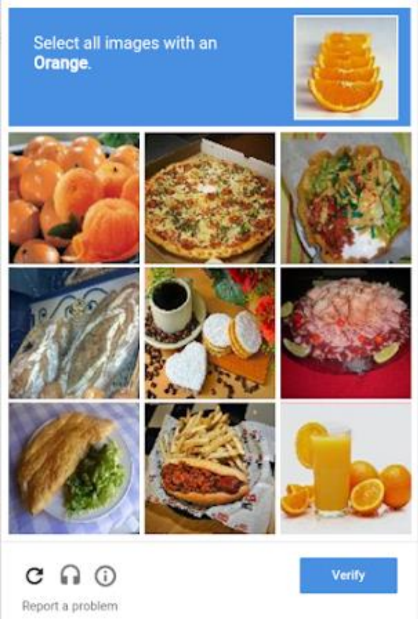
Figure 5: Emergence of Behavioral Features Related to “Input Anomalies”



Source: NuData Security

During the same time period, a similar shift in attack patterns was observed in attempts to overcome CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) controls that many web-based businesses deploy to thwart fraudulent enrollments or login attempts by bots. One example of a CAPTCHA includes displaying pictures of multiple objects in contiguous segments (Figure 6). Some of the pictures have a common subject, such as a car, in them, while others have similar objects, such as a pickup truck. The user is asked to click on the pictures that contain a truck. Until recently, bots were unable to distinguish between a car and a truck, so most would fail a CAPTCHA challenge.

Figure 6: Example of a Picture CAPTCHA



Select all images with an **Orange.**

Source: Google

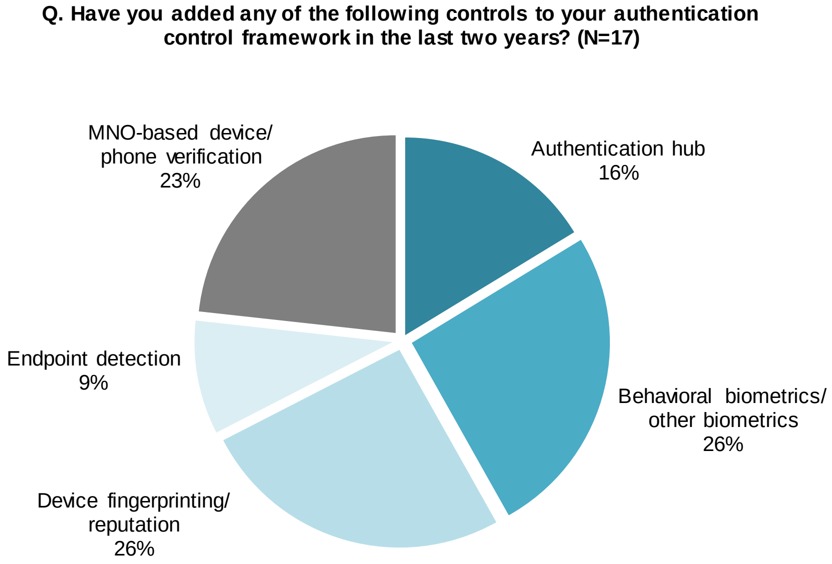
The recent shift that was observed indicated that fraudsters were increasingly able to automatically defeat CAPTCHA challenges. While some bots that are available for purchase come with the capacity to configure them in such a way that enables them to overcome some CAPTCHA defenses, they’re usually rare. An analysis of the shift in trends revealed that the fraudsters were likely leveraging human farms to overcome the CAPTCHA challenges. Specifically, the data indicated that the bot was redirecting the CAPTCHA challenge screen to another device and that the inputs that were supplied by the user of the redirected device were consistent with those made by humans. The data also revealed that multiple devices were being used for a single event, and that there was a high volume of events with similar profiles, displaying unusual behavior while solving a CATPCHA. While no forensic analysis has revealed empirical evidence of this, it's likely that the fraud rings are employing human farms—pools of inexpensive outsourced labor usually in foreign countries—to augment their automation tools to perform tasks that are designed specifically to thwart their automation.

IMPLICATIONS AND CONSIDERATIONS

As mentioned previously, perhaps the most striking characteristic of the shift in ATO tactics was the ambitious scale of it. Some of the affected banks suffered a 10-fold increase in incident rates. These impacts have multiple dimensions, but the operational efficiency and client experience implications are the most noteworthy.

Refreshing digital channel controls to ensure that gaps in their overlapping coverage are adequately addressed is imperative for fraud executives to ensure proper protection against ATO threats. Recent research with 20 fraud executives from 18 of the top 40 U.S. banks has revealed that almost all of them are in the process of deploying transformation initiatives to upgrade or augment existing digital fraud controls. Many of them, 26%, have deployed or are in the process of deploying behavioral biometric solutions (Figure 7) similar to those that have proven so useful in detecting the kinds of anomalies that would give away attempts by fraudsters' automation tools to penetrate victims' online or mobile profiles or in to create mule accounts.

Figure 7: Preferences for Digital Fraud Controls



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

Banks that lack automation in their claim intake and case management processes are likely to suffer more than those that have either the manpower or the automation necessary to absorb dramatic spikes in volume. Consumers are traumatized and highly agitated by fraud, but particularly so when their online profile has been compromised and significant portions of their deposit accounts mysteriously disappear via unauthorized ACH payments. As a result, when they call to report that their deposit account has been drained by an unknown assailant, it's not uncommon for them to require an explanation and to be "talked off the ledge" by a skilled agent. This translates to calls that are considerably more lengthy and more labor-intensive than those regarding a typical check- or card-fraud claim. When they exceed staffing model thresholds, increases in handle times translate to increased hold times and, if not planned appropriately, could cause contact center managers to struggle to redeploy resources on the fly. This would put yet more strain on an already volatile and highly unpleasant client experience and would affect other client-servicing operations and client-experience performance.

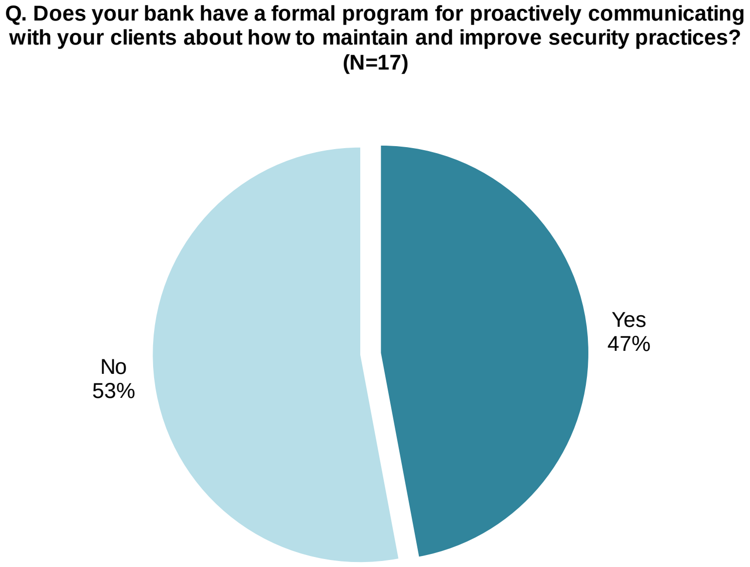
Because the root-cause diagnostics and remediation efforts to address gaps in the control framework frequently take days, weeks, or, in some extreme environments, months, the most viable (albeit unwelcome) option for many banks in circumstances such as this is to increase headcount. Unfortunately, for most small and midsize banks that manage their own contact centers, fielding new agents with the skills to effectively manage this kind of event can take as long as six weeks. This outcome would not only amplify the negative impact of operational efficiency but also prolong the effects of those impacts.

Another implication related to operational efficiency, particularly for banks that lack automation, is the impact to recovery rates stemming from missed deadlines for submitting recovery notices to the ODFI. As case volume increases and begins to overwhelm capacity, average cycle times grow longer, and the number of claims that age past their service-level agreements increases. Without stress-testing staffing models or incorporating redundancies and quality controls to safeguard against significant spikes in volume, it's possible that recovery rates would suffer and losses would increase.

Among the most valuable client-experience-related lessons learned from this recent trend has been the value of more deliberately and proactively controlling clients' proclivity to use the same username and password for their online banking profile as for other online services.[2] As the saying goes, "an ounce of prevention is worth a pound of cure," yet FIs prioritize client discussions meant to promote revenue-generating behaviors rather than proactive discussions about good security practices. For FIs that have not been targeted by this trend, that is a well-rationalized decision. But in the era of the industrial-scale ATO attacks, when it's possible to risk the termination of thousands of client relationships in the span of just a few weeks, that rationalization becomes less compelling. As the number of clients who have been impacted by fraud increases, there is mounting evidence that consumer clients (and, perhaps even more so, commercial clients) expect their bank to help them learn about security vulnerabilities that may leave them at high risk and the practices that they can adopt to mitigate these risks. This recent trend has served as a wake-up call to some and a reminder to many of the compelling return on the relatively small investment of proactively training clients on good security hygiene (Figure 8).

[2] See Aite Group's report *Global Consumers' Authentication Preferences: Have Your Cake and Eat It Too*, September 2018.

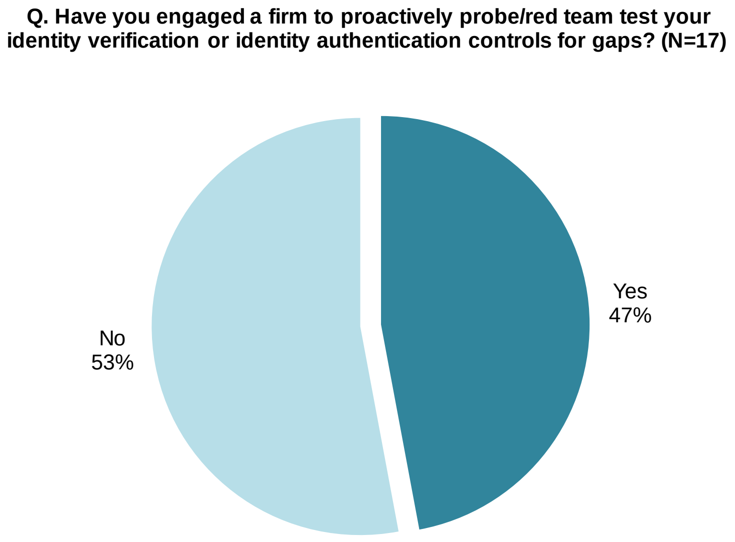
Figure 8: Proactive Communications



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

Another lesson learned that falls under the "preventive controls" umbrella is to take a close look at the effectiveness of authentication controls and whether their distribution across channels is consistent with the balance between client experience and loss mitigation. Are there gaps or inconsistencies in the FI's authentication control framework, especially around high-risk events or channels such as aggregators? Many FIs have discovered the value of red-teaming fraud controls (Figure 9), particularly for the purpose of identifying gaps in the identity authentication space. Such an effort, if scoped carefully, can be a relatively affordable and exceptionally effective way to reveal the "unknown unknowns" in the control framework. It's also the kind of exercise that could provide an FI with the knowledge and foresight to avoid exposing itself unnecessarily to this kind of trend.

Figure 9: Red Teaming



Source: Aite Group interviews with 20 fraud executives from 18 large North American FIs, July to October 2019

The last implication, also related to preventive controls, foreshadows the future of faster payments. Most FIs have either limited controls or no controls at all for outbound payments. Generally, this is a reflection of the network's policies governing liability in the event of disputed payments. The thinking goes that if the ODFI (in the case of ACH) is liable for the loss, then the onus is on it to control for the vulnerabilities that would lead up to an unauthorized payment. While many FIs are finding great value from investing in identity verification technologies, and some are even stitching together next-generation identity control hubs, it's clear from this recent trend that the battle to detect stolen or synthetic identities is far from over. This highlights the importance of efforts to design more controls at the network layer (such as those under consideration by The Clearing House for its RTP network) to monitor for indications of fraud that are made more evident when looking at the transaction in a way that enables banks to connect the dots more effectively than is possible from the originator's or the receiver's perspective. Additionally, it reveals the wisdom behind shifting emphasis on controls for outbound payments, such as the rule change Nacha has proposed, to clarify requirements for RDFI controls for monitoring web debit transactions.[3]

[3] "Supplementing Fraud Detection Standards for WEB Debits," Nacha, accessed June 11, 2019, https://www.nacha.org/rules/supplementing-fraud-detection-standards-web-debits.

CONCLUSION

The era of industrial-scale ATO attacks is here, and the table stakes for FIs to remain competitive in defending against the ever-evolving threat landscape are increasing. Here are some recommendations for fraud executives to consider in getting prepared to defend against the latest trends**:**

- Consider refreshing digital-channel user-verification controls, particularly those that have proven to be particularly effective at revealing anomalies in behavioral patterns that distinguish between legitimate identity authentication and identity verification events, and those that are the result of automation tools that are increasingly being leveraged by fraud rings.
- Consider revisiting your staffing models' parameters to accommodate significantly larger spikes in volume than conventional wisdom suggests. Industrial-scale ATO attacks are a thing, and if you're unprepared for a coordinated attack, it can severely disrupt operations and threaten thousands of relationships over a brief span of time.
- Revisit business cases supporting greater automation, particularly among your claim intake and case management investments. The impact resulting from these large-scale concentrated ATO attacks is significantly larger and has broader dimensions (particularly relating to market and reputational risk) than anything seen before, and it foreshadows what could happen as faster payments services gain adoption .
- Don't underestimate the value of the relatively small cost of proactively engaging with your clients about common security vulnerabilities and best practices for addressing them. This is particularly true of making deliberate efforts to control reused or exposed credentials that are vulnerable to automated penetration attacks. As is the case with revisiting business cases for claim and case management automation and stress-testing staffing models, the scale of the risks has shifted the equation in favor of making bolder investments in preventive measures.
- Get engaged in efforts by networks, including Nacha and TCH, as well as industry groups such as The Bank Policy Institute's BITS Fraud Reduction Working Group (BITS), the American Bankers Association (ABA), and The National Cyber Forensics Training Alliance (NCFTA), in advocating for the design and development of more holistic payment controls. These payment controls should provide a broader perspective on potentially unauthorized payments, whether or not there are provisions to protect against liability and regardless of whether they're not, strictly speaking, fraud controls. The fraudsters are counting on those who manage fraud and anti-money laundering in the banking industry to allow gaps in the collective control framework to persist. Let's not play their game.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Trace Fooshée
+1.857.406.3515
tfooshee@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com