Aite PARTNER. ADVISOR. CATALYST.

Application Fraud: Accelerating Attacks and Compelling Investment Opportunities

This report provided compliments of:

NOVEMBER 2020

Trace Fooshée

TABLE OF CONTENTS

LIST OF FIGURES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACT POINTS

- Application fraud continues to be a major issue for financial institutions. As such, investing in application fraud controls 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 Impact Report 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 report.
- 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.
- Despite significant innovations in detection and prevention capabilities over the past two years and despite significant investment in these solutions, many FIs continue to struggle to articulate the impact that application fraud and its derivative forms of financial crime have not only on losses but also on demand deposit account (DDA) and credit card portfolio quality as measured by profitability.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INTRODUCTION

As the digital economy grows and evolves, so too does the challenge to protect 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, which most agree 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 is has gotten significantly worse in 2020. This Impact Report examines the latest trends in application fraud in DDA 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

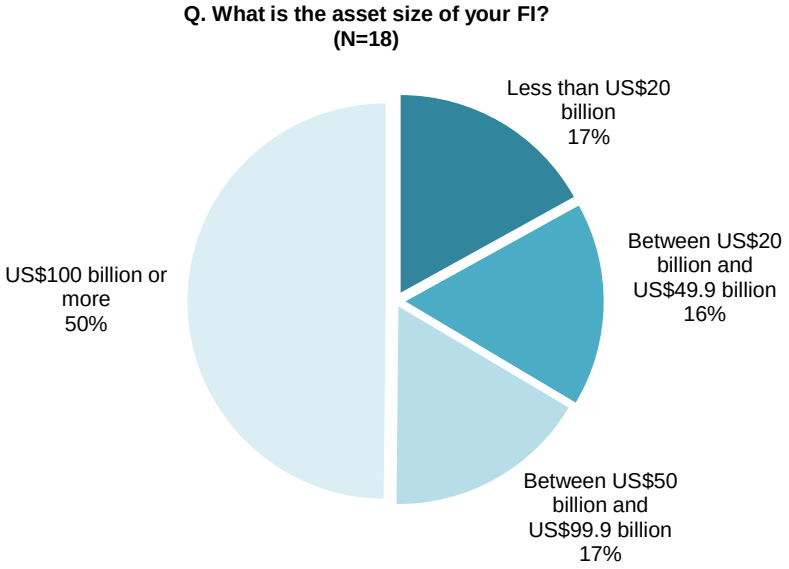
Aite Group conducted research using an online survey from July 2020 to September 2020 to examine trends in application fraud for both DDAs and credit cards. Executives from 18 U.S. FIs completed the application fraud survey, and several interviews with fraud executives at these and other FIs supplemented 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 Impact Report represents a refresh of Aite Group 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.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

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 report 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 North America.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

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 among fraud executives. This trend has been steadily 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 report, the simplest definition of the term "first-party fraud" is "any form of fraud committed against a financial institution 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 like 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 that 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 that 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.

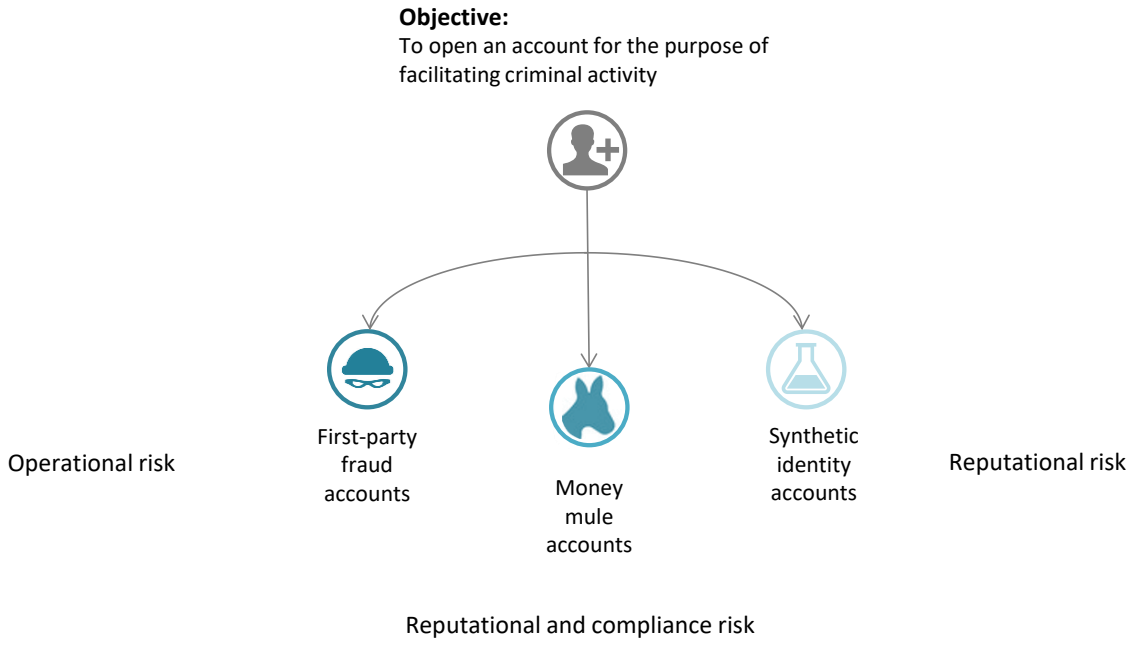
5. "Fraud Definitions," Fraud.net, accessed October 23, 2020, https://fraud.net/d/.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

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 challenges 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 report, application fraud was defined as a kind of umbrella term used 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. Also illustrated in Figure 2 are the types 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 the downstream manifestations of it 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:

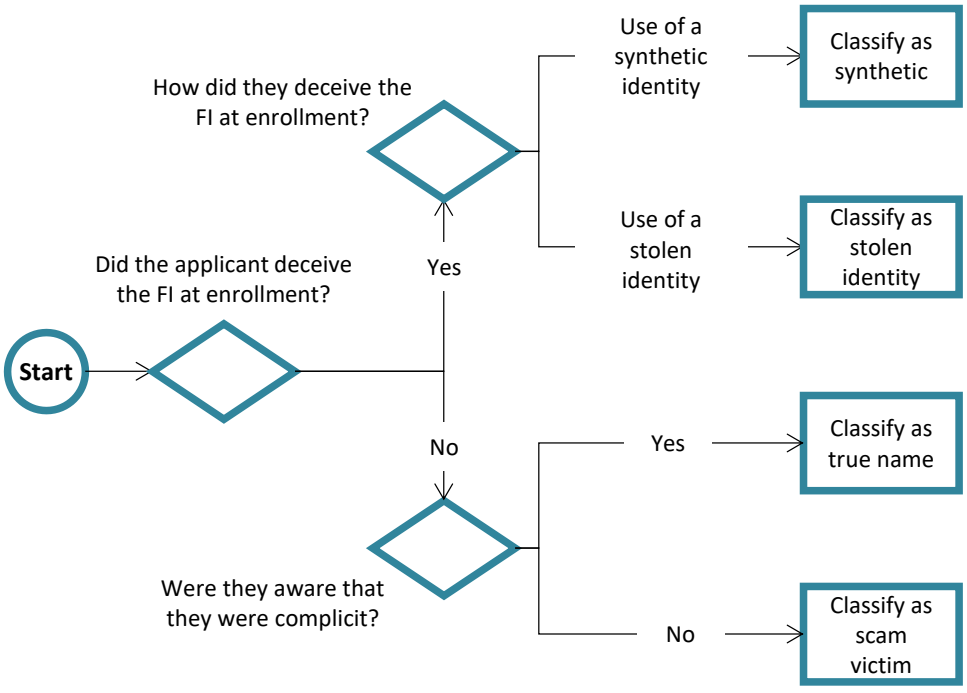
- **Classify the means of deception at the time of enrollment:** The objective of this stage is to establish whether and how the applicant deceived the FI at enrollment in order to classify the means that the bad actor used to defeat application fraud controls (Figure 3). It should be noted that if the applicant deceived the FI at the time of enrollment for the purpose of committing a crime or abusing the account at

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

any time after enrollment, then all outcomes of this stage must be described as "first party," meaning that it was the applicant's intent to deceive and, subsequently, to defraud the FI. For circumstances in which the applicant did not deceive the FI at enrollment and was later found guilty of committing a fraud or abusing the account, that is considered by many to be another form of first-party fraud. Only one circumstance results in an outcome that is not classified as a form of first-party fraud, and that is when there is evidence that the applicant was unwittingly duped or manipulated into committing the fraud or abuse by a third party. That circumstance is often classified as a scam (though, again, there is a tragic lack of well-established definitions that a majority of FIs agree to).

- **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 their deception in the enrollment process (Figure 4). These are referred to as the "manifestations" of application fraud.

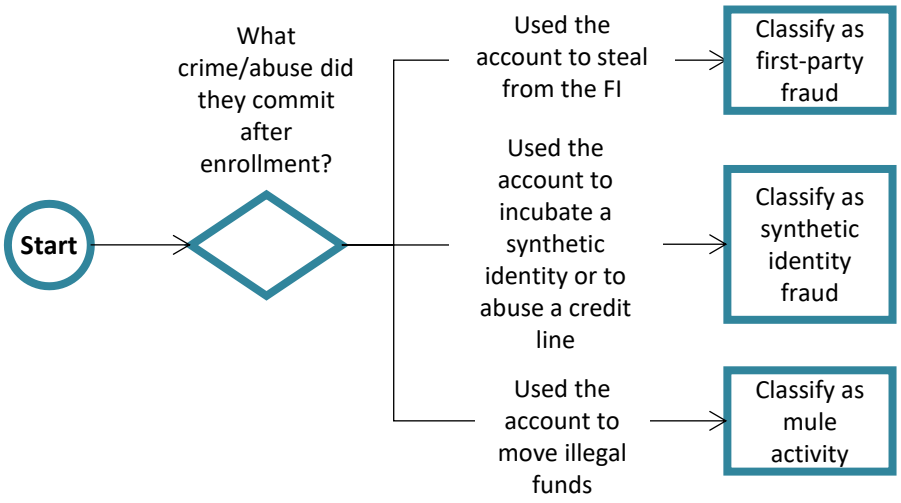
Figure 3: Conceptual Forensic Model for Classifying the Type of Deception Employed at Enrollment



Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

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 report, 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.

With those definitions and assumptions established, it's useful to also discuss the challenges that result from inconsistencies in definitions for the manifestations of application fraud events and how they're measured. While there is general agreement on high-level definitions for the more common forms fraud that result from application (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 often not measured at all.[6]

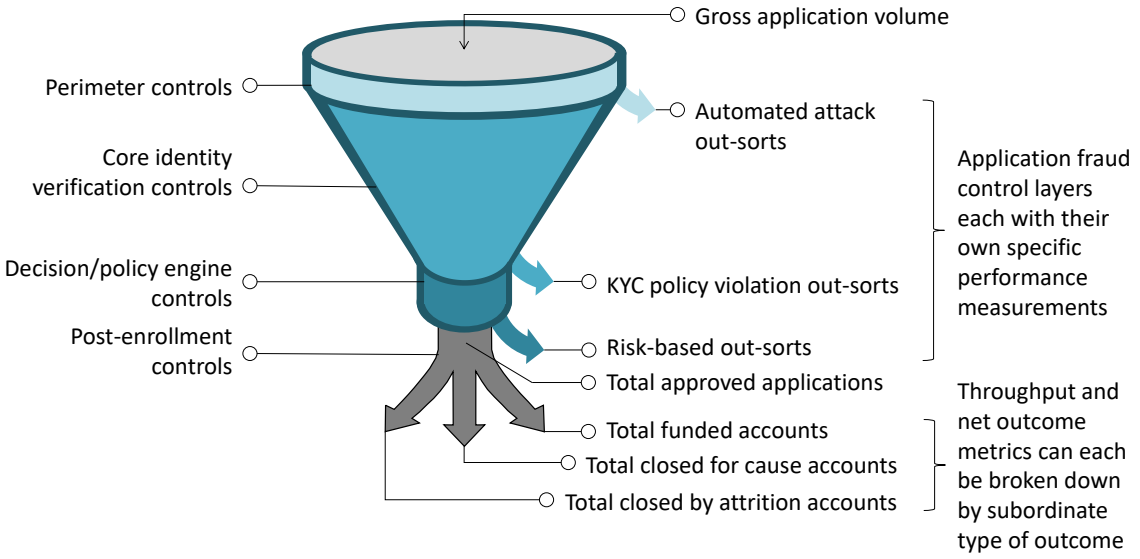
Despite this challenge, one of the objectives of the research for this report was to attempt to gather specific performance metrics that would provide a more detailed perspective on the trends in the specific kinds of attacks. Such an approach would also enable a much more effective means of quantifying and articulating the benefits that transforming application fraud control frameworks can have on loss reduction and also on the quality and health of the

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

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

portfolio. Regrettably, however, that objective proved to be a little too ambitious. 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

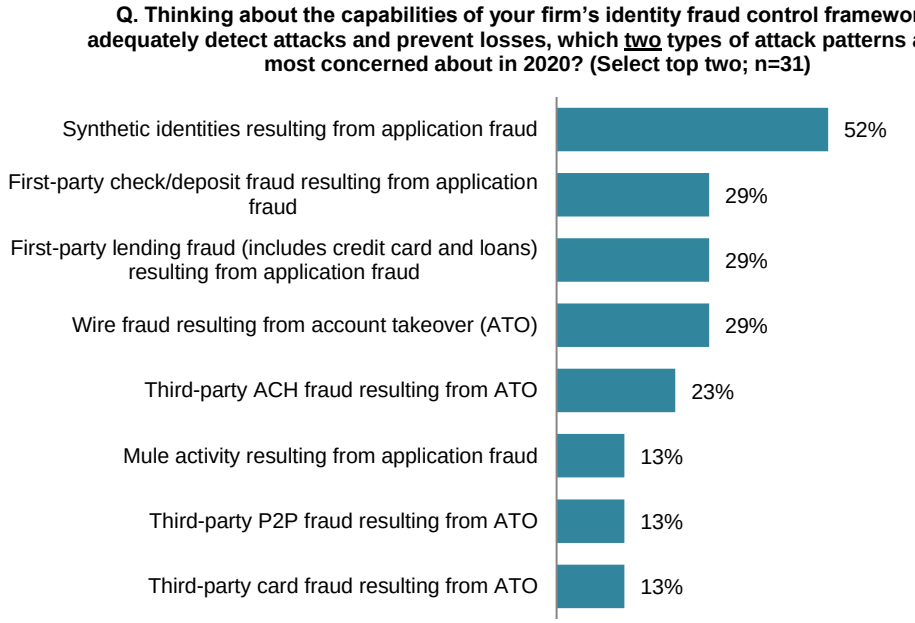
Whether this is a reflection of the siloed nature of application fraud frameworks, of the inadequacy of metrics and reporting capabilities, or simply of the lack of a standardized (and unanimously agreeable) benchmarking model is at least somewhat beside the point. The unfortunate truth is that when it comes to measuring the performance of application fraud frameworks, many in the industry have a way to go before they're able to 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 on those investments. The capacity to benchmark the performance of their frameworks 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 the 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 an Aite Group survey of 27 fraud

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

executives from 2019, the second most commonly cited pain point (33% of respondents versus 37% for the number one most commonly cited pain point) was application fraud.[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.

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]

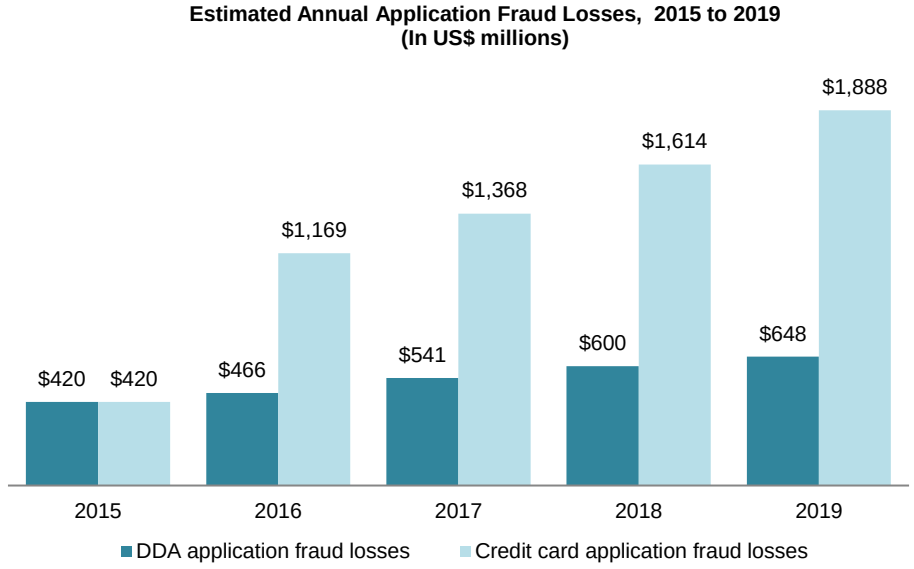
Estimates of application fraud losses based on data collected in 2016, 2018, and 2020 can be found in Figure 7.

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

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

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 7: Estimated Historical Application Fraud Losses



Source: Aite Group

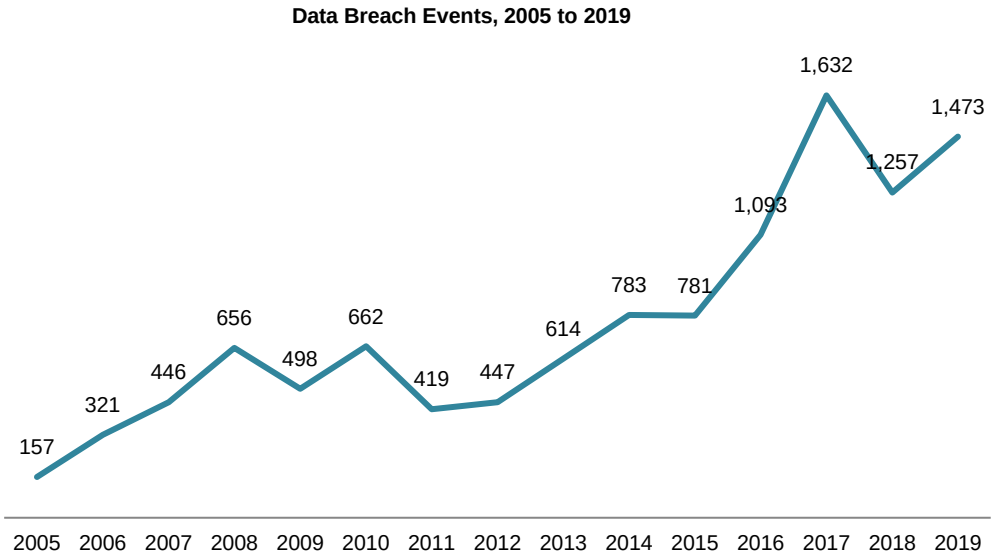
MARKET FORCES DRIVING APPLICATION FRAUD

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 significant 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, the foundational building block necessary for fueling 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.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 8: Rate of Increase in Data Breach Events



Source: Statistica.com

As long as there is an abundant supply of raw material in the form of personally identifiable information, 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.

ENVIRONMENTAL CONDITIONS DRIVING APPLICATION FRAUD

If the growth in application fraud is partly attributable to the market forces that shape the cost-benefit equation of the crime as a commercial enterprise, then an understanding of the nature of the growth would be incomplete without also examining the environmental conditions that contribute to growth. Unfortunately, 2020 has been an extraordinary year in terms of the kinds of environmental conditions that are favorable to identity-related fraud. To begin, consider the impacts that the pandemic has had on economic conditions and how those conditions impact the three primary manifestations of application fraud (Table B).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table B: The Impact of the Environmental Conditions of the Pandemic on Application Fraud

Environmental condition	Impact on first-party fraud	Impact on mule activity	Impact on synthetic identity fraud
Widespread lockdowns lead to spikes in unemployment	Increased risk that those who are made financially vulnerable due to unemployment might turn to fraud as a means of income.	Increased risk that those who are made financially vulnerable due to unemployment might be more susceptible to mule recruitment schemes.	In addition to being another enticing way to replace lost income, the demand for increased production is driven by increases in first-party fraud and mule activity
Federal and state unemployment stimulus and Small Business Administration (SBA) loans	Some of the Paycheck Protection Program (PPP) cases being prosecuted have the perpetrators using their own identities, setting themselves up as principals of sham companies to obtain PPP loans.	As fraud rings flock en masse to intercept government stimulus payments, they require significantly more money mules to shuttle the intercepted funds to accounts that are protected from recovery efforts.	Seeking to avoid the "human resources (HR) problems" associated with managing recruited mules, many fraud rings seek to use synthetic identities to establish mule accounts that they manage directly.
Sustained economic uncertainty and disruptions to social and commercial behavioral patterns	Increased risk of "good-client-gone-bad" scenarios as unemployment insurance payments wane and economic pressures increase.	Increased demand to support money movement related to an increase in ATO attacks resulting from large-scale increases in the volume of vulnerable "digital newbies."	Increased demand to provide identities for mule accounts supporting the movement of money from ATO attacks.

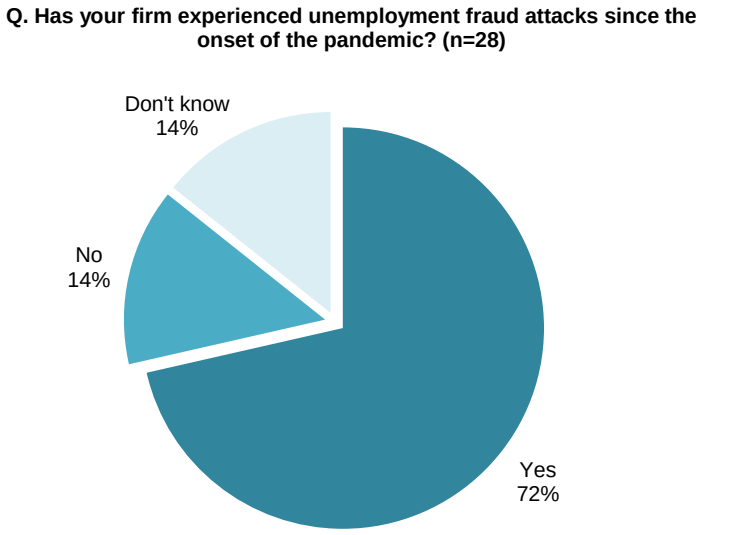
Source: Aite Group

Many fraud executives interviewed for this report agree that while it's hard to estimate the scale of fraud and waste from federal and state stimulus programs, they expect that it will be dramatic. Consider that even early-stage investigations by federal investigators revealed that as much as US$1.4 billion in unemployment stimulus checks went to individuals on the Social Security Administration's Master Death File.[10] Of the 47 FIs that participated in the fraud survey from Aite Group's 2020 Financial Crime Forum, 14 FIs report a total of US$160 million in estimated cumulative unemployment fraud payments observed since the start of the pandemic. Overall, 72% of the 28 fraud executives who responded report that their institution had been impacted by unemployment fraud (Figure 9).

10. Alan Rappeport, "$1.4 Billion in Stimulus Funds Sent to Dead People, Watchdog Finds," The New York Times, June 25, 2020, accessed October 16 2020, https://www.nytimes.com/2020/06/25/us/politics/coronavirus-stimulus-dead-people.html.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

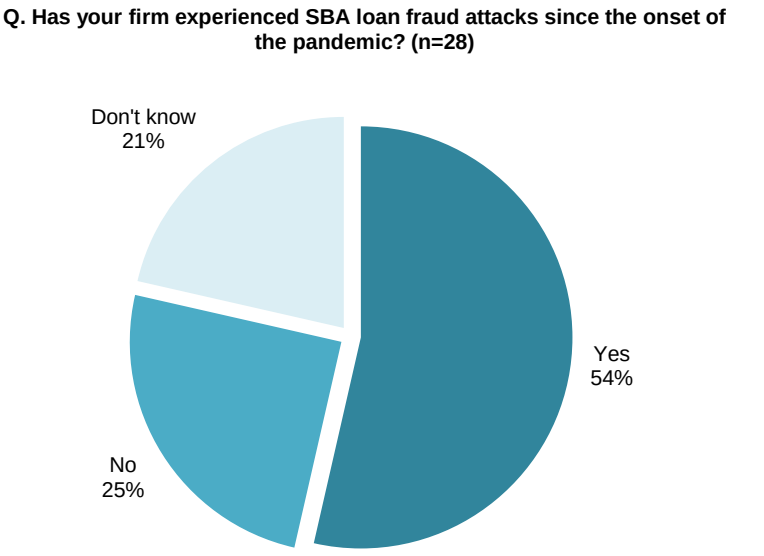
Figure 9: Distribution of FIs Impacted by Unemployment Fraud



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

Another 11 of the 47 FIs report an estimated US$60 million in PPP fraud observed at their institutions since the start of the pandemic. Of the 28 fraud executives who responded, 54% report that their institution has been impacted by SBA loan fraud (Figure 10).

Figure 10: Distribution of FIs Impacted by SBA Loan Fraud

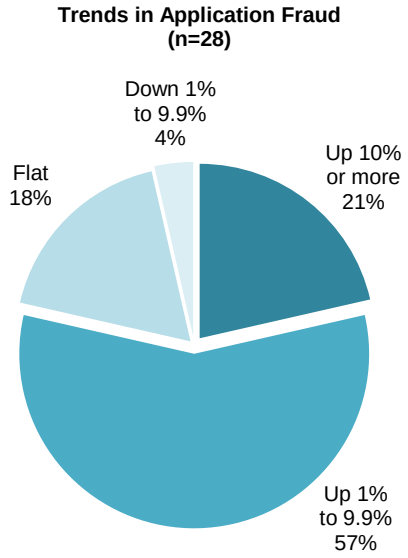


Source: Aite Group's survey of 47 financial services fraud executives, September 2020

Regardless of the scale of the impact of these programs, the majority (78%) of the 28 fraud executive respondents at the Financial Crime Forum report increases of varying degrees in application fraud in 2020 compared to pre-pandemic rates (Figure 11).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 11: Distribution of Application Fraud Attack Rates



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

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 they provide for fraud rings as well as a means of refining the raw material, personally identifiable information, into a form that can be repurposed for use in many other forms of identity fraud, including deposit fraud and mule activity. 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.[11] 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.

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 remains elusive, there are few doubts among fraud executives that the fraudsters are making liberal use of them

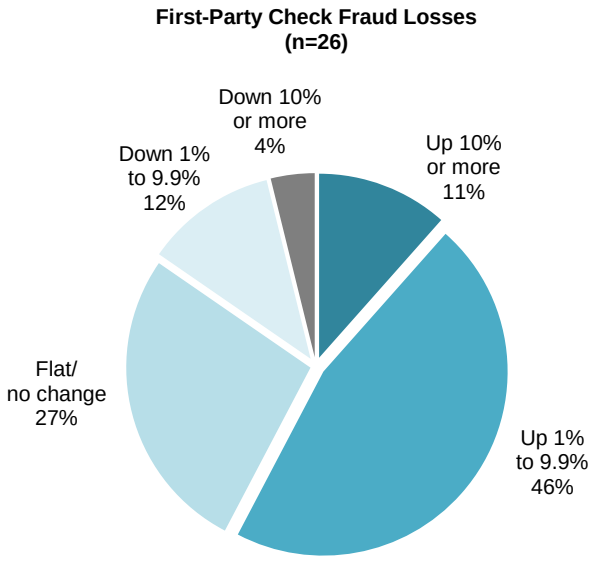
11. See Aite Group's report *Synthetic Identity Fraud: The Elephant in the Room*, May 2018.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

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 goes on to comment 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.

Despite challenges in measuring the degree to which synthetic identity fraud plays a role in first-party check fraud, 57% of fraud executives report that losses are up between 1% and more than 10% from two years prior (Figure 12).

Figure 12: Trends in First-Party Check Fraud



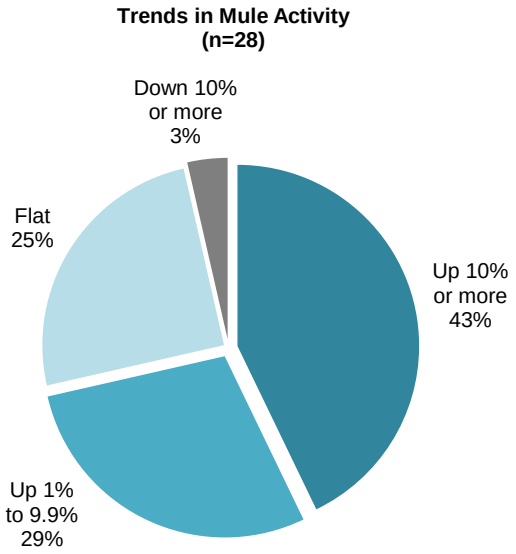
Source: Aite Group's survey of 47 financial services fraud executives, September 2020

Tracking mule activity suffers from the same challenge in many U.S. FIs,[12] 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, whereas synthetic identities provide a relatively low-cost means of establishing drop accounts that can be directly controlled by the fraud ring without what one fraudster on a dark-web forum chatroom referred to as the "messy HR problems" of dealing with recruited money mules. Regardless, the consensus among fraud executives is that the overall level of mule activity during the pandemic is significantly elevated over the rates of mule activity prior to the pandemic (Figure 13).

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

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

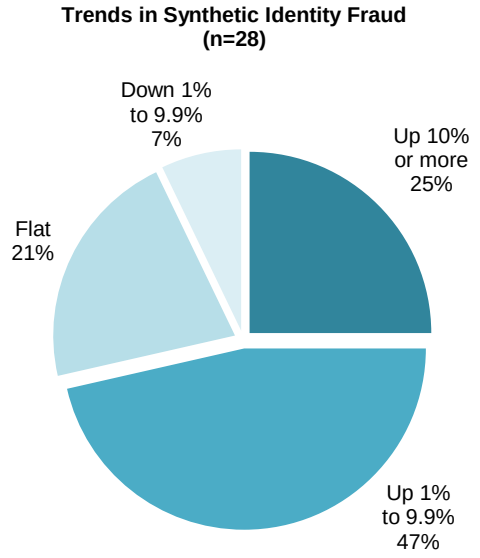
Figure 13: Rate of Increase in Mule Activity Since the Start of the Pandemic



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

Synthetic identity fraud continues to be perceived as a significant threat, and the rates of increase in synthetic identity fraud among the three dominant manifestations of application fraud reflect the same overall rates of increase as mule activity (Figure 14).

Figure 14: Rate of Increase in Synthetic Identity Fraud Since the Start of the Pandemic



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

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

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

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 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

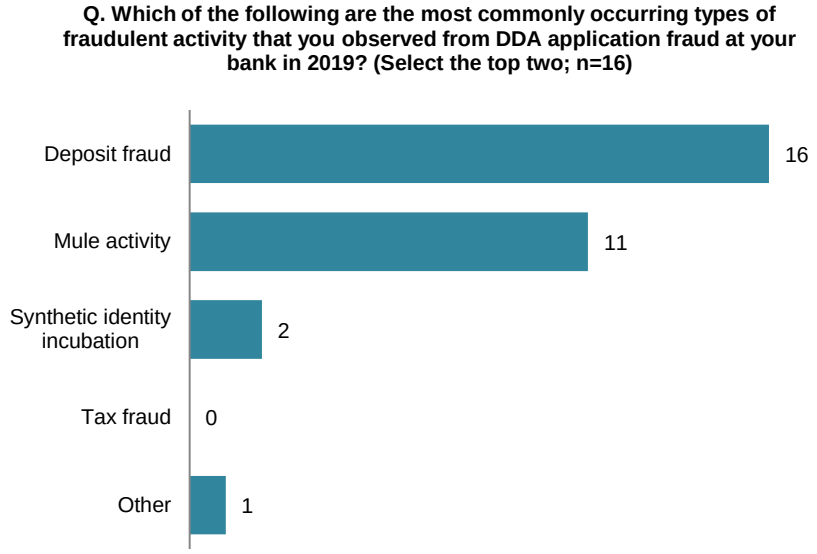
Analysis of application fraud trends isn't complete without breaking out the trends by the types of accounts that the fraudsters seek to exploit. While the derivative forms of application fraud that have been examined thus far have a tendency to skew toward one type of an account or the other, they are not exclusive to any particular one. Breaking down the trends by application type 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 and which, sadly, still remains a largely unfulfilled goal.

The absence of these standards resulted in inconsistent and often low rates of responses to questions that sought detailed performance indicators within specific components or segments of the application fraud control "funnel."

In analyzing the most common manifestations of DDA application fraud, it's helpful to examine the shifts in the kinds of activity from the pre-pandemic period to now. Figure 15 illustrates the trends in the most common manifestations of DDA application fraud in 2019, though it's worth noting that synthetic incubation may be understated since many FIs do not have robust controls for synthetic identity fraud within their DDA portfolios.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

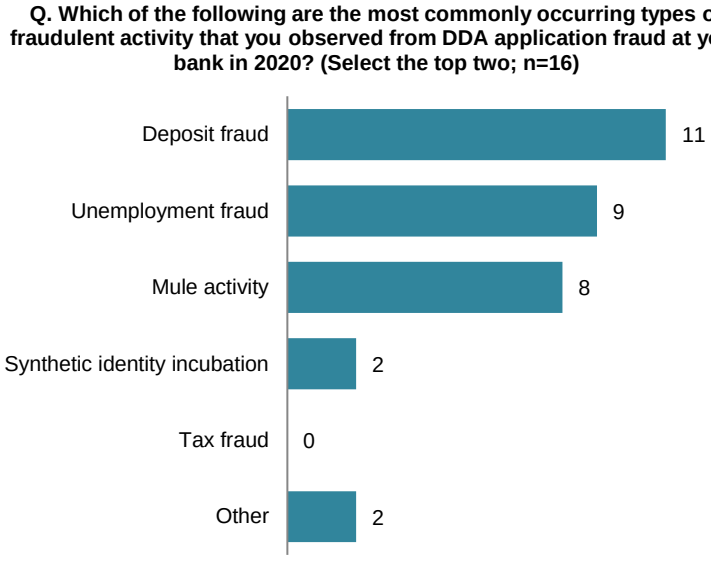
Figure 15: Most Common Forms of DDA Application Fraud in 2019



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

The fraudsters' shift in focus toward intercepting federal and state stimulus payments as the pandemic period unfolded appears to have shifted the distribution of the types of application fraud specific to DDA (Figure 16). While deposit fraud retained the top spot, unemployment fraud clearly became a real issue for FIs.

Figure 16: Most Common Forms of DDA Application Fraud in 2020



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

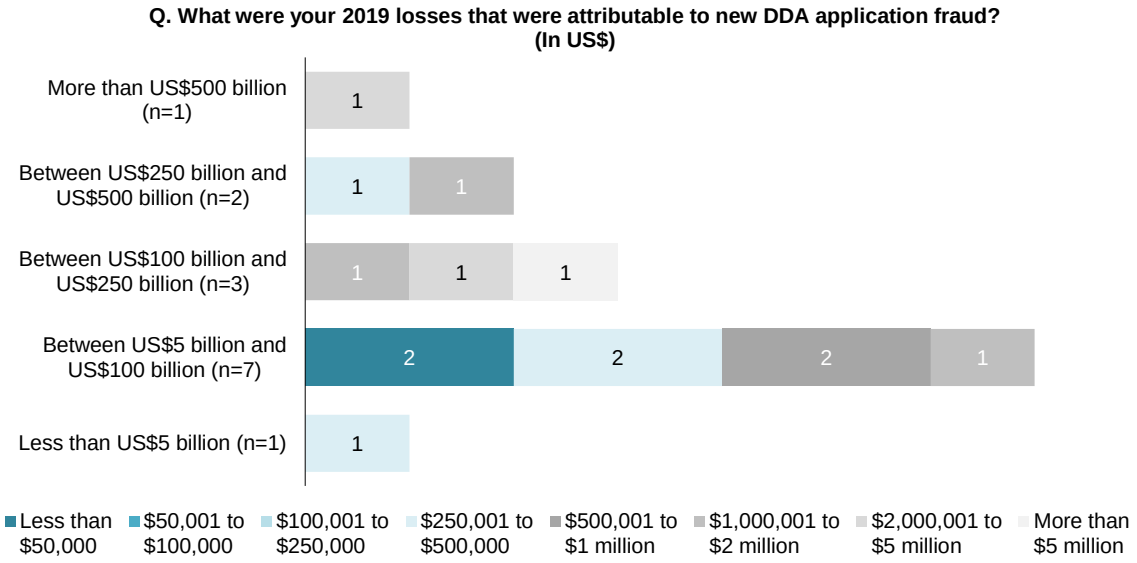
While it's tempting to jump to the conclusion that Figure 16 might suggest that mule activity became a less-common form of DDA application fraud, it's important to note that the question

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

was posed in such a way that required the respondent to choose only the top two types of DDA application fraud. That being said, however, the fact that deposit fraud retained the top spot over mule activity is surprising given the rates of increase that have been anecdotally reported during the pandemic period. Also worth noting is that tax fraud was not reported by any FI prior to or during the pandemic period as a common form of DDA application fraud, which is notable insofar as it's a type of fraudulent activity that often goes underreported. It's also likely that it's not commonly thought of as a manifestation of application fraud, or that it's lumped in with mule activity or even deposit fraud which, again, highlights the yawning gap in standardized definitions for measuring fraudulent activity in the U.S. market.

In terms of trends in DDA application fraud losses, it's helpful to examine them in the context of asset size (Figure 17).

Figure 17: DDA Application Fraud Losses by Asset Size



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

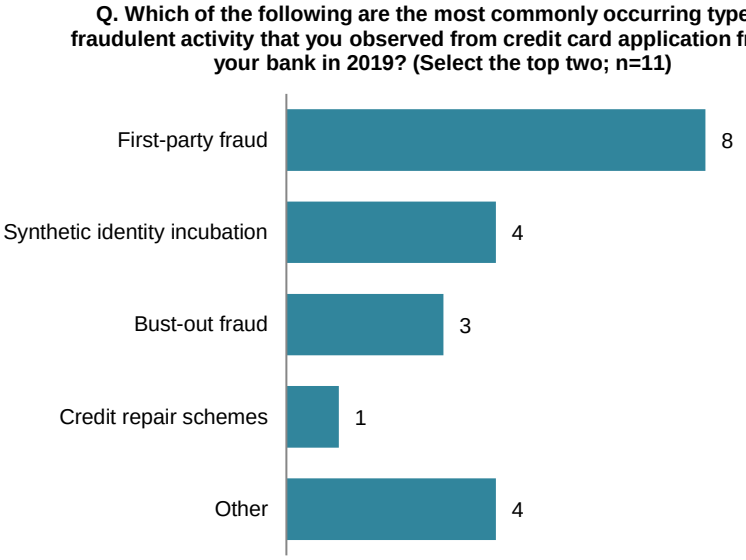
While the sample size is far from sufficient to plot a correlation, it nonetheless triggers the intuition to question whether a more robust analysis of the impact that various segments of the application fraud control framework have on losses within the constraints of application volume and asset size.

TRENDS IN CREDIT CARD APPLICATION FRAUD

While credit card application fraud has a range of fraudulent activity that is equally 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 18).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

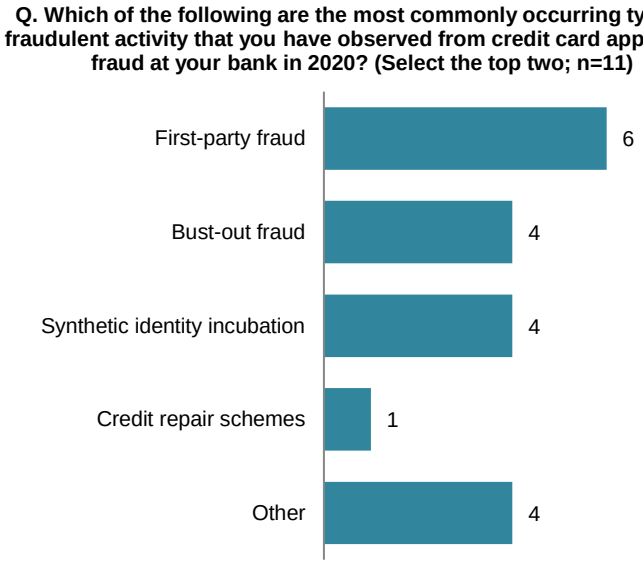
Figure 18: Most Common Forms of Credit Card Application Fraud in 2019



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

In terms of the impacts on the types of fraud that participants report resulting from the effects of the pandemic, there is evidence that forms of first-party fraud are edging upward (Figure 19). As was noted in the rate of first-party deposit fraud, at least some of this shift in activity can be attributed to deteriorating economic conditions for large segments of consumers. It's also worth noting, of course, that the same challenges in measuring synthetic identity fraud activity within a deposit portfolio are equally challenging for credit portfolios.

Figure 19: Most Common Forms of Credit Card Application Fraud in 2020

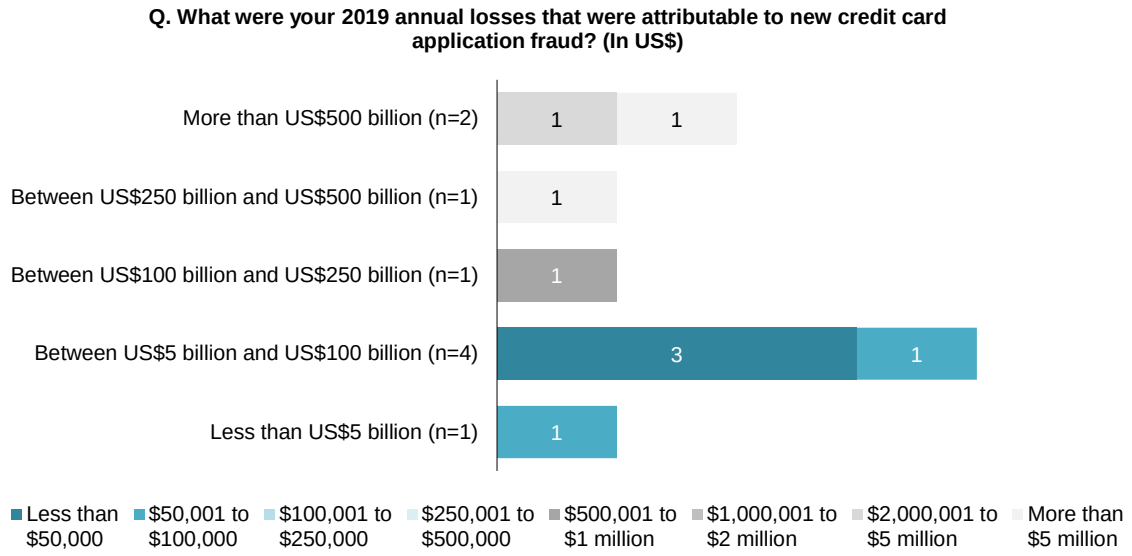


Source: Aite Group's survey of 18 FIs, July to September 2020

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

While the sample size of respondents was insufficient to provide a year-over-year comparison of loss trends, Figure 20 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 20: 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 drawn the conclusion that this growth will likely continue at least so long as the environmental conditions persist. In estimating the growth projections for application fraud, several assumptions were made and are worthy of note:

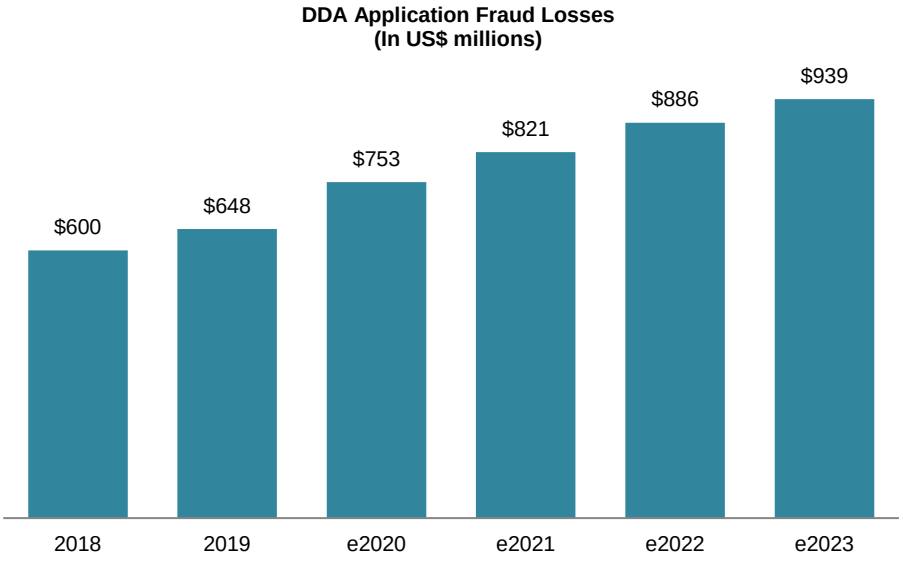
- The market forces that have been the primary growth driver and that have historically averaged roughly 16% per year in growth will remain relatively stable in terms of their weight of impact over time and are considered to be the baseline rate of increase.
- The rate of increase above or below the baseline rate of increase is estimated to be a function of the degree to which environmental conditions persist in creating a positive or negative impact on that baseline rate of growth.
- Synthetic identity fraud makes up the lion's share of total application fraud volume, and the rate of growth in synthetic identity fraud is driven primarily by overall market forces and secondarily by environmental conditions.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- While baseline estimates for the overall volume and rate of growth in synthetic identity fraud were based on estimated ratios between them and overall credit charge-off rates, the projected rates of growth in synthetic identity fraud are estimated independently from the ratios that were used to establish baseline estimates. As overall credit charge-off rates begin to accelerate as the economic impact of the pandemic unfolds, whatever correlative relationship there may have been between credit charge-off and synthetic identity fraud will collapse as overall credit charge-off rates are likely to far outstrip the rate of growth in synthetic identity fraud.
- The economic conditions that result from the pandemic are likely to provide upward pressure on growth rates through 2021 and well into 2022 but will begin to return to rates of growth similar to pre-pandemic levels by 2023.

The projections for DDA application fraud and credit card application fraud were estimated separately. Figure 21 projects application fraud losses for DDA application fraud to hit US$939 million in 2023.

Figure 21: Estimated and Projected U.S. FIs' DDA Application Fraud Losses

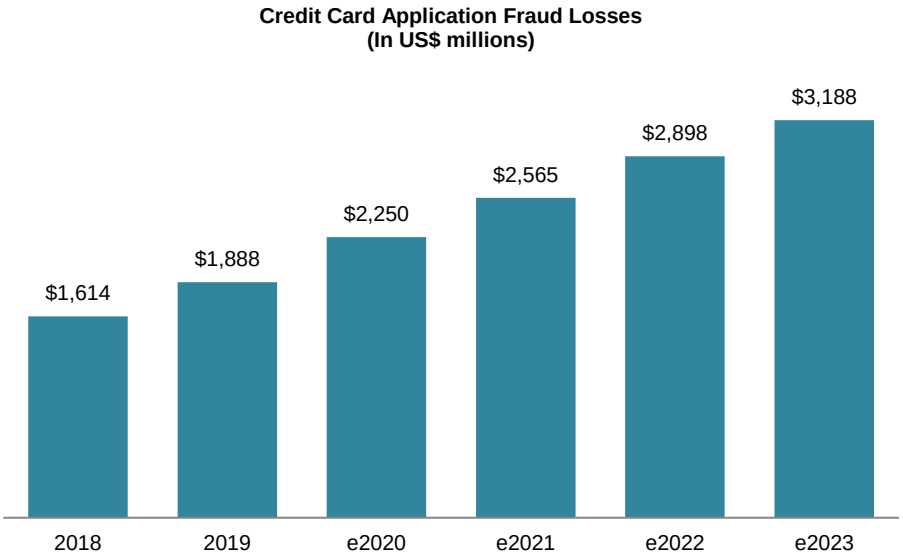


Source: Aite Group

Figure 22 projects credit card application fraud losses to reach US$3.188 million by 2023, driven predominantly by synthetic identity fraud losses.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 22: Estimated and Projected U.S. FIs' Credit Card Application Fraud Losses



Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

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.

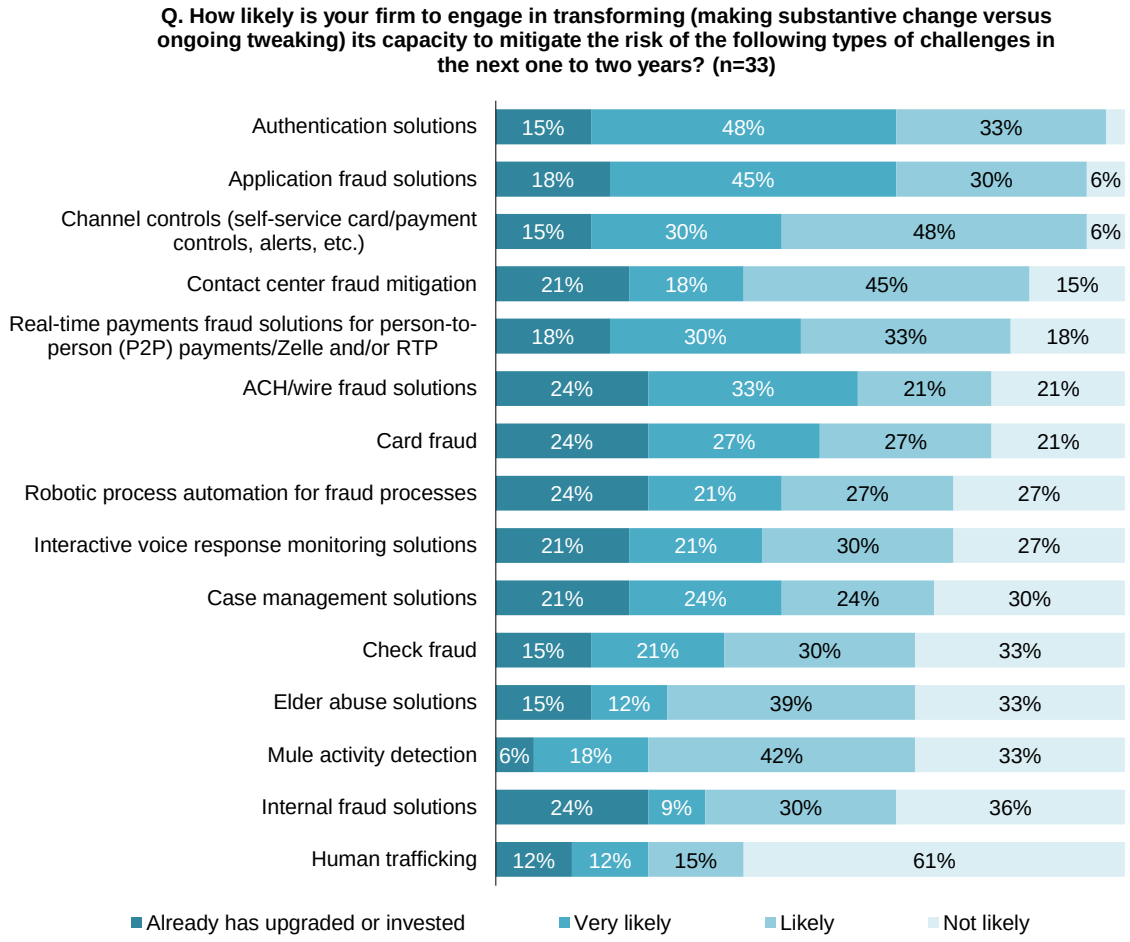
To better understand why this is the case, consider what one fraud executive interviewed for this report relayed about a firm's efforts to build support for investments in application fraud controls. In the early stages of the effort to make the case for renovating the firm's application fraud control 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 credit to his analysts for demonstrating to his peers how examining the profitability of the portfolio in such 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."

It's important to note that the fraud executive made a particular effort to establish or modify the means of measuring false-positive rates, enrollment throughput, and account profitability. In fact, the fraud executive reports that "it took a lot of effort" to work with analytics units that served the firm's peers' business units in the interest of establishing a mutually agreed-upon specification for capturing these metrics and their subordinate components. He went on to say, though, that having a shared vocabulary that everyone agreed upon was an accurate reflection that the health of the portfolio was worth the investment of resources.

Considering the relative rate of transformation in application fraud controls across the industry (Figure 23), 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.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 23: Likelihood of Transformation of Capacity to Mitigate Risks in the Next Two Years

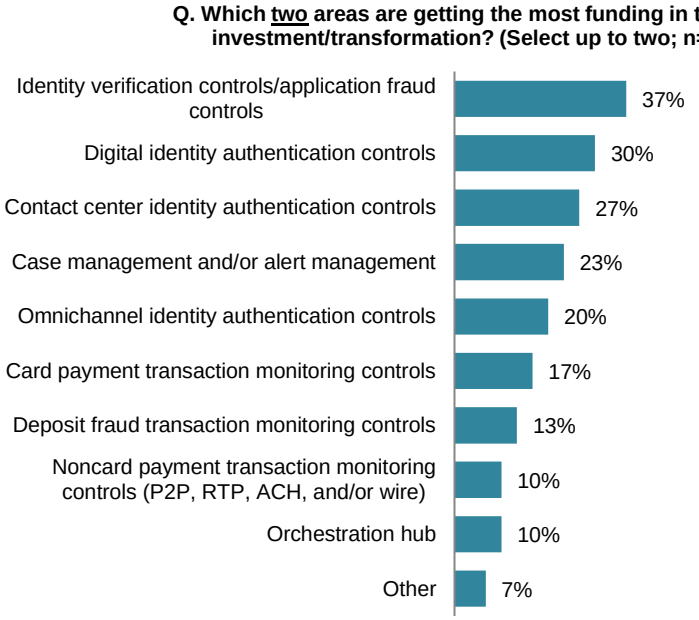


Source: Aite Group's survey of 47 financial services fraud executives, September 2020

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 24).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 24: Areas of Investment Receiving the Most Funding



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

SUPPORTING REVENUE GROWTH

The considerable pressure to support revenue growth objectives by way of optimizing new client acquisitions is a motivating force for strengthening the layers of identity verification controls. The challenge for many FIs is whether to augment existing layers of control or to "rip and replace" aging systems in favor of one or more emerging solutions that work alone or in concert with one another in such a way that significantly outperforms the legacy solutions at the FI. Complicating this challenge is whether to deploy a common infrastructure that can be leveraged across DDA and credit-line application processes. Regardless, the overriding objective is to deepen and broaden the span of layers of control for verifying the identity. For a growing majority of FIs, this means expanding the number and nature of identity data sources with a particular emphasis on those that focus on the applicant's digital identity and elements that are tangential to it, such as device-related characteristics and network-related characteristics (e.g., mobile network operator signals).

The net result of this on the market for identity verification controls has been twofold. First, FI investment dollars are increasingly favoring those vendors either with strong digital identity data sources (if the FI is looking to augment existing capabilities) or with strong digital and conventional data sources (if the FI is looking to rip and replace existing infrastructure with something that can boost accuracy and/or increase its capacity to target "thin file" applicants). Second, solution providers are actively expanding their digital identity capabilities either through organic growth natively within their solution or through acquisition. While there are a great

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

variety of ways to segment the solution providers in the space of identity verification,[13] particularly in the context of the degree to which the solution enables the augmentation of existing capabilities or whether it's more suited as a means of replacing existing capabilities, Table C provides a list of the most common identity verification solution providers that have developed functionality that includes the native capacity to verify personally identifiable information (as opposed to solutions that provide this functionality by way of integration with a third party) and that can support either or both of those demands.

Table C: Identity Verification Vendors

Vendors				
Acuant	Acxiom	Early Warning Services	Ekata	Equifax
Experian	GBG	ID Insight	IDology	LexisNexis Risk Solutions
Melissa Data	MicroBilt	Neustar	Pipl	Prove
Socure	TransUnion			

Source: Aite Group

REENGINEERING CLIENT EXPERIENCE

In addition to supporting revenue growth objectives, there have also been significant pressures on business units within FIs to reengineer client journeys that are competitive with digitally native disruptors that are skewing consumer expectations of onboarding and identity recognition. One needn't even go outside the industry for an example of this trend. Consider the onboarding process sponsored by Apple Incorporated's Apple Card unit and hosted by Goldman Sachs. Like many of the emergent digital-first fintech firms, FIs, and products in the past few years, particular attention was paid by product managers and process engineers to the application process with the objective of minimizing many of what one fraud executive described as "high-friction identity verification steps" commonly found in most conventional application processes among FIs today. The trend is clearly toward eschewing many of the overtly invasive steps in the application process and favoring investment in controls that operate in a way that another fraud executive described as "behind the curtain." The net result of this trend has been an emphasis among FIs on investing in behavioral biometrics solutions (Table D), device fingerprinting solutions (Table E), and mobile device authentication solutions (Table F). All of the solution providers listed are those that have native functionality and that do not rely on integrations with third parties for the service in question.

13. See Aite Group's report *The Digital Channel Under Attack: How to Protect Yourself and Your Customers*, June 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table D: Behavioral Biometric Solution Providers

Vendors				
Arkose Labs	BehavioSec	BioCatch	buguroo	Callsign
FICO	IBM Trusteer	ID R&D	IDMERIT	Incognia
Kofax	Neothone	Neuro-ID	NuData Security	Optimal IdM
Precognitive	Samsung SDS	SecuredTouch	ThreatMark	TypingDNA
XTN				

Source: Aite Group

Table E: Device Fingerprinting Solution Providers

Vendors				
Accertify	Arkose Labs	buguroo	Callsign	Cleafy
Daon	DataVisor	Entersekt	Entrust Datacard	Experian
FraudHunt	IBM Trusteer	Incognia	IPQualityScore	LexisNexis Risk Solutions
MaxMind	Neothone	Neustar	NuData Security	OneSpan
Oneytrust	Precognitive	RSA Security	SEON	ThreatMark
TransUnion	XTN			

Source: Aite Group

Table F: Mobile Device Authentication Solution Providers

Vendors				
Accertify	Boku	Callsign	Equifax	Experian
LexisNexis Risk Solutions	Neustar	Next Caller	OneSpan	Prove
Pindrop	RSA Security	Socure	Thales	TrustID
Zumigo				

Source: Aite Group

DEFENDING AGAINST BOT ATTACKS

Another significant objective that has been influential in shaping the market for application fraud controls is 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 personally identifiable information from identity theft victims, or synthetic identities either manufactured or purchased from online marketplaces. Fortunately, though, there are a

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

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 G lists the solution providers who specialize in this area.

Table G: 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

ADDRESSING THE GAME OF "WHACK-A-MULE"

Another trend that has been a driving force behind market trends in the application fraud control market has been the persistent and growing challenge of arresting the movement of bad actors from one FI to the next. One fraud executive voices a perspective, echoed by a handful of other fraud executives, that consortium-based account abuse databases hold untapped potential to make material impacts on the game of "whack-a-mule" that FIs have found themselves playing as serial account abusers and money mules move from one FI to the next. The fraud executive explained that as consumer protection oversight tightened around FIs' contributions of "closed for cause" events to consortium-based account abuse databases in the wake of the financial crisis of 2008, the perception was that there was an industrywide contraction of reporting to consortia-based suspicious identity, account abuse, and known fraudster database providers that are compliant with Fair Credit Reporting Act (FCRA) guidelines (Table H). The fraud executive concluded that while these tools are exceptionally useful in identifying serial account abusers today, they have a great deal of untapped potential in arresting the movement of these bad actors from one institution to the next if participating FIs were given better guidance around the do's and don'ts of labeling abuses in more detail. In summary, the sooner the industry is able to share more detailed information about the nature of what these serial offenders have done, the sooner those in the industry will be able to "reduce the profitable commodity of mules."

Table H: North American Consortia-Based Suspicious Identity, Account Abuse, or Known Fraudster Data

Vendors				
Early Warning Services	Experian	FIS	LexisNexis Risk Solutions	Visa

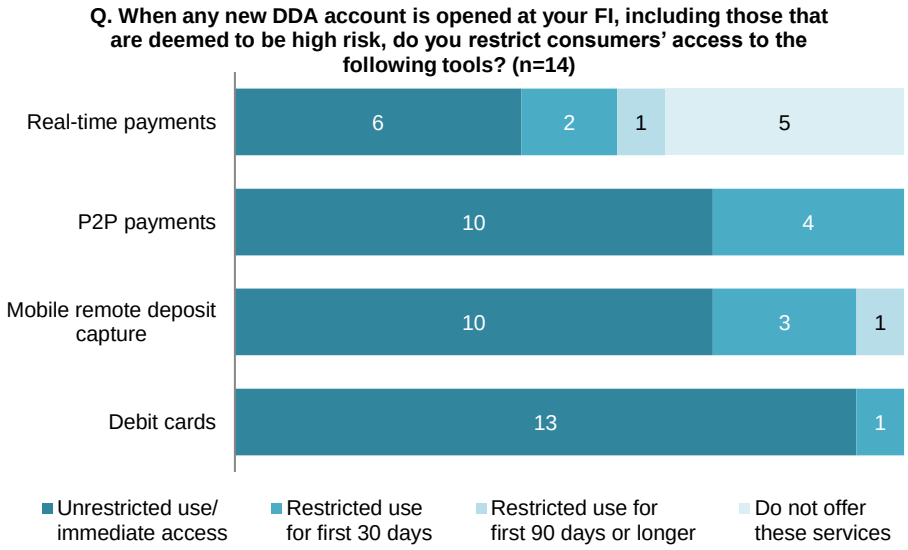
Source: Aite Group

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

EXPANDING POST-ENROLLMENT CONTROLS

One of the most compelling reasons for investing in application fraud controls is the notion of "front-loading" the broader fraud control framework. Conventional wisdom holds that the better one performs in detecting attempts to deceive at the proverbial front door, the more likely one is to prevent bad actors from gaining access to the means of committing downstream acts of fraud. In summary, the stronger the perimeter defense layers are, the less stress will be placed on inner layers of defense. True as that may be, no fraud executives worth their salt would leave inner layers of their defenses neglected. At least one manner in which this approach manifests itself is in policy-based controls that are linked to new accounts. Figure 25 illustrates the degree to which participants in the application fraud survey have deployed policy-based controls for the purpose of restricting new accounts to instruments or services that are commonly believed to be vulnerable to exploitation by first-party fraud attacks.

Figure 25: Distribution of Policy-Based Controls on Account Features



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

Another emerging trend in this space is the concept of a longitudinal identity risk engine. Most risk engines that are deployed to function as a means of automating risk-based assessments of applicants are designed to fire once at the entry point of the account life cycle. The assumption is that once applicants have passed the test necessary to verify their identity, inner layers of control (such as those deployed to monitor deposits for indications of deposit fraud) should be sufficient to secure the FI from attack. For fraud types such as first-party fraud, in which transaction monitoring controls are capable of providing the necessary added layers to compensate for losses, this assumption holds up well. For fraud types in which there are fewer inner-layer controls (if any at all), this assumption fails. Such is the case with synthetic identity fraud and mule activity.

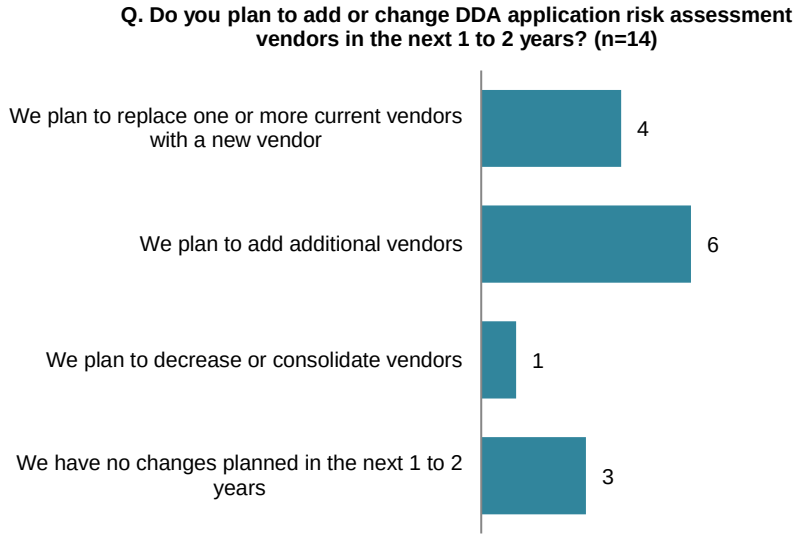
101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

The concept of a longitudinal identity risk engine has the potential to fill the gap between application fraud controls and transaction monitoring controls, especially for mule activity and synthetic identity fraud that are, at most FIs in the U.S. market, poorly controlled for. A longitudinal identity risk engine would accomplish this by continually evaluating the risk of an identity on day one and every day thereafter throughout the life cycle of the identity's tenure with the FI. In addition to the intelligence accumulated during the application process, the longitudinal identity risk engine would accumulate the kinds of channel interaction and monetary transaction patterns that could automate risk decisions for various forms of first-party fraud, mule activity, and synthetic identity fraud. As many practitioners are aware, patterns of nonmonetary interactions are, in and of themselves, insufficient to trigger interdiction efforts, but with the right analytics and tuning they have been proven to be an effective means of improving the accuracy of predicting which accounts should be placed on watch lists. This, in turn, improves the capacity to take swift and decisive action if or when a suspect monetary transaction presents on the account associated with the identity.

TRENDS IN APPLICATION FRAUD CONTROL SOLUTIONS

If there is a silver lining to the rates of application fraud increases, it primarily takes the form of the pace of innovation and the expanding diversity in application fraud solution providers. If there is such a thing as a "typical application fraud control framework," then it could be said that there has been a great deal of change in terms of both the quantity and mix of solutions that comprise its constituent components over the last few years. The consensus among the fraud executives interviewed for this report is that the quantities of solutions for DDA application fraud are expanding more so than the replacement or reduction in control solutions (Figure 26).

Figure 26: Plans to Change DDA Application Fraud Controls

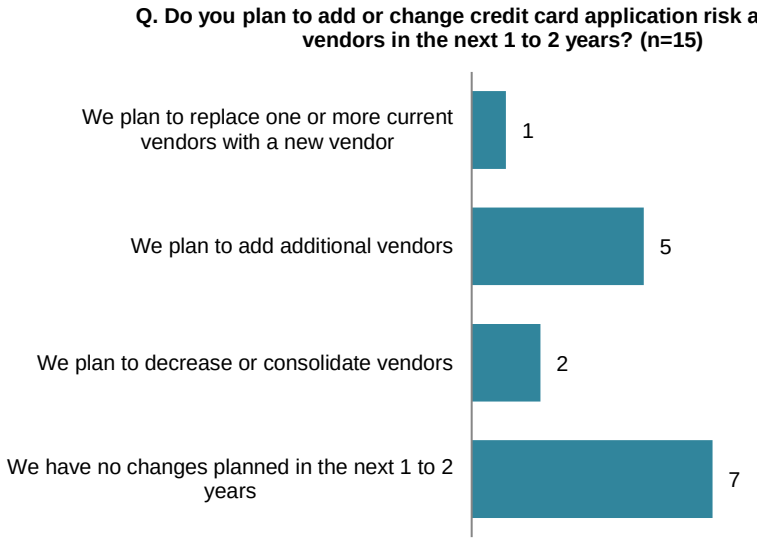


Source: Aite Group's survey of 18 FIs, July to September 2020

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

While there is still a fair amount of additive changes being made to credit card application fraud controls, there is also evidence that fraud executives have already deployed the countermeasures necessary to address the gaps in their credit card portfolios (Figure 27).

Figure 27: Plans to Change Credit Card Application Fraud Controls



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

In terms of the mix of solutions for DDA application fraud controls, many fraud executives report high rates of satisfaction with consortia-based suspicious identity, account abuse, or known fraudster data providers as well as with behavioral biometric and device identity solutions. One notable recurring theme in interviews is the trend toward deprecating those controls that are perceived to not only be less effective at detecting application fraud but that also generate friction in the application process. Despite this trend, it's worth noting that dynamic knowledge-based authentication (KBA) remains an active and still commonly used control solution at many FIs for DDA application fraud (Figure 28).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 28: Distribution of DDA Application Fraud Controls

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

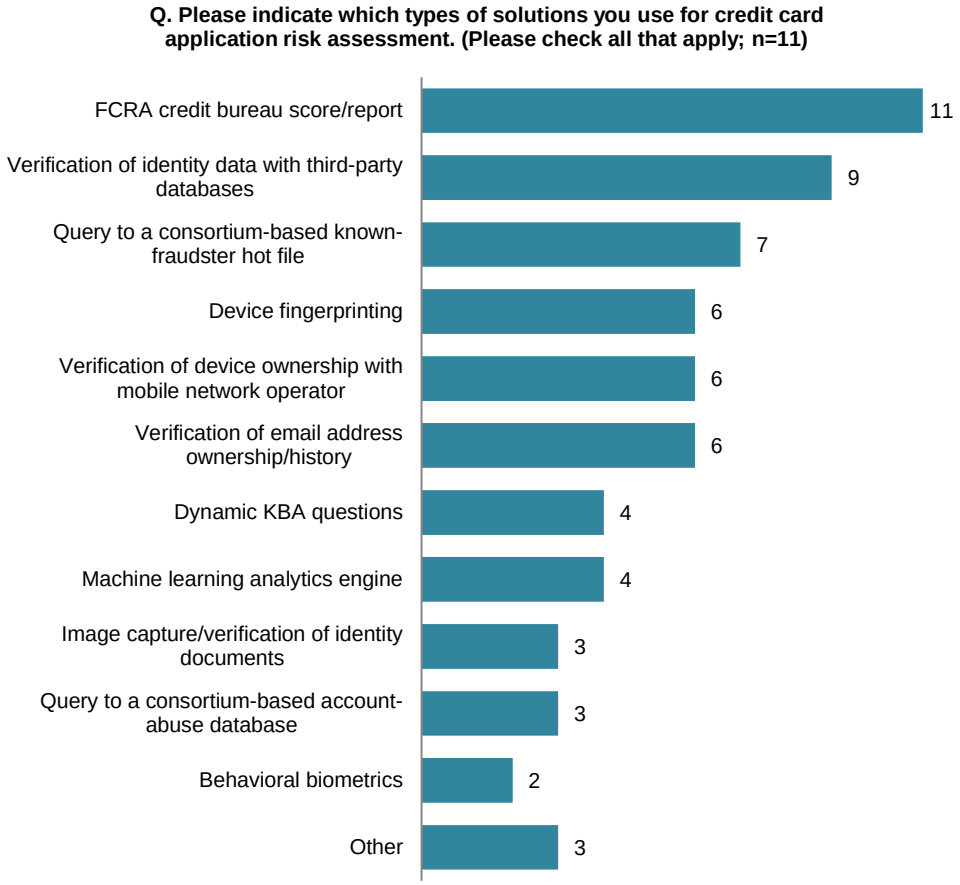
It's worth briefly explaining the rationale behind the move away from controls that introduce friction into the process in general, and KBA in particular. Fraud executives have been growing frustrated with KBA largely because many have analyzed its performance only to discover that it is often the source of complaints from clients and channel partners, and also because it has become less effective as a means of accurately detecting fraudsters.[14] To illustrate this frustration, one fraud executive from a large U.S. FI says that the firm "threw a party" after a years-long effort to sunset its KBA controls wrapped up.

Fortunately for those who manage credit card application fraud, KBA appears to be less of a factor (Figure 29). This is presumably, again, due to the notion that many FIs have prioritized transforming credit card application fraud controls over DDA application fraud controls.

14. See Aite Group's report *Market Trends in Digital Fraud Mitigation*, December 2019.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Figure 29: Distribution of Credit Card Application Fraud Controls



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

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

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; it 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.
- Despite the fact that many FIs are still a long way from being able to easily articulate detailed performance metrics of their application fraud control frameworks, there is a trend among many toward developing a more holistic perspective of performance in this important area.
- A tragic lack of standards remains in industrywide definitions for the kind of performance metrics that are well suited to provide a more granular view of the degree to which application fraud controls contribute to loss avoidance and to revenue growth.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RELATED AITE GROUP RESEARCH

The Digital Channel Under Attack: How to Protect Yourself and Your Customers, June 2020.

Mule Activity: Find the Mules and Stop the Fraud, April 2020.

Market Trends in Digital Fraud Mitigation, December 2019.

Synthetic Identity Fraud: The Elephant in the Room, May 2018.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

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

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com