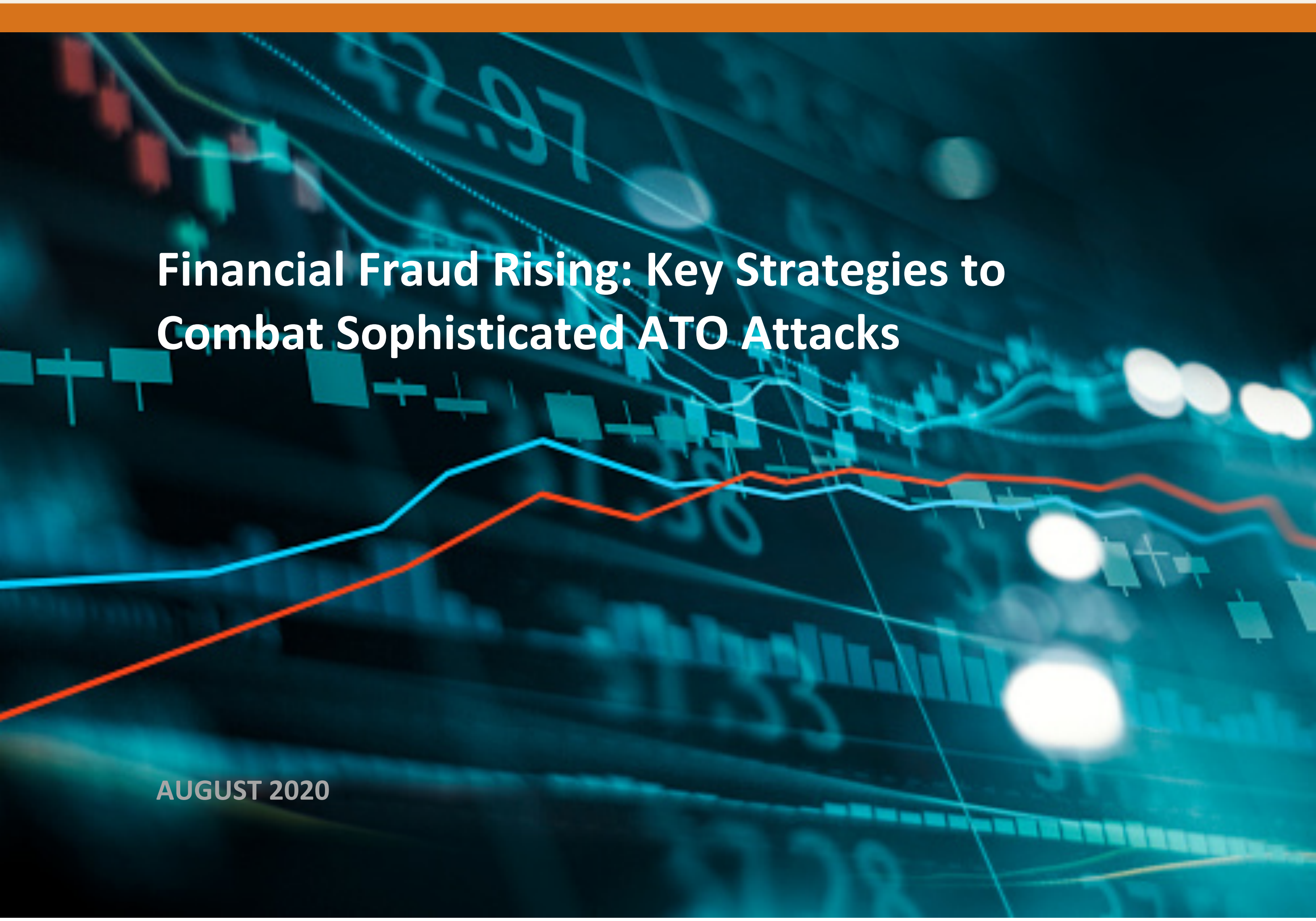
PARTNER. ADVISOR. CATALYST.



Financial Fraud Rising: Key Strategies to Combat Sophisticated ATO Attacks

AUGUST 2020

Prepared for:

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Financial Fraud Rising: Key Strategies to Combat Sophisticated ATO Attacks, commissioned by F5 and produced by Aite Group, addresses the rapidly increasing sophistication with which organized crime rings are targeting financial institutions (FIs), payment firms, and e-commerce merchants. It goes on to examine the ways in which these firms can fight back to turn the economics of the attack upside down and ward off the perpetrators.

Key takeaways from the white paper include the following:

- Organized crime rings have been targeting the banking and payments ecosystem with sophisticated and automated attacks for many years. Long gone are the days when sole operators were the primary drivers of fraud activity—now, the vast majority of fraud losses are the result of complex organized crime rings.
- Because the majority of consumers continue to use the same handful of usernames and passwords across all of the websites they interact with, credential pairs are particularly valuable to organized crime rings as they seek to maximize their post-breach monetization opportunities.
- After a breach, one of the first steps cybercriminals engage in is credential stuffing—the automated testing of breached credential pairs to find websites on which the consumer has reused them. One large-FI fraud executive interviewed by Aite Group says that for every good customer login his bank sees, there are 10 malicious attempts.
- As the attacks rapidly get more sophisticated, the available attack surface continues to expand, making the tasks of detection and mitigation that much more complex. This stems from a number of trends driving digital commerce, including the growth in digital users, the increased transactional capabilities in digital channels, the pressure for a seamless user experience, and the rapid growth of APIs as a means of data interactions.
- Rapidly escalating attack volume and sophistication, combined with the expanding attack surface, mean that it is imperative that firms deploy equally sophisticated defenses. Machine learning is a critically important component, as is consortium data. These enable businesses to harness internal and external data and apply advanced, iterative analytics to detect fraud and abuse.
- Time is money when it comes to fraud detection—a firm that can detect an emergent attack minimizes the impact. Organized crime rings also study their prey, and those firms with robust defenses will see attack volume decrease as criminals focus their efforts on easier targets.

INTRODUCTION

Within a short period of time, the global pandemic has dramatically shifted the way commerce is transacted. The online and mobile channels for banks and retailers alike are seeing sharp increases in transaction volume, as face-to-face commerce shifts to the digital channels. This increases the attack surface for the organized crime rings that have long been targeting these channels with advanced automated tactics. It also heightens the urgency of deploying technology that can detect sophisticated credential stuffing and API attacks while not unduly burdening the user experience.

This white paper discusses the myriad challenges risk executives face as they seek to address the escalating threat environment while at the same time ensuring a seamless customer experience. It then discusses the solutions available to help strike this balance. As criminals up the ante in the cybercrime arms race, it is important for firms to leverage equally sophisticated countermeasures, such as artificial intelligence and machine learning analytics.

METHODOLOGY

This research is based on ongoing Aite Group conversations with risk executives at financial institutions, fintech lenders, and e-commerce merchants.

ESCALATING ATTACKS, INCREASING TARGETS

Organized crime rings have been targeting the banking and payments ecosystem with sophisticated and automated attacks for many years. Long gone are the days when sole operators were the primary drivers of fraud activity. Now, the vast majority of fraud losses are the result of complex organized crime rings, with the ability to specialize functions and disperse their activities across multiple jurisdictions, which makes it very difficult for law enforcement to significantly impede their activities.

Data breaches are the fuel that power the crime rings' activity. One would think that breaches would be getting harder to perpetrate thanks to readily available technologies such as point-to-point encryption and tokenization, which can protect and devalue sensitive data. That is not the case, unfortunately—2019 alone saw 15.1 billion breached data records, a 284% increase from 2018.[1] These records include personally identifiable information, payment card numbers, and username/password pairs.

Because the majority of consumers continue to use the same handful of usernames and passwords across all of the websites they interact with,[2] credential pairs are particularly valuable to organized crime rings as they seek to monetize breaches. As of June 2020, login credentials for online banking averaged US$35 on the dark web, while payment card details averaged between US$12 and US$20 apiece.[3]

THE EVOLUTION OF CREDENTIAL STUFFING

After a breach, one of the first steps cybercriminals engage in is credential stuffing—the automated testing of breached credential pairs to find websites on which the consumer has reused them. In the early days of cybercrime, this was usually accomplished via simple kernel script routines that used aged credentials, so these attacks were fairly easily detected. The industry has seen a rapid evolution of this attack vector in recent years, however, with robust and sophisticated automated tools available for purchase at a reasonable price on the dark web.

To fraud prevention executives, this often feels like a lopsided game of chess, whereby the attackers get two moves for every one move by the good guys. One large-FI fraud executive interviewed by Aite Group says that for every good customer login his bank sees, there are 10 malicious attempts. Table A illustrates how the point-counterpoint between payment and banking firms and the crime rings attacking them have evolved and escalated in recent years. Figure 1 and Figure 2 illustrate examples of the attack tools that are available to crime rings.

1. "In 2019, a Total of 7,098 Breaches Exposed 15.1 Billion Records," Help Net Security, February 11, 2020, accessed July 10, 2020, https://www.helpnetsecurity.com/2020/02/11/2019-reported-breaches/.

2. See Aite Group's report *Second Annual Global Security Engagement Scorecard*, October 2017.

3. "How Much Is Your Data Worth on the Dark Web?," Help Net Security, June 19, 2020, accessed July 10, 2020, https://www.helpnetsecurity.com/2020/06/19/dark-web-prices/.

Table A: Fraudsters—Leveraging Technology to Gain an Edge

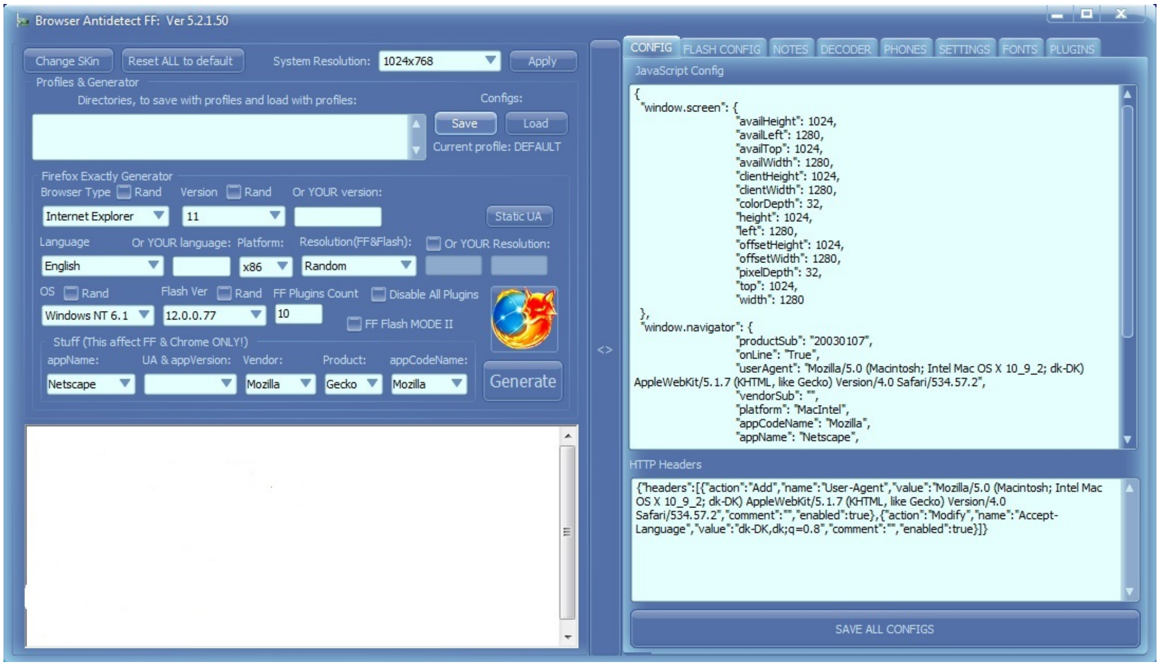
Defensive controls	Contravening attack methods	Description
IP velocity controls and CAPTCHA	Sentry MBA	As automated account takeover (ATO) attacks ramped up in the early part of the 2010s, many firms deployed IP velocity checks as well as CAPTCHA routines to detect and/or prevent these attacks. Sentry MBA is an automated tool that was rolled out by crime rings around 2015 with great success. It includes the ability to load vast numbers of compromised credential pairs and rotate the attacks through multiple IPs and proxies to bypass velocity controls. Sentry MBA has an optical character recognition (OCR) capability to defeat CAPTCHA and can moderate the attack velocity.
Device fingerprinting	Antidetect, FraudFox, and Genesis	Antidetect and FraudFox appeared in the dark web forums in the mid-2010s to help fraudsters bypass the device fingerprinting that is increasingly prevalent as a defensive control. These systems enable fraudsters to quickly and easily change their system components to fool device fingerprinting technologies, including configuration of browser type, language, operating system, time zone, etc. Genesis, a marketplace that emerged in 2018, takes device compromise to the next level. Genesis malware infects a victim's machine, then maps the attributes that comprise the user's device fingerprint. The device fingerprint is then sold in conjunction with the victim's login credentials to various online banking, commerce, and social media sites. Thus, when the attacker logs in using the victim's credentials and simulated device profile, it will defeat any device fingerprinting solutions that the firm has in place. Genesis also provides attackers a generator to enable them to create a completely new device profile.
Behavioral biometrics	Browser Automation Studio	Browser Automation Studio surfaced in late 2017 as a solution available on the dark web that allows attackers to combine emulated human behavior with CAPTCHA solving and proxy rotation.
User-centric controls	API and aggregator attacks	As more firms better protect their front-end applications from credential stuffing, attackers are increasingly targeting back-end APIs as well as the financial aggregators, such as Mint and Plaid. Banks interviewed by Aite Group indicate that they have been seeing rising fraud attempts via the aggregators over the past 18 months. In late 2019, NCR briefly blocked all traffic from the aggregators in response to a coordinated ATO attack on its Digital Insight banking platform.[4]

[4] "NCR Barred Mint, QuickBooks From Banking Platform During Account Takeover Storm," KrebsonSecurity.com, November 3, 2019, accessed August 5, 2020,

Defensive controls	Contravening attack methods	Description
Automation detection	Human click farms	In recognition of the fact that many firms have some level of defense in place to detect automated attacks, crime rings escalate to click farms, in which they employ workers to manually enter compromised credential data in an effort to evade detection routines looking for automated credential stuffing.

Source: Aite Group

Figure 1: Antidetect



System Resolution: 1024x768

Current profile: DEFAULT

Browser Type □ Rand: Internet Explorer
Version □ Rand: 11
Or YOUR version:
Language: English
Or YOUR language:
Platform: x86
Resolution(FF&Flash): Random
□ Or YOUR Resolution:
OS □ Rand: Windows NT 6.1
Flash Ver □ Rand: 12.0.0.77
FF Plugins Count: 10
□ Disable All Plugins
□ FF Flash MODE II
appName: Netscape
UA & appVersion:
Vendor: Mozilla
Product: Gecko
appCodeName: Mozilla

JavaScript Config

```
{
 "window.screen": {
                   "availHeight": 1024,
                   "availLeft": 1280,
                   "availTop": 1024,
                   "availWidth": 1280,
                   "clientHeight": 1024,
                   "clientWidth": 1280,
                   "colorDepth": 32,
                   "height": 1024,
                   "left": 1280,
                   "offsetHeight": 1024,
                   "offsetWidth": 1280,
                   "pixelDepth": 32,
                   "top": 1024,
                   "width": 1280
 },
 "window.navigator": {
                   "productSub": "20030107",
                   "onLine": "True",
                   "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2; dk-DK)
AppleWebKit/5.1.7 (KHTML, like Gecko) Version/4.0 Safari/534.57.2",
                   "vendorSub": "",
                   "platform": "MacIntel",
                   "appCodeName": "Mozilla",
                   "appName": "Netscape",
```

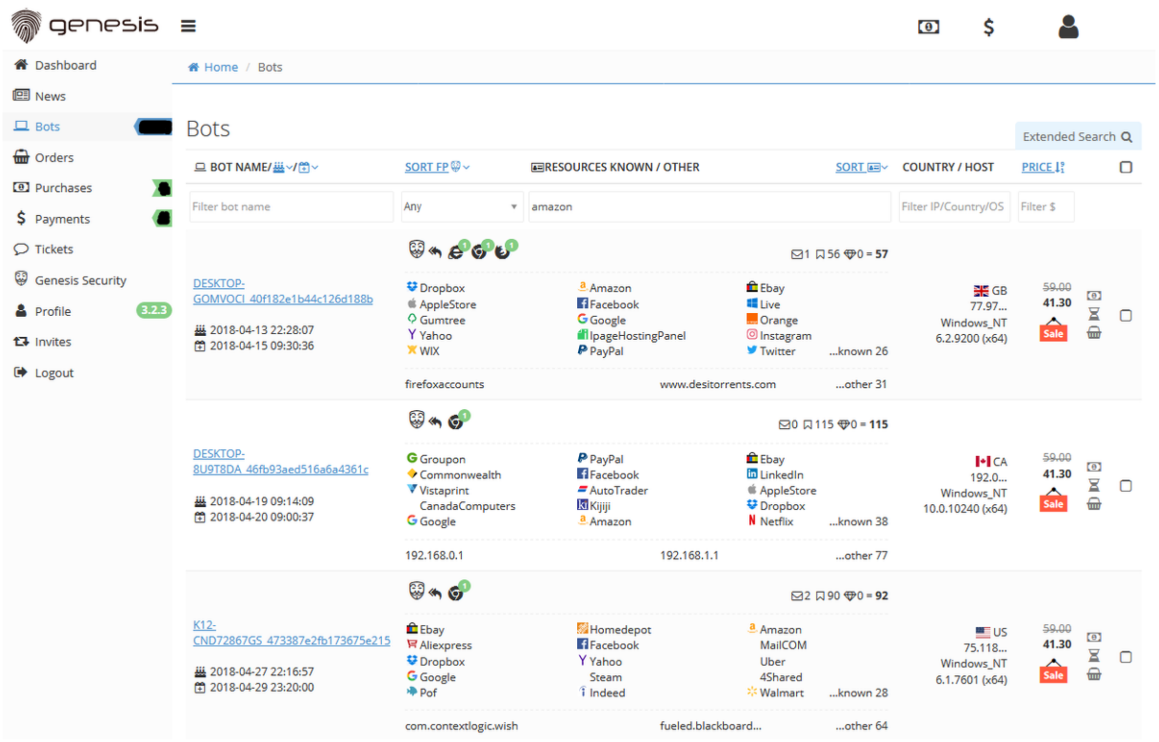
HTTP Headers

```
{"headers":[{"action":"Add","name":"User-Agent","value":"Mozilla/5.0 (Macintosh; Intel Mac
OS X 10_9_2; dk-DK) AppleWebKit/5.1.7 (KHTML, like Gecko) Version/4.0
Safari/534.57.2","comment":"","enabled":true},{"action":"Modify","name":"Accept-
Language","value":"dk-DK,dk;q=0.8","comment":"","enabled":true}]}
```

Source: Payhip.com

https://krebsonsecurity.com/2019/11/ncr-barred-mint-quickbooks-from-banking-platform-during-account-takeover-storm/#more-49409.

Figure 2: Genesis Marketplace



BOT NAME/	SORT FP	RESOURCES KNOWN / OTHER			SORT	COUNTRY / HOST	PRICE	□
Filter bot name	Any	amazon				Filter IP/Country/OS	Filter $	
DESKTOP-GOMVOCI_40f182e1b44c126d188b 2018-04-13 22:28:07 2018-04-15 09:30:36	Dropbox AppleStore Gumtree Yahoo WIX firefoxaccounts	Amazon Facebook Google IpageHostingPanel PayPal www.desitorrents.com	Ebay Live Orange Instagram Twitter	...known 26 ...other 31	1 56 0 = **57**	GB 77.97... Windows_NT 6.2.9200 (x64)	~~59.00~~ **41.30** Sale	□
DESKTOP-8U9T8DA_46fb93aed516a6a4361c 2018-04-19 09:14:09 2018-04-20 09:00:37	Groupon Commonwealth Vistaprint CanadaComputers Google 192.168.0.1	PayPal Facebook AutoTrader Kijiji Amazon 192.168.1.1	Ebay LinkedIn AppleStore Dropbox Netflix	...known 38 ...other 77	0 115 0 = **115**	CA 192.0... Windows_NT 10.0.10240 (x64)	~~59.00~~ **41.30** Sale	□
K12-CND72867GS_473387e2fb173675e215 2018-04-27 22:16:57 2018-04-29 23:20:00	Ebay Aliexpress Dropbox Google Pof com.contextlogic.wish	Homedepot Facebook Yahoo Steam Indeed fueled.blackboard...	Amazon MailCOM Uber 4Shared Walmart	...known 28 ...other 64	2 90 0 = **92**	US 75.118... Windows_NT 6.1.7601 (x64)	~~59.00~~ **41.30** Sale	□

Source: ZDNet

Another unfortunate side effect of these tools' increased sophistication and ability to bypass traditional controls is that they can significantly increase the time it takes an organization to realize it is under attack. Time is money in this case—the longer an attack goes undetected, the costlier it is to the targeted firm.

INCREASED TARGETS

As the attacks rapidly progress in sophistication, the available attack surface continues to expand, making the tasks of detection and mitigation that much more complex. This stems from a number of trends driving digital commerce:

- **Increase in digital users:** Consumers and businesses have been steadily migrating transaction activity to digital channels for years, and the pandemic has substantially accelerated that movement. Customers are forming new behavior patterns, many of which will persist once the crisis is past, as follows:
    - U.S. Bank stated that 75% of all service transactions and 46% of loan sales are taking place in digital channels in the wake of the pandemic, a significant

increase from 2019.[5] U.S. Bank executives further stated that they firmly believe these digital behaviors will persist after the pandemic is past.

  - Wells Fargo saw 340,000 customers newly enroll in digital banking during the first two months of the pandemic.[6]
  - Most FIs interviewed by Aite Group in Q2 2020 have seen a 250% increase in digital channel usage since March 2020.[7]

- **Increased use of APIs:** The movement to open APIs—driven by regulation in Europe and by market forces elsewhere—creates myriad new opportunities for fraudsters to exploit. Aggregators already leverage APIs as a back door into institutions for their data collection services, and many times key defenses, such as authentication and bot detection, are bypassed. Attackers recognize this and target the aggregators directly as well as deploy attacks that emulate aggregator behavior to backdoor their way into the FI.

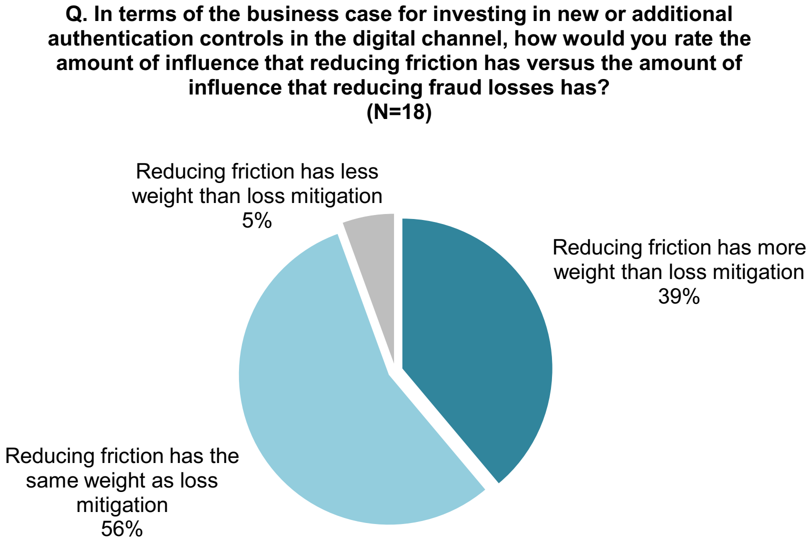
- **Increased digital channel functionality:** Not only are more consumers and businesses engaging with online and mobile channels, but they also expect a wide array of transactional capabilities in those channels. At the same time, a smooth and easy customer experience is viewed as a competitive differentiator. Among FI and merchant fraud executives interviewed by Aite Group, improving the customer experience is consistently one of the key business case drivers for enhancements to the anti-fraud control framework (Figure 3). They recognize that too much friction in the customer experience can drive current and prospective customers to competitors. That said, striking the balance between fraud mitigation and customer experience is not an easy task in the face of the sophisticated tactics used by organized criminals.

[5] "US Bancorp (USB) Q2 2020 Earnings Call Transcript," Motley Fool, July 15, 2020, accessed July 17, 2020, https://www.fool.com/earnings/call-transcripts/2020/07/15/us-bancorp-usb-q2-2020-earnings-call-transcript.aspx.

[6] Allissa Kline, "Banks Tore Up Digital Scripts Once Pandemic Hit," American Banker, May 13, 2020, accessed July 10, 2020, https://www.americanbanker.com/news/banks-tore-up-digital-scripts-once-pandemic-hit.

[7] See Aite Group's report *Workplace Distancing: Adapting Fraud and AML Operations to COVID-19*, April 2020.

Figure 3: Importance of Client Experience in Business Cases



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

ANSWERING FIRE WITH FIRE

Rapidly escalating attack volume and sophistication, combined with the expanding attack surface, mean that it is imperative that firms deploy equally sophisticated defenses. The crime rings are largely motivated by profit, and if a target is too difficult to compromise profitably, they will quickly move on to the next in line. Successful identification of bot activity not only reduces fraud but also diminishes impacts to server capacity and response time, since malicious bots represent a significant drain on these resources.

The good news is that the customer's digital identity data available to FIs, merchants, and payment firms is a key asset in this fight against cybercriminals, if properly harnessed and analyzed. Artificial intelligence and machine learning technologies are critically important components to this control framework. They enable businesses to harness internal and external data, and apply advanced, iterative analytics to detect fraud and abuse.

To stop and address credential stuffing and API attacks, it is important to look for solutions that can employ advanced analytics to understand the context, behavior, and reputation of inbound transaction requests. Key elements to look for in these solutions follow:

- **Transaction analysis:** Analytics should be able to analyze inbound transaction requests in real time to determine risk, including network, activity, user, device, and account factors. Supervised machine learning is an important component to these models, learning from prior attack patterns, but unsupervised analytics are also an important component, since attack patterns evolve rapidly. And analytics need to be in place to detect anomalies from the baseline of good user behavior. Best-in-class solutions not only will be able to detect automation but also should be able to highlight indicators of human-powered click farm attacks.

- **Consortium data:** This is another key input—the hive mind is critically important in detecting and mitigating fraud, since crime rings usually do not target their activity against any one victim.

- **Appropriate friction:** While firms seek to minimize friction and create a positive customer experience, a certain level of friction is appropriate for certain borderline transactions. Best-in-class solutions provide firms with the ability to minimize friction for the majority of the population but invoke stepped-up controls where appropriate.

CONCLUSION

Organized crime rings will continue to enjoy their advantage in the lopsided chess game, but more firms are investing in sophisticated technology that will checkmate their attackers. This highlights the importance of making sound decisions when choosing how to combat the rapidly escalating threat of credential stuffing and API abuse. Here are a few recommendations:

- **Look for solutions that can detect and deter automated attacks.** Organized crime rings' automated attacks will only get more sophisticated. This not only impacts fraud losses and customer experience but also exerts a marked drain on ancillary metrics, such as server capacity and response time. Firms need a solution that can leverage data analytics in real time to keep pace with automated attacks, detect the diversion of these attacks to click farms, and block malicious activity before it affects the business.

- **Disrupt the economics.** Organized crime rings are motivated by profit. Those firms with robust and sophisticated defenses will see attack volume decrease as criminals focus their efforts on easier targets.

- **Knowledge is power—look for solutions that have a consortium data component.** Crime rings do not target in isolation; they attack a wide range of targets. Look for firms with a broad range of insight into the reputations and velocities associated with devices and IPs—this is instrumental in helping to sort the good from the bad.

- **Iterative optimization of analytics is critical.** Rules-based systems have historically been used to govern decisions regarding ATO risk. The reality, given the vast quantity of historical and real-time data inputs now available, is that machine learning analytics are the only way to optimize decisioning and adapt to rapidly evolving attack vectors. Attackers will often retool when countermeasures are deployed, so effective control frameworks require analytics that can automatically adapt without human intervention.

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

Julie Conroy
+1.617.398.5045
jconroy@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

ABOUT F5

F5 (Nasdaq: FFIV) powers applications from development through their entire life cycle, across any multicloud environment, so its customers—enterprise businesses, service providers, governments, and consumer brands—can deliver differentiated, high-performing, and secure digital experiences.

ABOUT SHAPE SECURITY

The world's leading banks, airlines, retailers, hotel chains, and federal agencies rely on Shape Security, wholly owned by F5, as their primary line of defense against sophisticated cybercrime. The Shape technology platform, covered by more than 50 patents, stops automated fraud and other attacks on web and mobile applications, including credential stuffing, account takeover, scraping, and unauthorized aggregation. Shape is one of the largest processors of login traffic and protects more than 1.3 billion user accounts. Every 24 hours, Shape blocks more than 2 billion fraudulent login attempts and other transactions, while ensuring that more than 200 million legitimate human transactions are kept safe. Shape prevented more than US$1 billion in fraud losses in 2019.