Aite PARTNER. ADVISOR. CATALYST.

Application Fraud: Strategies for a Head Start in the Identity Fraud Arms Race

FEBRUARY 2021

Prepared for:

NuData Security

mastercard

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Application Fraud: Strategies for a Head Start in the Identity Fraud Arms Race, commissioned by NuData Security and produced by Aite Group, examines recent trends in application fraud among North American financial institutions (FIs). The findings are based on application fraud research conducted by Aite Group that drew from surveys and interviews of fraud executives from North American FIs from July through September 2020.

Key takeaways from the study include the following:

- Application fraud continues to be a major issue for FIs. It also remains among the most compelling ways to reduce losses while also supporting growth in revenue and improving the client experience in what is arguably the most important client-facing process.
- This whitepaper delves into how FIs are managing this challenge today and how market forces and environmental conditions are shaping trends among practitioners and solutions providers in their efforts to exert greater control over it. Two surveys and multiple interviews with fraud executives were used to reveal insights into the trends examined in this whitepaper.
- Synthetic identity fraud accounts for the lion's share of losses associated with application fraud, which is projected to reach more than US$4.1 billion by 2023.
- Many FIs have enjoyed benefits from investment strategies that have prioritized transformation efforts around identity verification controls meant to renovate their Know Your Customer (KYC) control framework.
- Automated application fraud attacks and those that rely on large quantities of outsourced labor to complete fraudulent enrollments, known as human farm attacks, have influenced many FIs' investment strategies.
- Many fraud executives have found value in investing in behavioral biometric solutions to counter emerging application fraud threats, such as automated and human farm attacks. These solutions have proven to be an effective additional layer of security and that improve accuracy without negatively impacting the enrollment process. They can also be applied as an exceptionally useful additional layer in securing the authentication process.

INTRODUCTION

As the digital economy grows and evolves, so too does the challenge of protecting sensitive information from abuse and fraud. The epic struggle between security professionals and legitimate participants on one side and the hackers and criminals on the other rages on and even finds itself significantly accelerated by the unprecedented disruption of a pandemic and widespread social unrest. Despite encouraging advancements in security capabilities and the efforts of thousands of principled and highly motivated security professionals, FIs still struggle with managing application fraud. Most agree that application fraud is the primary manifestation of what one fraud executive summarized as the core of the problem: "Identity is broken."

Application fraud has consistently been reported to be among the top two or three biggest pain points for fraud executives at North American FIs for the last five years, and there is evidence that it has gotten significantly worse in 2020. This white paper examines the latest trends in application fraud in direct deposit accounts (DDAs) and credit card accounts, how North American FIs are managing these risks, and why investments in application fraud controls continue to be among those with the most appealing business cases.

METHODOLOGY

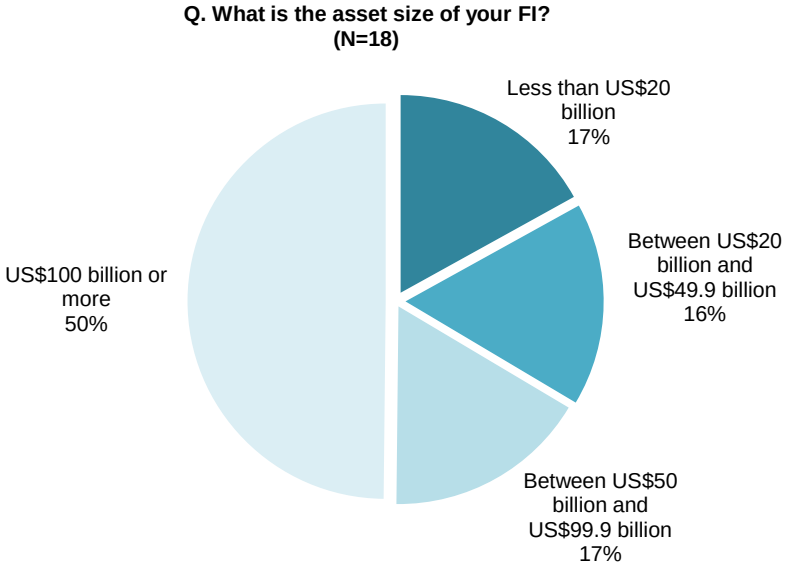
Aite Group conducted research using an online survey from July 2020 to September 2020 to examine trends in application fraud for both DDAs and credit cards. Executives from 18 U.S. FIs completed the application fraud survey, and several interviews with fraud executives at these and other FIs supplemented the data gathered via the survey. Asset sizes of the participating FIs range from under US$1 billion to over US$100 billion. A distribution of participating FIs by asset size can be seen in Figure 1.

This white paper represents a refresh of Aite Group's application fraud reports published in March 2016[1] and December 2018.[2] Given the size and structure of the research sample, the data provide a directional indication of conditions in the market.

1. See Aite Group's report *Application Fraud Rising as Breaches Fan the Flames*, March 2016.

2. See Aite Group's report *Application Fraud: Fighting an Uphill Battle*, December 2018.

Figure 1: Asset Size of FI Respondents to the Application Fraud Survey



Source: Aite Group's survey of 18 FIs, July to September 2020

This white paper is also informed by data gathered from Aite Group's Financial Crime Forum held on September 16 and 17, 2020. During that virtual event, the Financial Crime Forum survey gathered responses from 47 fraud executives from 30 financial services firms. With one exception (Thailand), these FIs are in North America, but the nature of the participating fintech firms' business allows them to cover a wider geographic area.

THE MARKET

Relative to all other forms of fraud attacks, application fraud has been steadily expanding its mindshare among the things that are of the greatest concern to fraud executives. This trend has been growing since at least 2017[3] and has only accelerated as a function of the environmental and economic conditions resulting from the global pandemic. The consensus among fraud executives as to the root cause of the overarching trend points to the growth of identity-related fraud in the post-EMV fraud threat landscape.[4] Considering that application fraud is the means by which financial criminals procure access to deposit and credit accounts that make first-party fraud (for the purposes of this white paper, the simplest definition of the term "first-party fraud" is "any form of fraud committed against an FI or merchant by one of its own customers"[5]), money muling, and the incubation and development of synthetic identities possible, it should come as no surprise that this kind of fraud is increasing.

As economic conditions have deteriorated and workers around the world find themselves in search of income, millions of people are vulnerable to turning to criminal activities, such as first-party fraud, or to agreeing to open a new account or use an existing account to move illegally obtained funds on behalf of organized crime rings. First-party fraud has been a consistent and growing form of revenue for fraudsters, and the demand for mule accounts has never been higher as fraud rings seek to funnel massive quantities of intercepted stimulus funds from federal and state agencies. Synthetic identities make a lot of these forms of fraud much easier to commission, but they are also a significant and growing source of revenue in and of themselves. Table A illustrates how these and other trends in application fraud will impact FIs in the market.

Table A: The Market

Market trends	Market implications
Data breaches, phishing attacks, social engineering, and malware enable fraudsters to successfully impersonate other consumers.	Many methods used by FIs to authenticate new and existing customers are no longer dependable.
Application fraud and other identity crimes are continual challenges for FIs.	Fraud losses due to identity crimes will continue to grow until new technology solutions are implemented to thwart these crimes.
Fraudsters are nurturing synthetic identities carefully before using them to commit fraud.	Synthetic identities have been nurtured so that they have credit bureau files and mobile numbers are extremely difficult to detect.
Technology changes are planned.	Many FIs are replacing existing vendors or adding additional vendors to improve overall fraud prevention performance.

Source: Aite Group

3. See Aite Group's report *Machine Learning: Fraud Is Now a Competitive Issue*, October 2017.

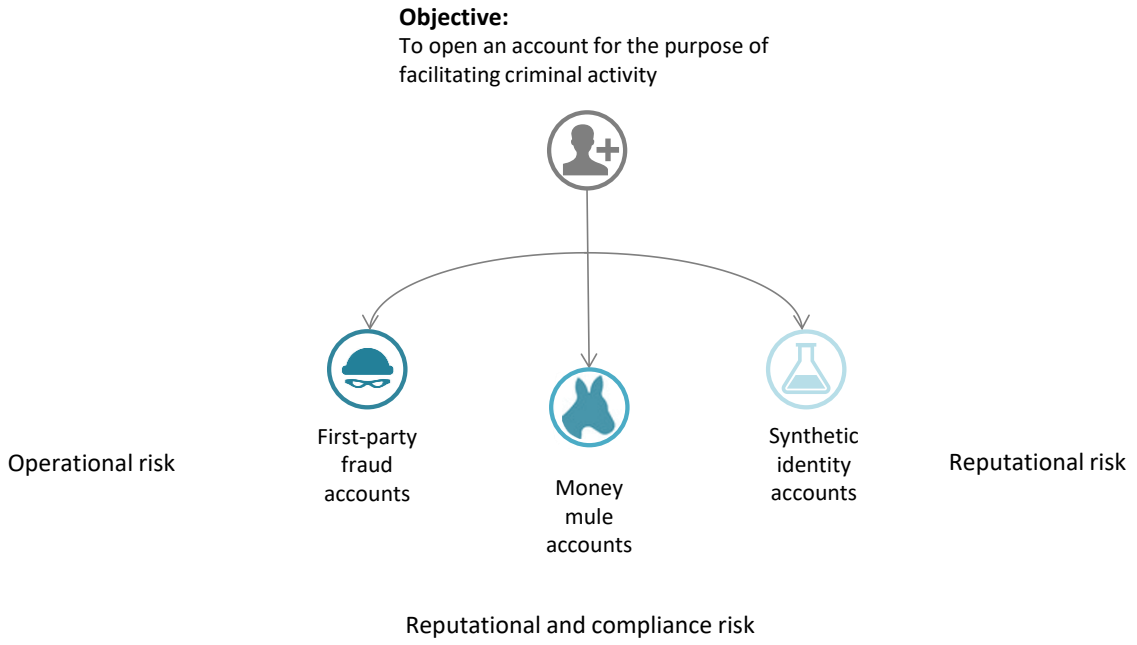
4. See Aite Group's report *Application Fraud: Fighting an Uphill Battle*, December 2018.

5. "Fraud Definitions," Fraud.net, accessed October 23, 2020, https://fraud.net/d/.

APPLICATION FRAUD TRENDS

Analyzing trends in application fraud is a challenging effort. As is the case with most kinds of fraud, one of the greatest difficulties is the lack of an established definition in the context of a taxonomy of fraud terms that all (or even most) practitioners agree on. That being said, for the purposes of this white paper, application fraud is used as an umbrella term to describe the act of establishing an account that is intended to be used to support malicious or criminal activity. Each application fraud event, therefore, typically manifests itself in one of three ways, as illustrated in Figure 2. Figure 2 also illustrates the kinds of risks associated with each type of fraud that stem from failures to detect and prevent fraudulent applicants.

Figure 2: Application Fraud Conceptual Model



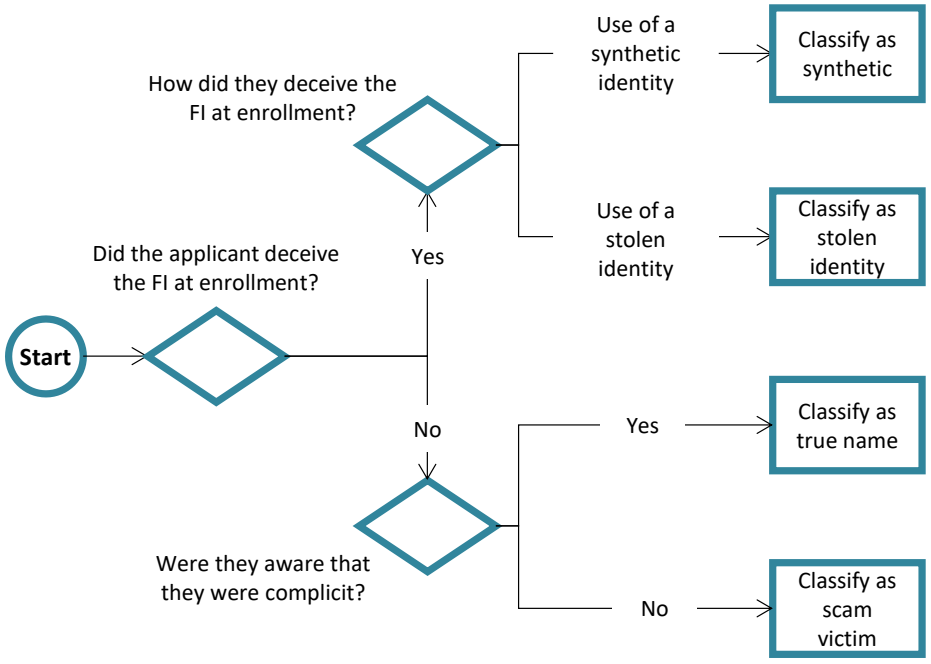
Source: Aite Group

To better understand the mechanics of application fraud, it's helpful to establish the terminology commonly used to illustrate how application fraud and its downstream manifestations relate to one another. It's worth noting that when it comes to terminology, some definitions are fairly well agreed upon, but many are not. The following analysis is, therefore, meant to establish a conceptual model for a basic understanding of the means by which application fraud is classified and how those classifications relate to the downstream manifestations of application fraud. The model is broken out into two stages:

- **Classify the means of deception at the time of enrollment:** The objective of this stage is to establish whether and how the applicant deceived the FI at enrollment in order to classify the means that the bad actor used to defeat application fraud controls (Figure 3).

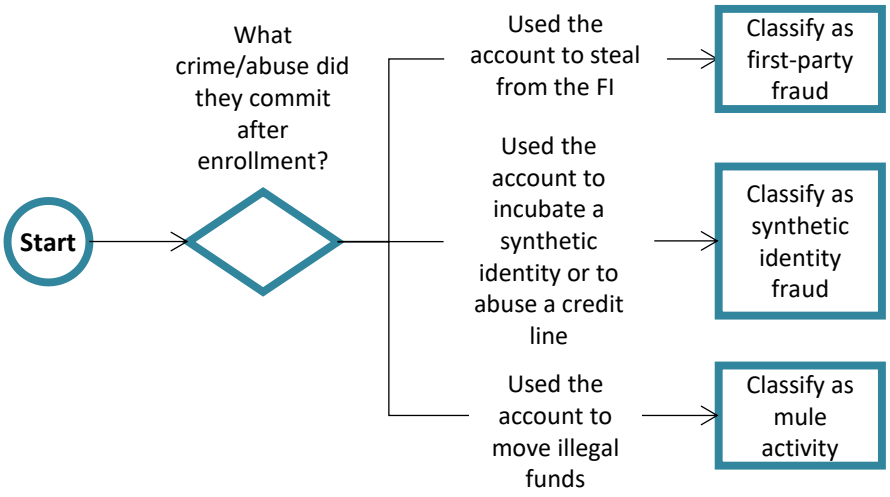
- **Classify the type of fraud or abuse that occurred as a result of the deception at enrollment:** The objective of this stage is to determine what type of fraud or other form of abuse the applicant committed after enrollment that was the downstream outcome of deception in the enrollment process (Figure 4). These are referred to as the "manifestations" of application fraud.

Figure 3: Conceptual Forensic Model for Classifying the Type of Deception Employed at Enrollment



Source: Aite Group

Figure 4: Conceptual Forensic Model for Classifying the Type of Fraud, Criminal Activity, or Account Abuse After Enrollment

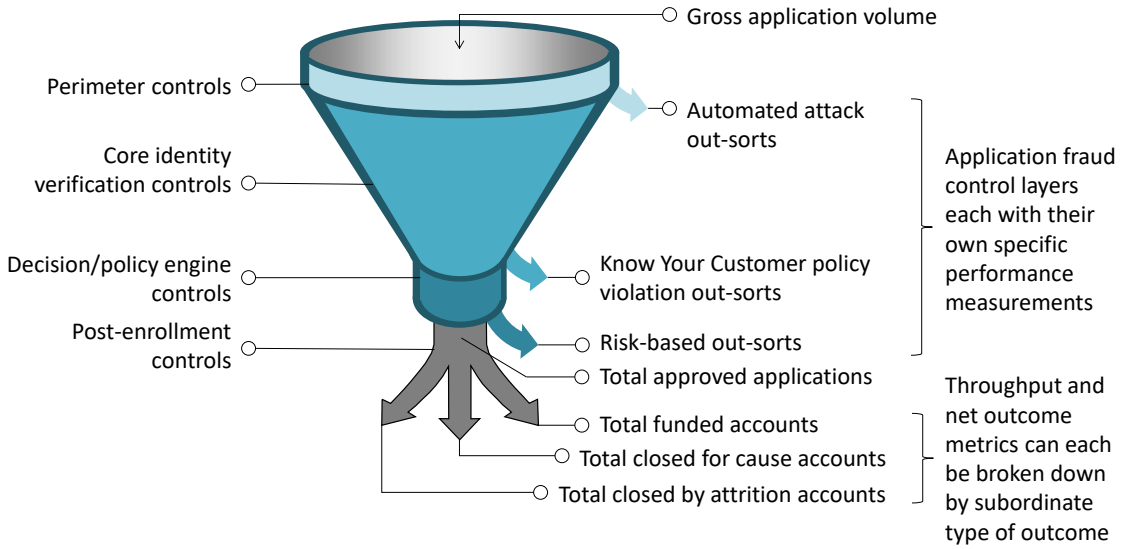


Source: Aite Group

Some practitioners and solution providers use the term "third-party application fraud" or "identity theft application fraud" when talking about a scenario in which fraudsters use a stolen identity to create an account that they intend to use to defraud the FI, to move illegal money, to incubate a synthetic identity, or to abuse a line of credit. With this model, it's possible to reexamine these terms. Use of the term "third party" in this context only works if it's used by the victim of identity theft, which would work if the victim of identity theft were interested in classifying the event. In virtually every scenario, however, the only entity interested in classifying the event is the FI that observed the event. For this reason and for the sake of this white paper, the terms used assume the role of the victim of the deception that resulted in the enrollment and/or the deception that resulted in the fraud or abuse after enrollment, as opposed to the role of the victim of identity theft used in those deceptions.

While there is general agreement on high-level definitions for the more common forms of fraud that result from application fraud (e.g., deposit fraud, mule activity, and synthetic identity fraud), there is a great deal of variation in the manner in which FIs observe, record, and account for these events. This is typically more often the case with synthetic identity fraud and mule activity, in which these kinds of events are rarely measured at all.[6] By way of illustrating the impact that this has on the capacity to measure the scope and scale of application fraud, consider that, of the 18 FIs interviewed for this report, only three were able to provide the level of granularity in the performance metrics of their application fraud control frameworks necessary to support a model for articulating the overall health and performance of the framework (Figure 5).

Figure 5: Conceptual Model for Measuring Performance of DDA Application Fraud Control Frameworks



Source: Aite Group

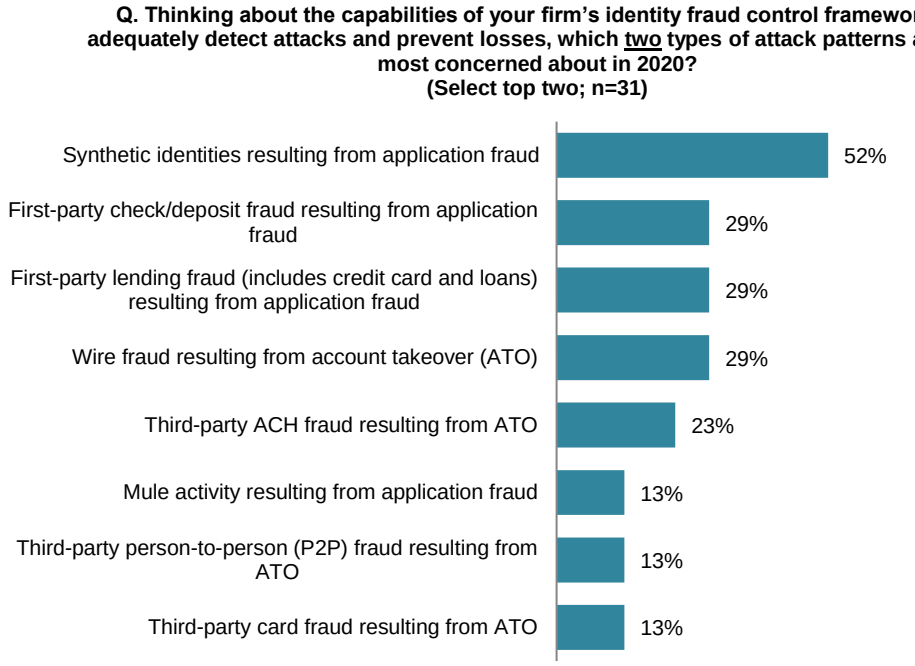
6. See Aite Group's report *Mule Activity: Find the Mules and Stop the Fraud*, April 2020.

Whether this reflects the siloed nature of application fraud frameworks, the inadequacy of metrics and reporting capabilities, or simply the lack of a standardized (and unanimously agreeable) benchmarking model is at least somewhat beside the point. The unfortunate truth is that when it comes to measuring application fraud frameworks' performance, many in the industry have a way to go before they can easily articulate and benchmark the performance of their efforts in this increasingly important domain. Since the evidence is fairly clear that application fraud controls are among those getting the most attention in terms of investment, it would stand to reason that those who have championed these investments would want to know, in as much detail as possible, what value they're getting from the capital expended. The capacity to benchmark their frameworks' performance has the added benefit of demonstrating the degree of effectiveness (or lack thereof) in their framework relative to peers in the service of defending recent or ongoing investments or in making a case for additional investments. Regardless, there appears to be a market opportunity for a more robust, industry-standard model for performance and benchmarking metrics for application fraud control frameworks.

Despite the lack of more detailed metrics of specific components within the funnel, however, most fraud executives agree on the basic definition of application fraud as well as how to measure basic forms of the discrete fraud events that manifest from it. The trends in responses among fraud executives suggest that it has been occupying a large and growing portion of the list of the top two things that keep them up at night. In a 2019 Aite Group survey of 27 fraud executives, the second-most commonly cited pain point was application fraud (33% of respondents versus 37% for the number-one most commonly cited pain point).[7] Though the question was posed to reflect the attack patterns that are among the chief manifestations of application fraud in 2020, the most recent data illustrate a continuation of this trend (Figure 6). Synthetic identity fraud resulting from application fraud, first-party lending fraud resulting from application fraud, and first-party check fraud resulting from application fraud made up the top three forms of attack patterns that concern fraud executives the most in 2020.

7. See Aite Group's report *Key Trends Driving FI Fraud Investments in 2020 and Beyond*, November 2019.

Figure 6: 2020 Attack Patterns That Concern Fraud Executives the Most



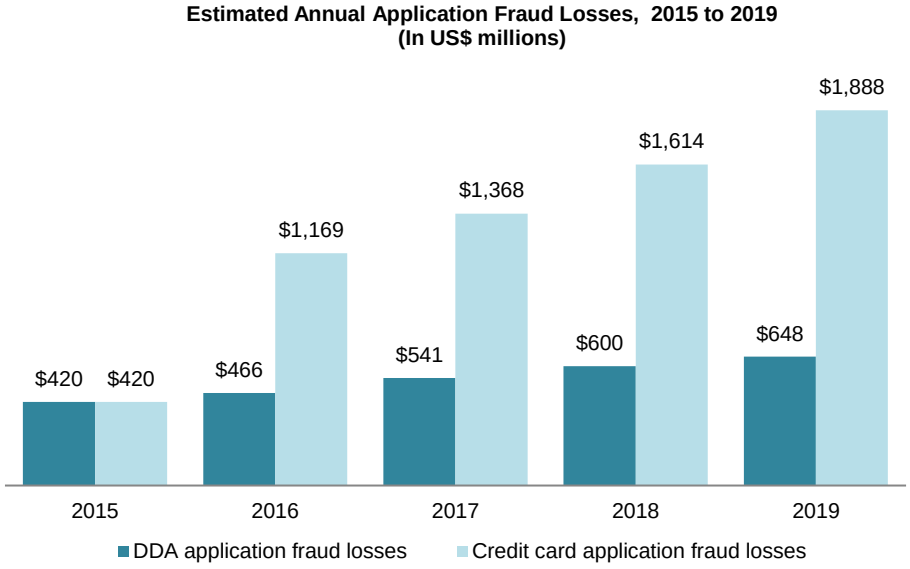
Source: Aite Group's survey of 47 financial services fraud executives, September 2020

Estimates of total application fraud losses were initially put forward in Aite Group's report on the topic in 2016.[8]

Estimates of application fraud losses based on data collected in 2016, 2018, and 2020 can be found in Figure 7.

8. See Aite Group's report *Application Fraud Rising as Breaches Fan the Flames*, March 2016.

Figure 7: Estimated Historical Application Fraud Losses



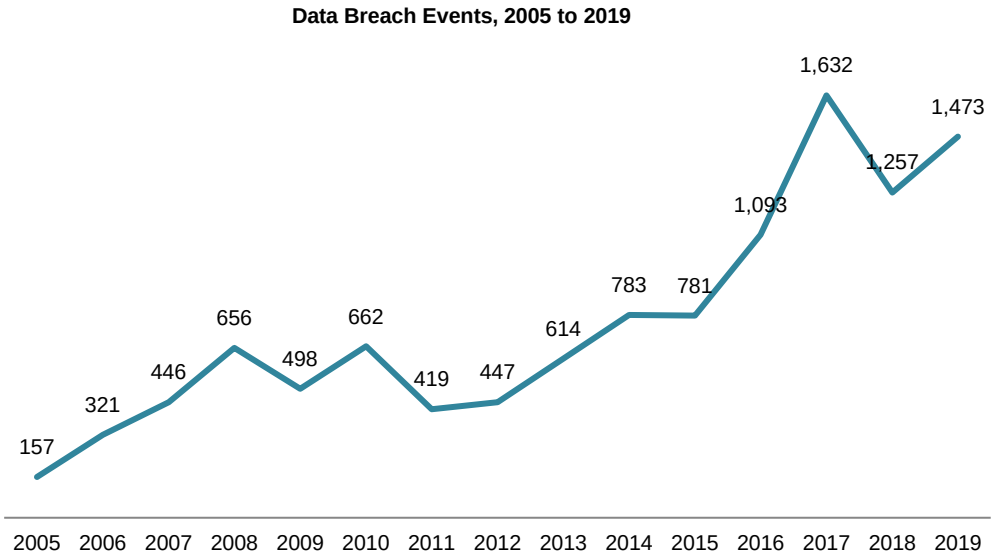
Source: Aite Group

MARKET FORCES DRIVING APPLICATION FRAUD

The consensus among fraud executives interviewed for this report indicates that the usual suspects among the market forces driving increases in application fraud attacks are a significant root cause for the growth in attack rates. Perhaps the most powerful market force stimulating growth in application fraud prior to the pandemic was the trend toward increasing supply in the raw material necessary for fueling the three derivative forms of application fraud. The cost of personally identifiable information (PII)—the foundational building block for all identity fraud—has plateaued over the last few years but remains at an accessible rate of between US$4 and US$10 per identity[9] as supply has increased. This supply, estimated by Breach Clarity (a solution provider of client-facing cyberthreat intel and risk analysis capabilities) to total more than 23 billion in accumulated records since 2017, is the direct result of the steady increase in data breach events (Figure 8).

9. Robert Lemos, "More Breaches, Less Certainty Cause Dark Web Prices to Plateau," Dark Reading, October 15, 2019, accessed October 2, 2020, https://www.darkreading.com/attacks-breaches/more-breaches-less-certainty-cause-dark-web-prices-to-plateau/d/d-id/1336094.

Figure 8: Rate of Increase in Data Breach Events



Source: StatSoft Europe

As long as there is an abundant supply of raw material in the form of PII, the barriers to entry and the costs for fraudsters who use stolen identities (or elements of stolen identities in cobbling together synthetic identities) to create accounts to support their fraud will remain low.

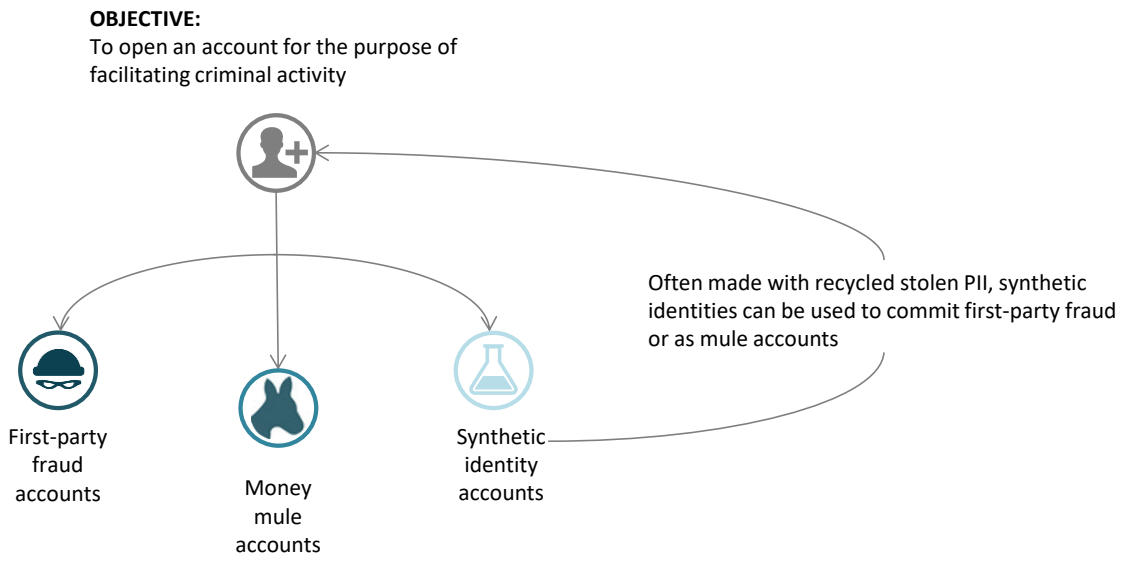
TRENDS IN APPLICATION FRAUD DERIVATIVES

The driving forces behind each of the derivative forms of application fraud deserve consideration, as each differs from the others, albeit with a bit of overlap, at least between synthetic identity fraud, third-party fraud, and mule activity. The economic forces driving growth in activity among first-party DDA fraud and first-party credit card fraud are fairly self-evident. Both represent significant, and growing, revenue channels for fraud rings seeking to exploit the relatively low costs of the raw material needed for identity-based fraud. The market forces driving the growth in synthetics and mule activity, on the other hand, are a little more complicated.

Growth in synthetics is a function of the significant amount of revenue that synthetic identities provide for fraud rings as well as a means of refining the raw material, PII, into a form that can be repurposed for use in many other forms of identity fraud, including deposit fraud and mule activity (Figure 9). To get an idea of the amount of influence that synthetics have on revenue growth for the fraudsters, consider that a 2017 study by a consulting firm estimated that as much as 20% to 30% of the total credit losses among large FIs could be associated with synthetic identity fraud losses.[10] The majority (US$1.2 billion) of the US$2 billion in total estimated credit card application fraud losses for 2020 are derived from synthetic identity fraud losses.

10. See Aite Group's report *Synthetic Identity Fraud: The Elephant in the Room*, May 2018.

Figure 9: Synthetic Identities Role in Fueling First-Party Fraud and Mule Activity



Source: Aite Group

While precise estimates of the portion of first-party check fraud losses (also known as deposit fraud) and first-party credit fraud losses that can be attributed to synthetics remain elusive, fraud executives have few doubts that the fraudsters are making liberal use of them to perpetuate those schemes. One fraud executive interviewed for this report estimates that approximately one-third of his firm's first-party check fraud losses are attributable to synthetic identities. He comments that it is difficult to say exactly what the impact is because the firm is still developing a consistent means of recording and tracking the prevalence of synthetics in its investigations.

Tracking mule activity suffers from the same challenge in many U.S. FIs,[11] so estimates of the portion of mules that use synthetic identities also remain elusive. Consider, though, the important role that money mules play as the backbone of the fraudster's logistics network. Also, consider that managing money mule networks that are often external to the primary members of the fraud ring represents costly overhead. In contrast, synthetic identities provide a relatively low-cost means of establishing drop accounts that the fraud ring can directly control without what one fraudster on a dark-web forum chatroom referred to as the "messy HR problems" of dealing with recruited money mules.

The rates of increase in all three forms of criminal activity stemming from application fraud support the notion that environmental conditions are playing an influential role in driving the increase in application fraud overall. The majority of respondents (72%) report an overall increase in mule activity and synthetic identity fraud. The percentage of significant increases (increases greater than 10%) is weighted in favor of mule activity (43% versus 25% for synthetic identity fraud), which suggests that the fraudsters have a significantly amplified demand for moving stolen funds. Given that the overall rates of increase in conventional forms of fraud are

11. See Aite Group's report *Mule Activity: Find the Mules and Stop the Fraud*, April 2020.

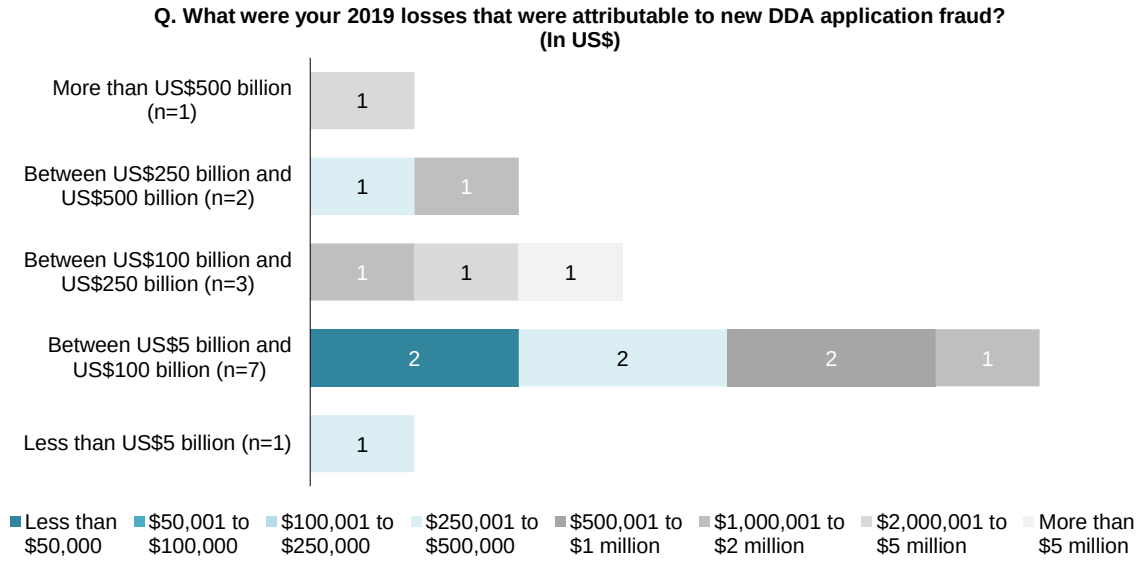
relatively mild, the consensus among most of the fraud executives interviewed for this report as well as those who participated in Aite Group's Financial Crime Forum in September 2020 is that the demand for mules is being driven primarily by the fraudsters' collective focus on intercepting payments from federal and state stimulus programs.

TRENDS IN DDA APPLICATION FRAUD

An analysis of application fraud trends isn't complete without breaking out the trends by the types of accounts that the fraudsters seek to exploit. Doing so sets the stage for an examination of the control frameworks that are dependent on the type of account being provisioned. It also affords the opportunity to establish a conceptual model for how application fraud control frameworks operate. Once established, this would, in theory, enable an examination of the means by which FIs measure the performance of their control frameworks. As alluded to previously, however, this is dependent on a consistent set of definitions for policies, metrics, and controls across the industry, which, sadly, still remains a largely unfulfilled goal.

In terms of trends in DDA application fraud losses, it's helpful to examine them in the context of asset size (Figure 10).

Figure 10: DDA Application Fraud Losses by Asset Size

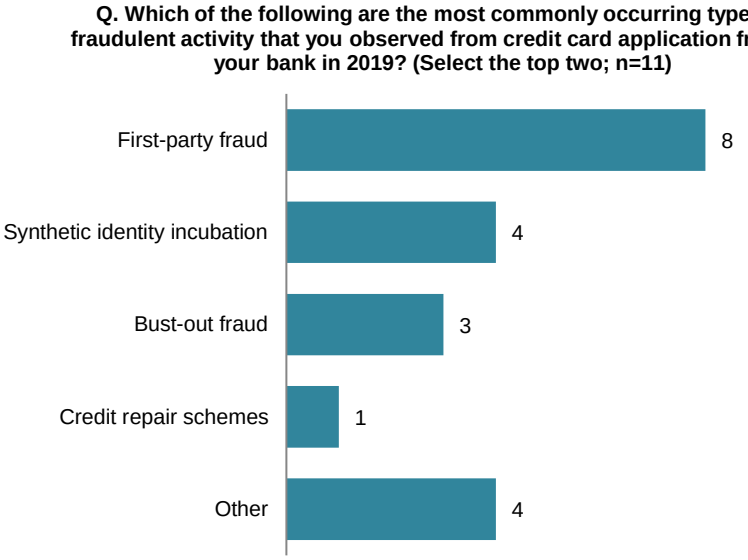


Source: Aite Group's survey of 18 FIs, July to September 2020

TRENDS IN CREDIT CARD APPLICATION FRAUD

While credit card application fraud has a range of fraudulent activity that is as diverse as that of DDA application fraud, the respondents cite first-party fraud and synthetic identity fraud as the two most commonly occurring manifestations of application fraud in their credit card portfolios (Figure 11).

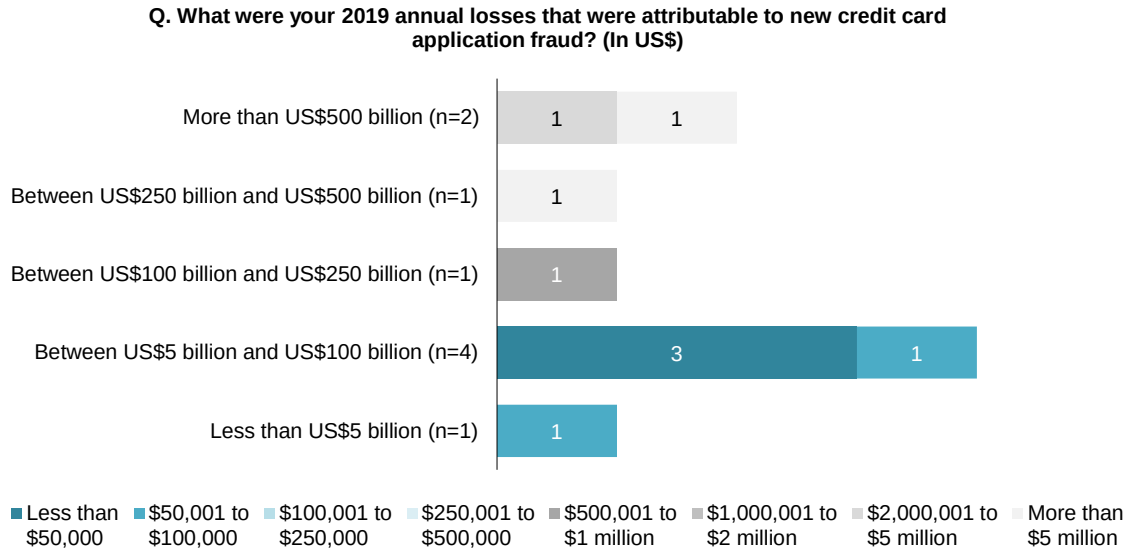
Figure 11: Most Common Forms of Credit Card Application Fraud in 2019



Source: Aite Group's survey of 18 FIs, July to September 2020

Figure 12 illustrates the distribution of credit card application fraud losses by asset size of respondents for the 2020 cohort. As was noted previously, the diversity among FIs in how they classify losses associated with synthetic identity fraud suggests that application fraud losses are much higher than they appear.

Figure 12: Credit Card Application Fraud Losses by Asset Size

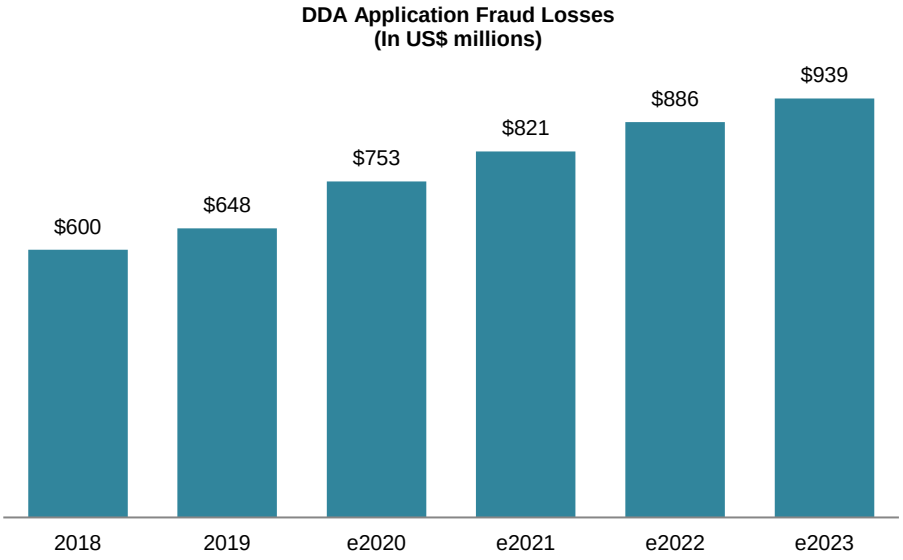


Source: Aite Group's survey of 18 FIs, July to September 2020

PROJECTED APPLICATION FRAUD LOSSES

If market forces have been behind the overall upward trajectory in growth, and the environmental conditions brought about by the pandemic have accelerated that growth since it began, then many fraud executives have concluded that this growth will likely continue at least so long as the environmental conditions persist. The projections for DDA application fraud and credit card application fraud were estimated separately. Figure 13 projects application fraud losses for DDA application fraud to hit US$939 million in 2023.

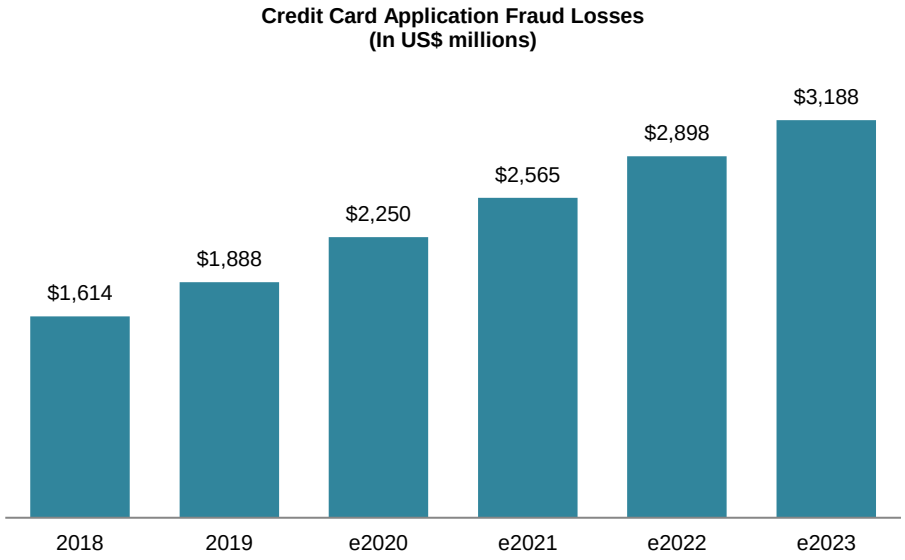
Figure 13: Estimated and Projected U.S. FIs' DDA Application Fraud Losses



Source: Aite Group

Figure 14 projects credit card application fraud losses to reach US$3.188 million by 2023, driven predominantly by synthetic identity fraud losses.

Figure 14: Estimated and Projected U.S. FIs' Credit Card Application Fraud Losses



Source: Aite Group

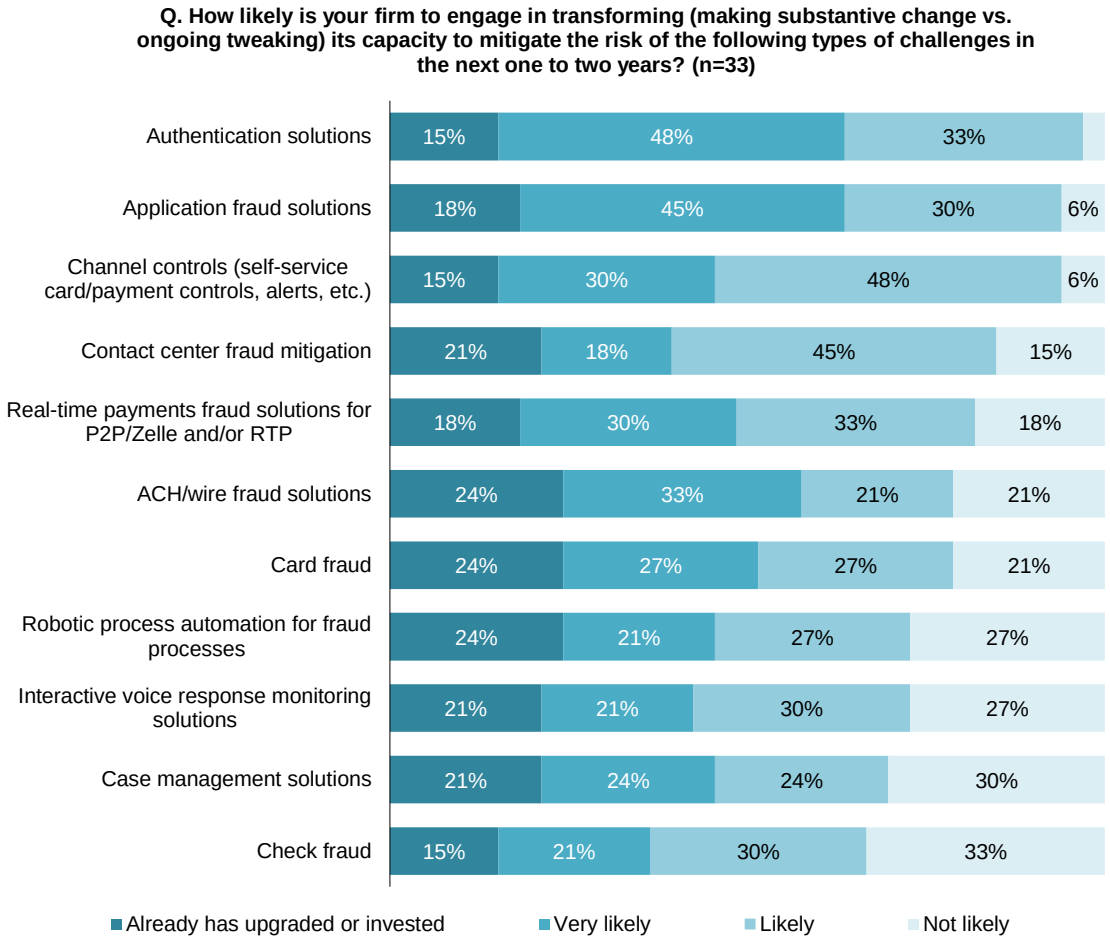
APPLICATION FRAUD MITIGATION TRENDS

Most fraud executives report that investments in application fraud mitigation pay handsome dividends when it comes to improving their capacity to balance fraud loss mitigation with improvements to client experience and by supporting enterprise's strategic priorities for revenue growth. Application fraud controls, such as authentication controls, have enjoyed a considerable amount of investment over the past several years. Anecdotal evidence suggests that those rates of investment are likely to continue to increase despite what is emerging as a challenging economic environment that is likely to result in a reinvigoration of cost containment programs across the industry.

To better understand why this is the case, consider what one fraud executive interviewed for this report relayed about a firm's efforts to build support for investments in application fraud controls. In the early stages of the effort to make a case for renovating the firm's application fraud control framework, the fraud executive commissioned a handful of proofs of concept (POCs) with leading solution providers. In analyzing the results of these POCs, care was taken to include estimates of the impact that each solution would have not only on the reduction of first-party fraud losses but also, notably, on net enrollment throughput, accuracy rates, attrition rates, funding rates, and overall portfolio profitability. The fraud executive reported that the firm's business partners who owned profit and loss for DDA, credit card, and retail channels were "really impressed" by the benefits put forward in the analysis. The fraud executive gave his analysts credit for demonstrating to his peers how examining the profitability of the portfolio in a way that incorporated a more holistic and empirically driven picture of the overall quality of the portfolio could lead to a much more mutually beneficial partnership with fraud and security business units. The net result was that the fraud executive's peers became eager to assist with prioritizing and funding the investment for the following investment year, which, he went on to say, was "a refreshing change from previous years."

Considering the relative rate of transformation in application fraud controls across the industry (Figure 15), it's not hard to see the value of the capacity to articulate the benefits of improving upon application fraud control capabilities. Transformation initiatives to address application fraud threats are only modestly behind those aimed at extending greater control over the digital channel to customers.

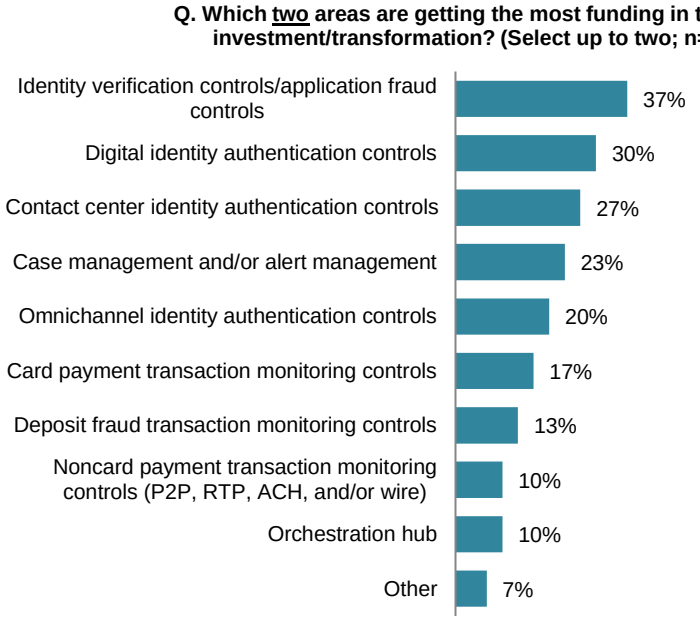
Figure 15: Likelihood of Transforming Capacity to Mitigate Risks in the Next Two Years



Source: Aite Group's survey of 47 financial services fraud executives, September 2020

Regardless, it appears that other fraud executives are finding similar success stories in securing investment into application fraud controls. Framed from another perspective, the rates of investment in the technologies most closely associated with application fraud controls are also at the top of most FIs' priority lists (Figure 16).

Figure 16: Areas of Investment Receiving the Most Funding



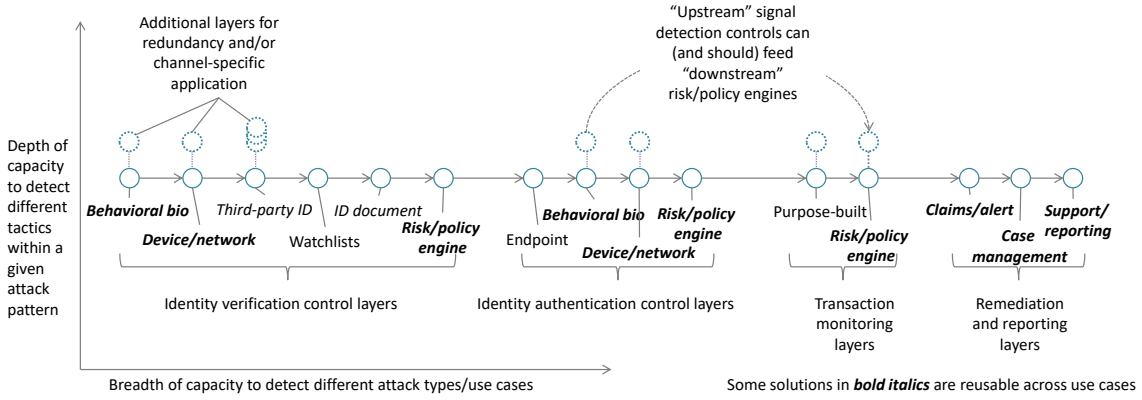
Source: Aite Group's survey of 47 financial services fraud executives, September 2020

The considerable pressure to support revenue growth objectives by optimizing new client acquisitions is a motivating force for strengthening the layers of identity verification controls. Similarly, there has been consistent market pressure to make client interactions easier for customers in the spirit of improving retention. If these are the two dominant motivating forces that are driving investment trends, then it's useful to examine the dynamics behind the leading strategies for achieving the goals of reducing application fraud while improving acquisition rates and operating expenses.

STRATEGIES FOR THE IDENTITY FRAUD ARMS RACE

Defense-in-depth remains the most effective and widely adopted design philosophy behind virtually every anti-fraud strategy active today. The strategy is based on the notion that the fraudsters will continue to seek out vulnerabilities in their opponent's control frameworks in an economically motivated effort to find the most cost-effective way to compromise the FI's security infrastructure for the purpose of defrauding either the FI or the FI's clients. The objective of the defense-in-depth strategy, therefore, is to find and deploy the combination of controls that provides not only a sufficient breadth of countermeasures to detect the range of attack types but also allows each countermeasure across the spectrum of attacks the sufficient depth of capability to thwart (or deter) the range of tactics within a given attack type. Figure 17 illustrates how a typical fraud control framework is structured around a range of fraud attack "use cases" that spread from left to right (breadth) and how various forms of functional capabilities are arrayed from bottom to top (depth) to counter a variety of tactics within the attack use case.

Figure 17: A Typical Fraud Control Framework Built Around the Defense-in-Depth Strategy



Source: Aite Group

When an FI encounters a new attack pattern or a new tactic within a given attack use case, the challenge becomes whether and how to deploy a countermeasure to detect and prevent the attack. In most cases, there is an urgent need to plug the vulnerability that the fraudsters have discovered, so many FIs are forced to rapidly develop and deploy some form of homegrown solution. Unfortunately, most of the time, these solutions are not sustainable and can often come at the cost of impugning a client experience or adding greater demand on staffing capacity. Regardless, the ability to reduce or eliminate the costs of mitigating the threat with one or more stop-gap solutions is what lies behind the business case for justifying a more robust and sustainable solution. The extent to which the investment can address multiple known gaps in either the depth of a given use case (e.g., detecting a variety of bot-driven credential stuffing tactics) or the breadth of fraud attack types (e.g., the ability to detect anomalous behavioral activity among applicants as well as the capacity to detect anomalous authentication activity among existing login attempts) determines the relative potential value of the investment. The greater the quantity of known or potential gaps that the solution can address competitively well, the more attractive the investment.

Of course, the fraudsters never rest on their laurels. They're constantly probing defenses and searching methodically and relentlessly for undiscovered vulnerabilities. For this reason, fraud executives must also be selective in finding a solution that provides the greatest possible flexibility in terms of how it can be adapted to respond not only to the variety of known tactics and attack profiles but also to the constantly changing landscape of emerging tactics and attack patterns. Behavioral biometric solutions have enjoyed robust adoption rates in recent history precisely because they offer the capacity to address a variety of specific tactics within an attack use case (depth of capability) and also because they can provide valuable layers of control across multiple attack use cases (breadth of utility). The leading solution providers in the space are able to cover more surface area in terms of depth and breadth but are also those that have proven to be exceptionally flexible in terms of responding to shifts in existing tactics as well as emergent tactics or attack use cases. Most fraud executives who have invested in behavioral biometric solutions do so largely because the robust additional layers of security that they provide give them a leg up in the ever-escalating arms race between fraud mitigation business units and their adversaries.

COUNTERING EMERGING ATTACK PATTERNS

An influential force in shaping the market for application fraud controls has been the trend among fraudsters to automate their attacks with bots—computer programs engineered to use the FI's online account application system to create accounts using stolen or purchased PII from identity theft victims, or synthetic identities either manufactured or purchased from online marketplaces. Fortunately, there are a great many signals in the digital channel, which has given rise to a rich variety of solution providers that have the capacity to determine whether the signals in the online interaction are consistent with those of a legitimate user or if they are consistent with an automated attack by malicious software. Table B lists the solution providers that specialize in this area.

Table B: Bot Detection Solution Providers

Vendors				
Akamai	Arkose Labs	BioCatch	buguroo	Callsign
F5	IPQualityScore	Kasada	NuData Security	PerimeterX
Radware	SecuredTouch	Signal Sciences	SpyCloud	

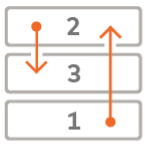
Source: Aite Group

Automated attacks are particularly appealing to fraudsters, primarily because they are highly scalable but also because the parameters of the bot that orchestrates the attack pattern can be relatively easily modified to overcome different countermeasures from one target institution to the next or in response to shifts in detection strategies over time. The most effective bot attacks, therefore, are those that provide the greatest range of options in configuring the attack pattern to mimic human-like behavioral activity and/or to disguise the device being used in the attack to appear to be legitimate. The greater the range of options that the bot caters to, the greater the capacity it has for discovering a gap in the target institution's capacity to detect suspicious signals in the channel. FIs forced to rely on homegrown solutions engineered to detect one or more signals characteristic of a narrow range of tactics are more likely to be susceptible to the expanding range of tactics employed by fraudsters looking to optimize their operations through automation.

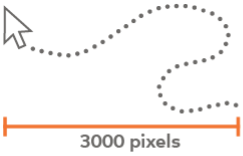
Another emerging trend in attack patterns is the use of human farms. Human farm attacks are often used to circumvent relatively basic signal detection controls such as inspection of the applicant's geolocation. In previous years, it was fairly common to use relatively basic controls to detect suspicious applications by way of deriving applicants' geolocation from their IP address. In the spirit of the arms race, the fraudsters began obfuscating their IP addresses (and, later, many of the tell-tale signals from the device and browser that they used) in an effort to circumvent FIs' growing arsenal of detection capabilities. Undeterred, the fraudsters hired large numbers of low-wage workers who were instructed to use specific devices configured in such a way that made them appear to be the same kind of machines operating with many of the same signals that one would find among legitimate domestic applicants. These pools of low-wage workers are known as "human farms," and for those without leading behavioral biometrics solutions, they can be exceptionally difficult to detect.

Leading behavioral biometrics solutions have become a popular choice for many fraud executives looking for an effective means of automating the inspection and risk assessment analysis that can be tuned specifically to reveal the tell-tale behavioral signals of human farm applicants in a manner that is completely transparent to the user and, therefore, has little to no negative impact on the user's experience. The analysis that leading behavioral biometric solution providers can provide is typically based on assembling a variety of disparate signals into patterns that, when added together in the right combination, result in a composite mosaic picture of the applicant that is greater than the sum of its parts. Figure 18 illustrates a variety of examples provided by NuData Security of the kinds of behavioral biometric patterns that, in isolation, may not be sufficient to flag a given applicant as being high risk. But when one or more of these signals are present in the right combination with other signals and are within the parameters of the FI's risk tolerances, the FI is able to make a much more robust determination of the level of risk that a given applicant represents.

Figure 18: Examples of Signals That Reveal Applicants Are From a Human Farm



Form flow: Legitimate users tend to fill the form from top-to bottom, whereas human farm applicants jump around based on the information that they have on file.



Form familiarity: The distance that the mouse travels around an application page can reveal the degree to which a user is familiar with the page or form.

Completion time: Legitimate users, on average, take longer to complete an application form than do human farm applicants owing, again, to their familiarity with the form.

Error rates and awkward pauses: Legitimate users make far fewer typing errors and demonstrate fewer pauses between inputting first name and last name, for example.

Window focus changes: Human farm applicants show a higher rate of switching from one window to another, often accompanied by copy and paste commands in lieu of typing.

Impossible device signals: Human farm applicants sometimes make errors inputting things such as browser versions in their spoofing software.

Source: NuData Security

Perhaps most importantly, the FI is able to detect a wider variety of signals that are, in aggregate, highly effective at scoring the relative degree risk of a given applicant, and they're able to do so with much greater precision than they were without the aid of behavioral biometrics. In an age when improving acquisition and retention rates is weighed with equal measure as reducing fraud losses when it comes to prioritizing return on investment criteria, additional layers of control that add to the FI's capacity to get a high-resolution image of the identity of the applicant matter more than ever.

CONCLUSION

The market forces that have been driving increases in application fraud for years remain very influential, and the environmental conditions brought about by the pandemic have only accelerated those trends. In addition to this, solution providers have had many compelling innovations, and application fraud solution providers have had notable expansions of range and diversity. For these reasons, investing in application fraud controls remains a top priority.

- Application fraud is not only here to stay, but it also will get worse before it gets better.
- Investing in application fraud controls remains among the most compelling ways to make substantive improvements to downstream manifestations of fraud, account abuse, and money laundering, and to make significant contributions to growing or optimizing revenue growth.
- Finding the right mix of controls and reducing dependence on those that introduce friction in the important process of acquiring new clients can go a long way toward improving client satisfaction, loyalty, and other metrics commonly used to measure client experience, such as net promoter score.
- Behavioral biometrics solutions have enjoyed an increasing amount of investment among FIs seeking to extend the depth of their defensive layers of controls against the growing volume of emerging application fraud attacks, including automated attacks and those that leverage human farms.
- In addition to adding depth to their layers of identity fraud controls, many fraud executives have prioritized investment in leading behavioral biometrics solutions because they can be applied to a wide range of identity fraud attacks, most notably application fraud and account takeover.

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

Research Design & Data:

Judy Fishman
+1.617.338.6067
jfishman@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 NUDATA SECURITY

NuData Security is a Mastercard company. It helps businesses identify users based on their online interactions and stops all forms of automated fraud. By analyzing over 650 billion behavioral events only in 2020, NuData harnesses the power of behavioral analytics and passive biometrics, enabling its clients to identify the human behind the device accurately. This allows clients to verify users before a critical decision, block account takeover, stop automated attacks, and reduce customer insult. NuData's solutions are used by some of the biggest brands in the world to prevent fraud while offering a seamless customer experience.

CONTACT

NuData Security, a Mastercard company
+1.604.800.3711
verifygoodusers@nudatasecurity.com