Aite PARTNER. ADVISOR. CATALYST.

Application Fraud: Trend Analysis and Mitigation Challenges

NOVEMBER 2020

Prepared for:

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

Application Fraud: Trend Analysis and Mitigation Challenges, commissioned by Early Warning Services and produced by Aite Group, examines the market, economic, and environmental trends impacting application fraud and its derivative forms of criminal activity, and the challenges faced by practitioners in mitigating the risk posed by these trends.

Key takeaways from the study include the following:

- Market forces have led to steady increases of approximately 16% per year in application fraud attack rates.
- Environmental conditions brought about by severe economic and social disruptions resulting from the COVID-19 pandemic since April 2020 have accelerated growth in application fraud rates as demand among financial criminals for money mules and bank accounts associated with stolen and synthetic identities has increased to support the movement of fraudulently intercepted payments from government stimulus programs.
- 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 financial institutions (FIs) have enjoyed the benefits of investment strategies that have prioritized transformation efforts around identity verification (IDV) 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.

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 and fraud 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 FIs across the globe for the last five years, and there is evidence that it is has gotten significantly worse in 2020. This white paper examines the latest trends in application fraud in DDA and credit card accounts, how U.S. FIs are managing these risks, and why investments in application fraud controls continue to be among those with the most appealing business cases.

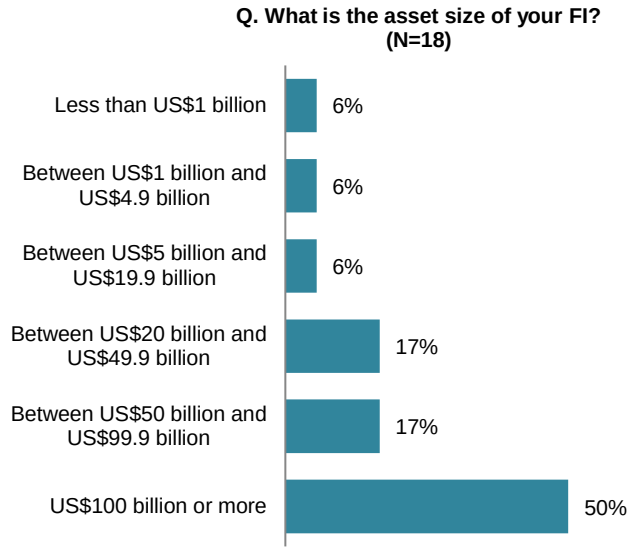
METHODOLOGY

Aite Group conducted research using an online survey engineered to collect data for both DDA application fraud and credit card application fraud. That survey was deployed between July 2020 and September 2020 with responses from 18 FIs in the U.S. Another survey engineered to collect a variety of fraud trend data was deployed in September 2020 to examine trends in application fraud more generally. The data reflects input from 47 financial fraud executives from 30 financial services firms. With one exception (Thailand), these financial institutions are in North America. In addition, several interviews with fraud executives at these and other FIs supplemented the data gathered from both surveys. Asset sizes of the participating FIs range from under US$1 billion to over US$100 billion. A distribution of FIs by asset size that participated in the application fraud survey can be seen in Figure 1. This Impact Report represents a refresh of research previously conducted in late 2015 for a report published in March 2016[1] and a report published in December 2018.[2]

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



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

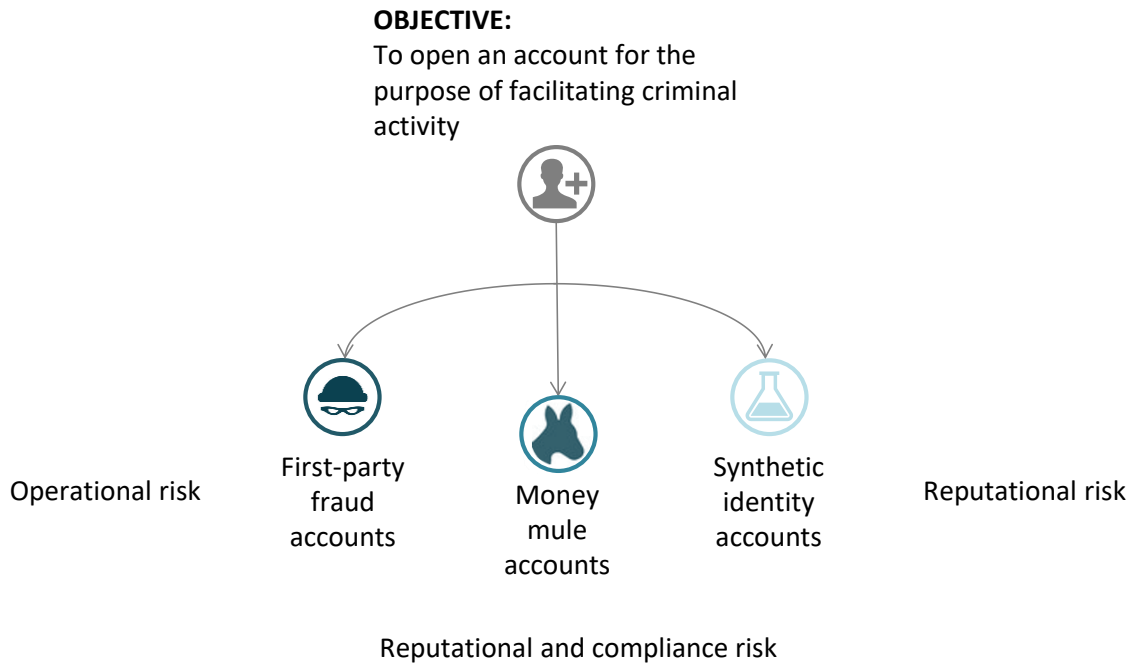
Given the size and structure of the research sample, the data provide a directional indication of conditions in the market.

APPLICATION FRAUD TRENDS

The unfortunate truth is that fraud is a growth industry. Estimating the rate of that growth has been an elusive challenge except in relatively isolated corners of the domain such as those, like card fraud, that enjoy an unusual amount of discipline in terms of how loss metrics are defined and consistency in terms of how they are recorded across practitioners. The net result of this lack of structure and consistency in fraud metrics and benchmarking has been an unfortunate absence of clarity among practitioners in seeking to better understand their performance relative to those of their peers. Additionally, while reports from 2016 and 2018 on application fraud have provided perspectives on trends on the topic as a whole, few insights have been shed on the derivative forms of fraud that result from application fraud.

In an effort to define the challenge more deliberately and to structure the analysis more precisely, it's helpful to reference a conceptual model for application fraud and how the primary derivative forms of fraud that stem from it relate to the concept (Figure 2). Armed with a more deliberate model for conceptualizing the threat and a more precise method for articulating how the threat manifests itself, it's possible to examine not only the overall impact of application fraud but also the severity and distribution of those impacts.

Figure 2: Application Fraud Conceptual Model

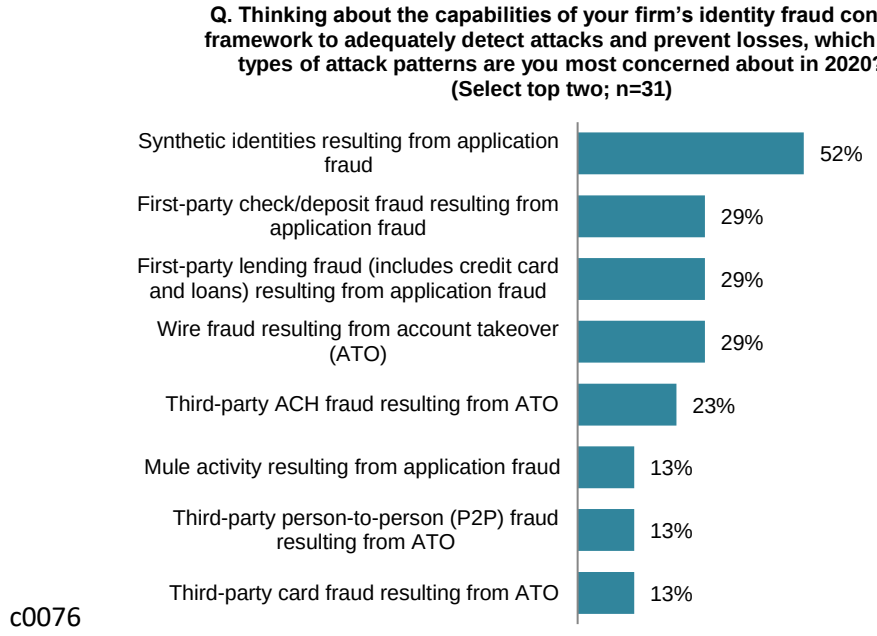


Source: Aite Group

Though the manner in which the challenge of application fraud has been articulated has changed over the years since Aite Group has analyzed the topic, 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 survey of 27 fraud 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. 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 3). Synthetic identity fraud resulting from application fraud, first-party lending fraud resulting from application fraud, and first-party check fraud resulting from application fraud make up three of the top four forms of attack patterns that concern fraud executives the most in 2020.

Figure 3: Attack Patterns That Concern Fraud Executives the Most

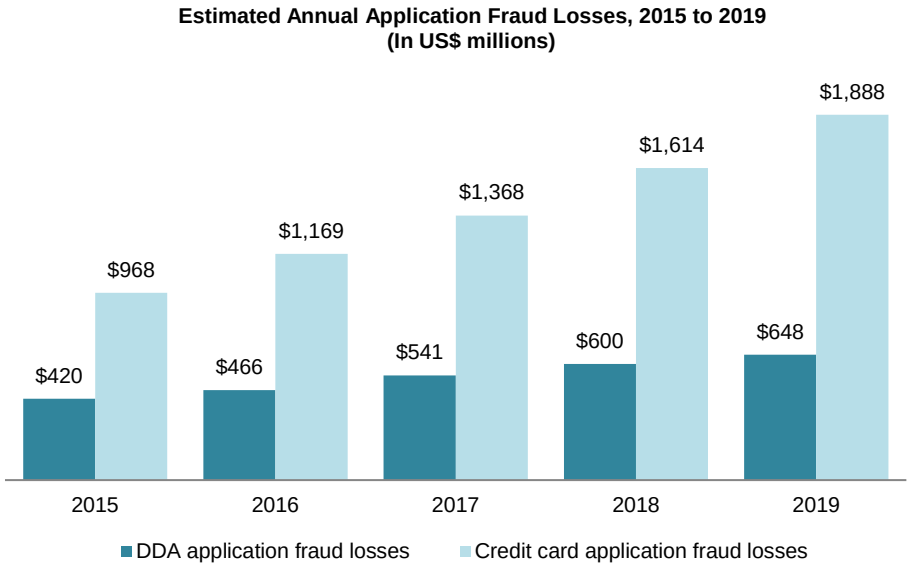


Source: Aite Group's survey of 47 FIs, September 2020

Estimates of total application fraud losses were initially put forward in Aite Group's report on the topic in 2016.[3] The estimates of application fraud losses based on data collected in 2016, 2018, and 2020 can be found in (Figure 4).

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

Figure 4: Estimated Annual Application Fraud Losses From 2015 to 2019

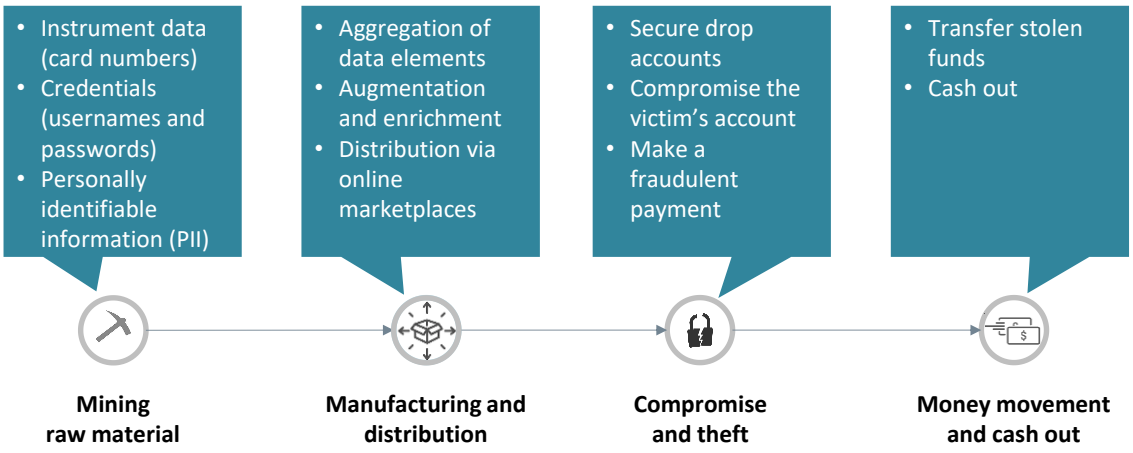


Source: Aite Group

MARKET FORCES IMPACTING APPLICATION FRAUD

It's important to acknowledge that the coronavirus pandemic of 2020 has impacted many types of fraud but has had a particularly profound impact on application fraud. Prior to analyzing those market forces, however, it's also important to examine the market forces that were clearly driving application fraud attack rates and losses upward well before—and independently of—the significant disruptions introduced by the pandemic. Here, again, it's helpful to break out application fraud into its derivative forms and examine how each was subject to elemental economic forces acting on the value chain that underlies financial crime as an enterprise (Figure 5).

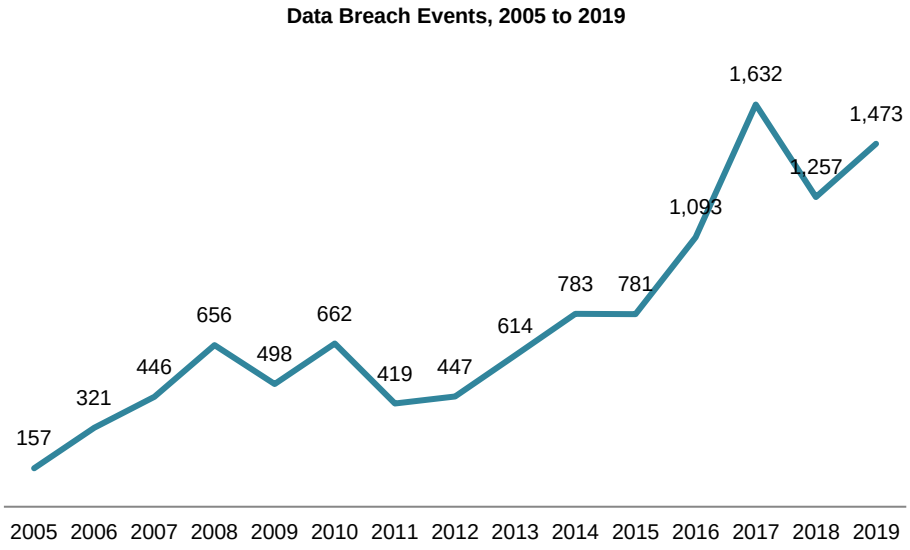
Figure 5: The Financial Crime Value Chain



Source: Aite Group

Perhaps the most significant market force stimulating growth in application fraud prior to and during 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 PII—the foundational building block necessary for fueling all identity fraud—has plateaued over the last few years but remains at a very accessible rate of between US$4 and US$10 per identity[4] 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 6).

Figure 6: Data Breach Events



Source: Statistica.com

The market forces driving 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 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 ever-lowering 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.

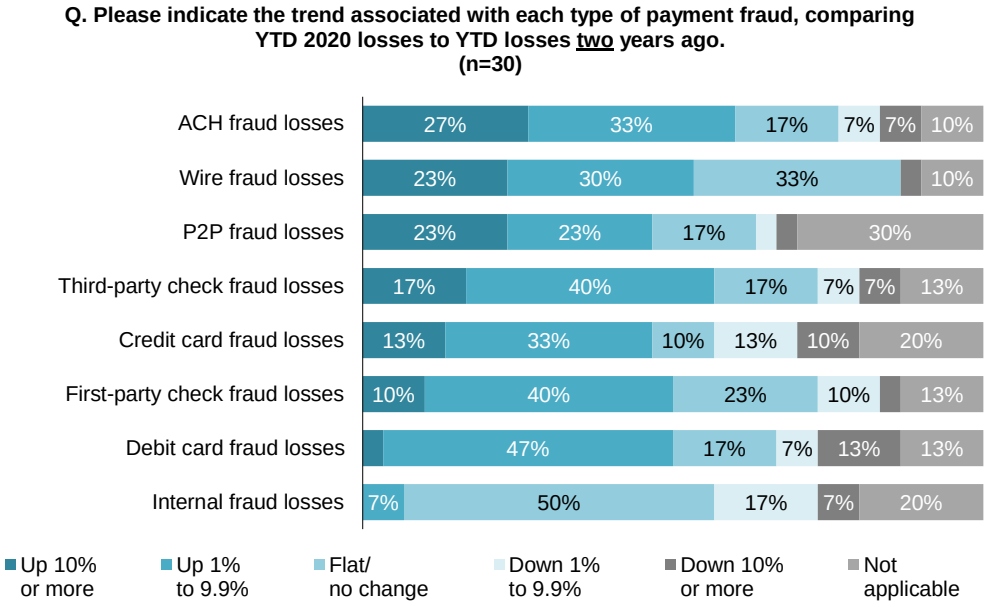
Growth in synthetics is a function of the significant amount of revenue that they provide for fraud rings as well as a means of refining the raw material, PII, into a form that can be repurposed for use in many other forms of identity fraud, including deposit fraud and mule

4. "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.

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.[5] The majority (US$1.2 billion) of the US$2.2 billion in total estimated credit card application fraud losses for 2020 in Figure 8 are derived from synthetic identity fraud losses.

While precise estimates of the portion of first-party check fraud losses 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 synthetics to perpetuate those schemes. One fraud executive interviewed for this white paper estimates that approximately one-third of his firm's deposit fraud losses were attributable to synthetic identities. He went on to comment that it was difficult to say exactly what the impact was because the firm was still developing a consistent means of recording and tracking the prevalence of synthetics in its investigations. Despite challenges in measuring the degree of synthetic identity fraud in first-party check fraud (deposit fraud), 50% of fraud executives report that losses were up from 1% to more than 10% from two years prior (Figure 7).

Figure 7: Trends in First-Party Check Fraud



Source: Aite Group's survey of 47 FIs, September 2020

Tracking mule activity suffers from the same challenge in many U.S. FIs,[6] 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, which are often external to the primary

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

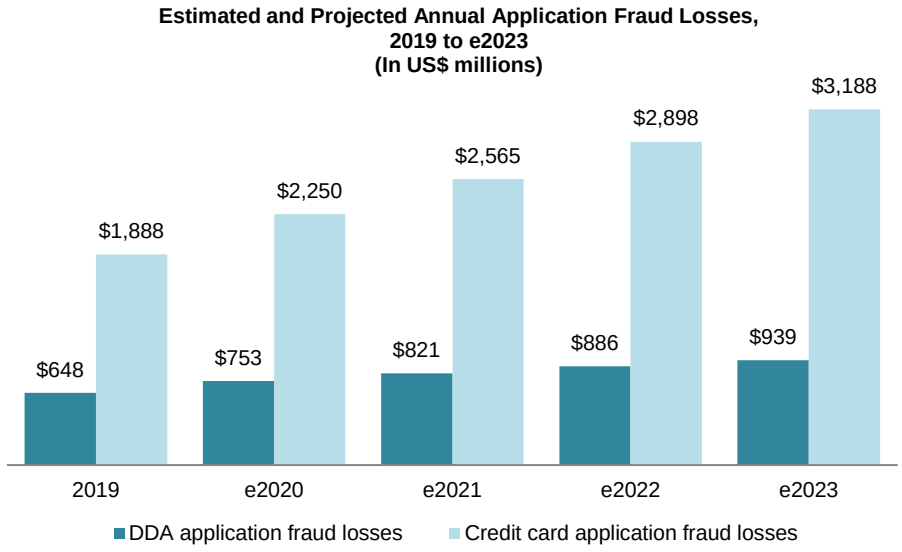
6. See Aite Group's report *Mule Activity: Find the Mules and Stop the Fraud*, April 2020.

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 chat room refers to as the "messy human resources problems" of dealing with recruited money mules.

ENVIRONMENTAL FORCES IMPACTING APPLICATION FRAUD

While growth in application fraud has followed a steady upward trajectory—averaging around 16% per year from 2015 to 2019, which was largely attributable to favorable market and economic conditions—the pandemic and the disruptions associated with it have contributed significantly as accelerants. Many of the variables that impact projections of application fraud losses that stem from these accelerants remain unknown—the total amount of credit charge-off and the portion of synthetics for the period therein being chief among them. The projections of application fraud losses, therefore, are based on a relatively conservative increase of approximately 18% in 2020 based on data collected for this white paper (Figure 8) on the assumption that while total credit charge-offs have a correlative relationship with rates of synthetic identity fraud, they are not a causative force.

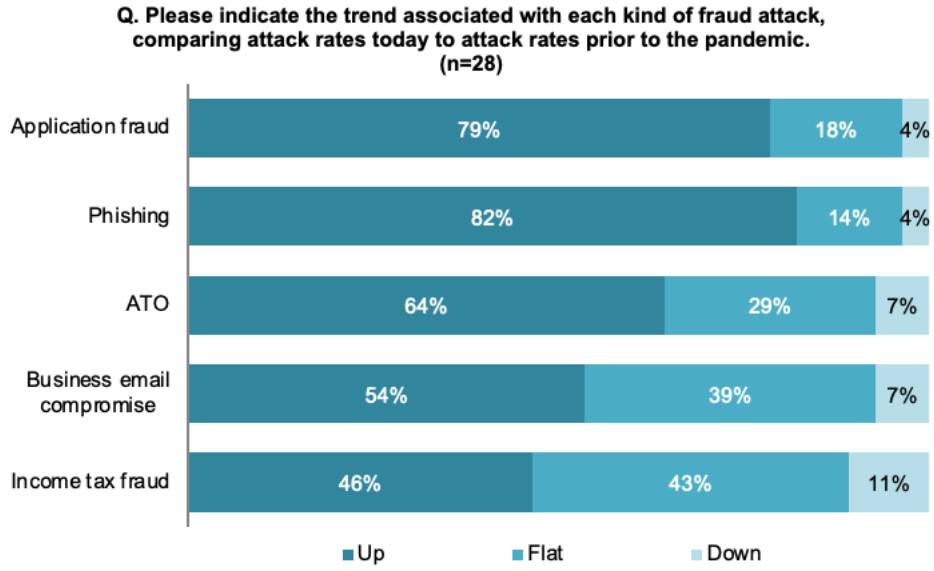
Figure 8: Impact of the Global Pandemic on Projected Application Fraud Losses



Source: Aite Group

What is clear is that there are unmistakable signs that application fraud as expressed by the derivative forms of fraud has accelerated since the pandemic began. The majority of respondents from a survey of 47 fraud executives from U.S. FIs reveal that they have experienced increases in application fraud since the pandemic began (Figure 9).

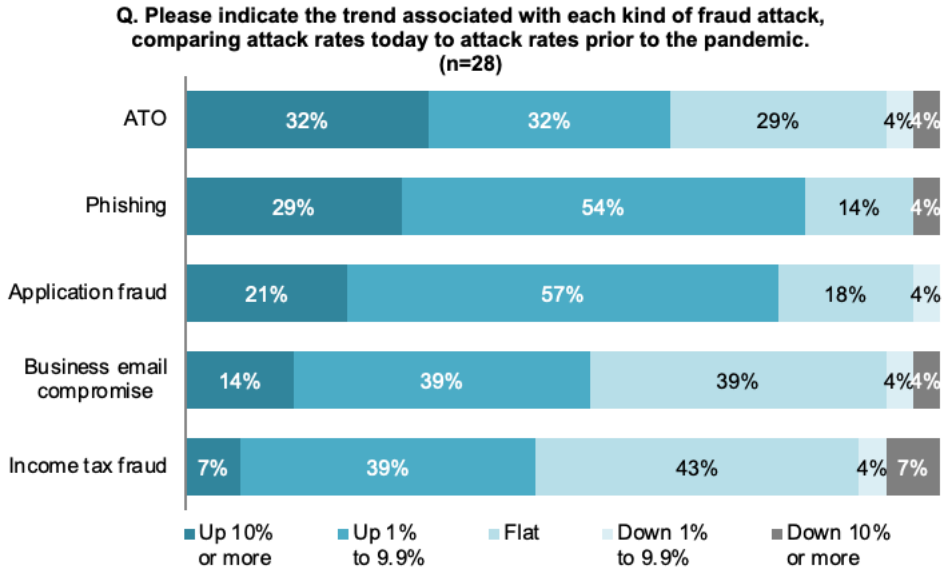
Figure 9: Trends in Fraud Attack Rates During the Pandemic



Source: Aite Group's survey of 47 FIs, September 2020

A closer look at the distribution of the rates of increase in application fraud attacks during the pandemic reveals that it was second only to ATO in terms of the severity of increases, with 21% of FIs reporting increases of more than 10% and 78% of FIs reporting increases in attack rates (Figure 10).

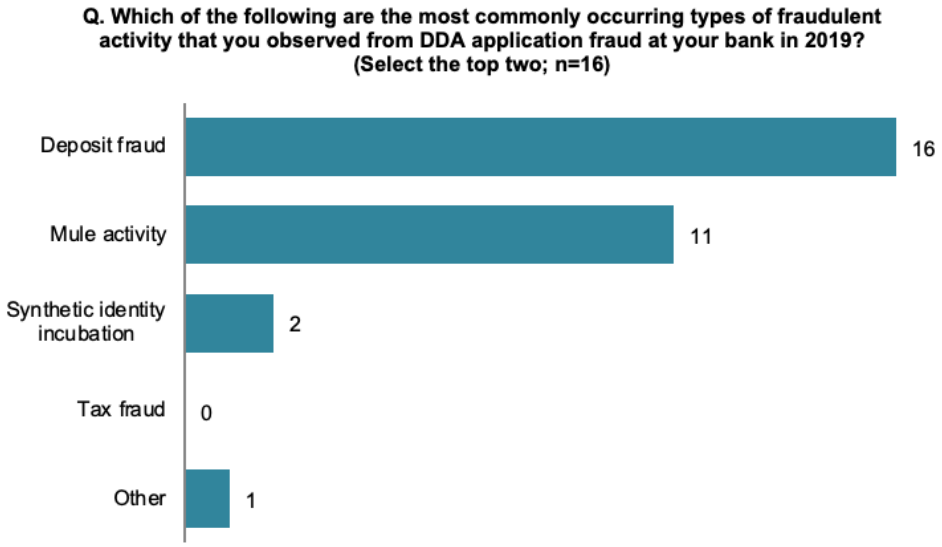
Figure 10: Distribution of the Rates of Increase in Application Fraud Attacks During the Pandemic



Source: Aite Group's survey of 47 FIs, September 2020

In terms of root cause of the increases in application fraud, it's helpful to compare the rates of increase in the types of fraudulent activity associated with DDA and credit card application fraud from before the pandemic with those reported after the pandemic. Prior to the pandemic, deposit fraud and mule activity dominated as the most common types of fraudulent activity associated with DDA application fraud (Figure 11).

Figure 11: Most Common Occurring Types of Fraudulent Activity Observed From DDA Application Fraud Prior to the Pandemic



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

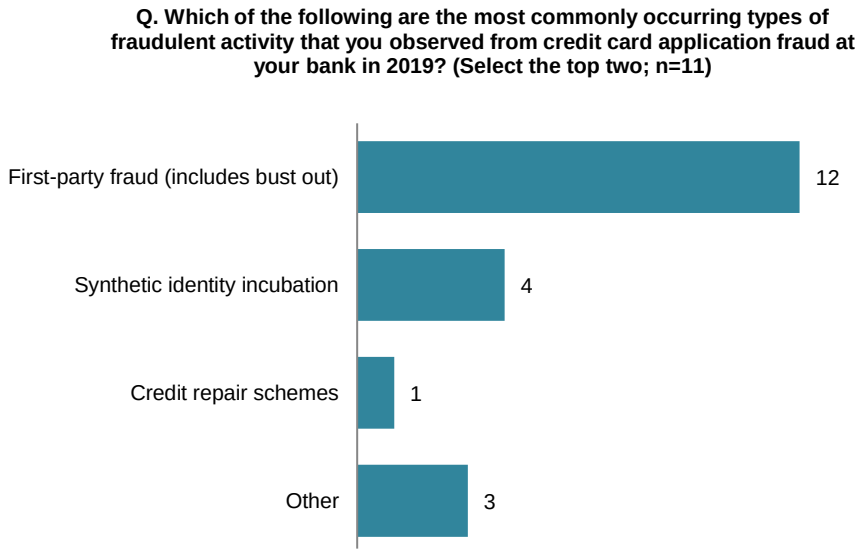
While deposit fraud retained the top spot among the types of fraudulent activity observed to be associated with DDA application fraud, it lost some ground to unemployment fraud—a phenomenon that has emerged as an area of great concern for many fraud and anti-money laundering executives as the proceeds of fraudulently intercepted government stimulus programs, including unemployment insurance and the Paycheck Protection Program (PPP), flow through the financial system (Figure 12).

Figure 12: Most Commonly Occurring Types of Fraudulent Activity Observed From DDA Application Fraud During the Pandemic

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

The distribution of the types of fraudulent activity associated with credit card application fraud remained stable throughout that transition from the pre-pandemic period to the pandemic period (Figure 13). Those responses that reported "other" were primarily responses indicating that they did not have the capacity to accurately report on the specific kinds of fraudulent activity associated with their application fraud.

Figure 13: Most Commonly Occurring Types of Fraudulent Activity Observed From Credit Card Application Fraud Before and During the Pandemic

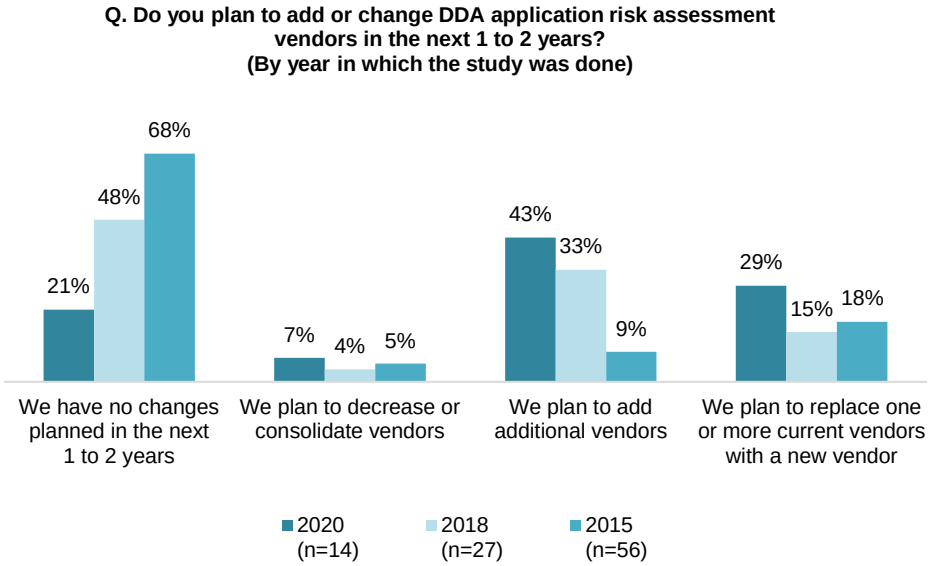


Source: Aite Group's survey of 18 FIs, July to September 2020

APPLICATION FRAUD MITIGATION CHALLENGES

Many FIs have benefitted from investment strategies that have prioritized transformation or expansion of the segments of their KYC control framework that revolve around IDV controls. The trend in investment shows little sign of slowing. Of the 14 fraud executives who responded to the question of whether they have plans to change their DDA application risk assessment vendors in the next one to two years, six report that they plan to add more vendors, and four report that they plan to replace one or more vendors. Another fraud executive reports that the firm has plans to reduce vendors in its control framework as older, less effective forms of IDV are augmented or replaced with those that have proven to be more effective and less intrusive in the account opening process. The overall trend of emphasizing investment by adding more layers to the application fraud control framework (Figure 14) reflects the strategic value of application fraud controls, which FIs recognize as a prophylactic means not only of reducing fraud losses but also of improving the account opening client experience and the revenue streams associated therein.

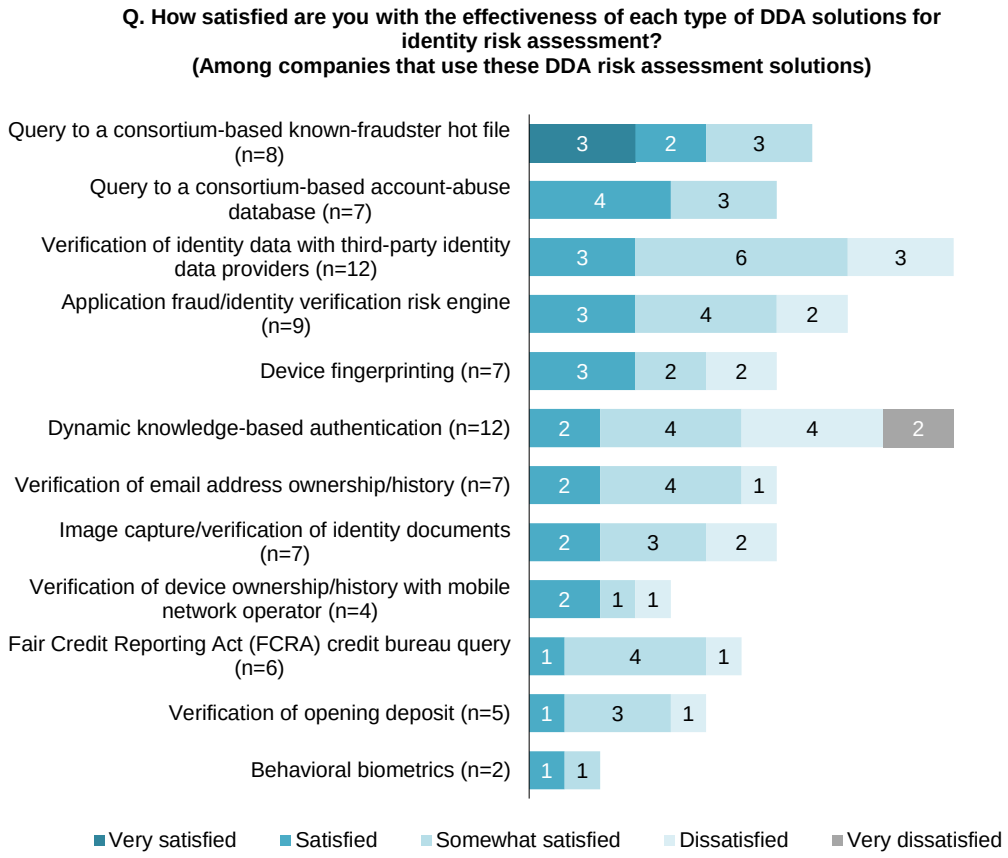
Figure 14: Trend in the Emphasis on Improving Application Fraud Controls



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

When asked about their satisfaction with IDV controls for DDA, fraud executives were bullish on consortium-based known-fraudster "hot files," with three out of eight reports of very satisfied, two reports of satisfied, three reports of somewhat satisfied, and no reports of dissatisfied. They were also bullish on consortium-based account-abuse databases, with four reports of satisfied, three reports of somewhat satisfied, and no reports of dissatisfied. Fraud executives report the highest level of dissatisfaction with knowledge-based authentication controls, with four reports of dissatisfied and two reports of very dissatisfied (Figure 15). They were also the most frequently cited in interviews as being the controls most likely to be replaced.

Figure 15: Satisfaction Levels With Solutions Used for DDA Application Risk Assessment



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

One fraud executive voiced 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. Solution providers such as Early Warning Services that are able to look at both positive and negative account activity across the entirety of the industry were cited by many fraud executives as among those that play an important role in stemming the capacity of money mules, synthetic identities, and first-party fraudsters to spread from one FI to the next.

Regarding other areas in which fraud executives believe there is room for improvement, evidence suggests that the means of tracking, recording, and articulating the performance of their application fraud control frameworks is among them. A segment of the survey that was designed to collect information for this research was engineered to seek out specific performance indicators that are often used to assess an FI's application fraud control framework along the lines of how well it detects and prevents fraudulent activity, and also how well it performs in terms of impacting funding rates, account quality as measured by profitability and measurements of throughput, and accuracy specific to various points in the application fraud control funnel across channels. Unfortunately, most of the 18 FIs that responded to the survey were unable to provide consistent information on these metrics.

Of the few that do track these metrics for both DDA and credit card, one of the fraud executives summarizes what he explained as a "significant effort" to establish a consistent metrics program as a "game changer" in securing partnerships with the owners of DDA and credit card profit-and-loss cost centers. He explained that had the firm not involved stakeholders, including DDA and credit card product owners, in the proofs of concept that it used to experiment with IDV solution providers, then it never would have been able to secure the support necessary to secure funding for its investments. Specifically, he says that articulating the value of accurately measuring—through A/B testing—material swings in funding rates, abandonment rates, and account profitability is key to winning over confederates in securing funding for the firm's investment priorities. If boosting revenue-generating performance indicators is not sufficient, then consider the potential benefits of reducing reputational, operational, and compliance risks, which many fraud executives cite as contributing factors to prioritizing investments in application fraud controls.

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 EARLY WARNING

Early Warning Services, LLC is a fintech company owned by seven of the country's largest banks. For almost three decades, our identity, risk management, and payment solutions have been empowering financial institutions to make confident decisions, enable payments, and mitigate fraud. Today, Early Warning is best known as the owner and operator of the Zelle Network®, a financial services network focused on transforming payment experiences. The combination of Early Warning's risk and payment solutions enables the financial services industry to move money fast, safe, and easy, so people can live their best financial lives.

OPEN MORE ACCOUNTS WITH CONFIDENCE

Early Warning provides solutions to help financial institutions better detect identity fraud and determine the likelihood of first-party fraud or account mismanagement—all in real time. It does the following:

- Provides breadth and depth of deposit data, enabling an holistic view of a consumer's banking behavior
- Leverages real-time, predictive analytics that enable better-informed decisions
- Determines the likelihood that a customer is who they say they are by leveraging Early Warning's industry-leading bank data
- Predicts the likelihood that a customer will default due to first-party fraud in the first nine months of account opening
- Predicts the likelihood that a customer will default due to account mismanagement in the first nine months of account opening
- Matches/verifies applicant Social Security Number (SSN), name and date of birth with the ultimate source of truth—the Social Security Administration
- Adds more customers into the mainstream financial system while managing risk tolerance to potentially increase revenue
- Enhances financial institutions' customer identification program (CIP) and KYC initiatives
- Ensures faster decisions and reduced friction, which translates to a better customer experience

To learn more about Early Warning, visit www.earlywarning.com or contact an Early Warning account manager.