Aite PARTNER. ADVISOR. CATALYST.

Application Fraud: Fighting an Uphill Battle

DECEMBER 2018

Shirley Inscoe

NuData Security mastercard

This report is provided compliments of NuData Security, a Mastercard company.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

IMPACT POINTS

- Application fraud continues to be a major challenge for financial institutions (FIs), along with other identity-related crimes, particularly in digital channels. This Impact Report delves into how FIs are combating this issue today and how that will evolve. Fraud executives at 30 FIs participated in this research via an online survey, and telephone conversations with fraud executives supplemented the survey findings.
- By 2020, it is projected that U.S. FI spending to combat demand deposit account (DDA) application fraud losses will reach US$599 million; spending by FIs to combat credit card application fraud will reach US$781 million.
- Three-quarters of FIs surveyed indicate that one of their top three pain points leading to application fraud is first-party fraud, followed by 56% indicating data breaches and 52% indicating social engineering in contact centers as top three pain points.
- The most common methods used to combat application fraud for DDAs are verifying identity data with third-party databases and checking consortium-based databases for account abuse and for known fraudsters.
- The most common methods of combating application fraud for credit cards are queries to a credit bureau and verifying identity data with third-party databases.
- On the DDA side, a third of FIs (33%) plan to add additional vendors, compared to only 9% that planned to do so in 2015. Fifteen percent of FIs plan to replace one or more current vendors with a new vendor, similar to the 18% that planned to do so in 2015.
- On the credit card side, over half of respondents are planning some changes in the vendor solutions they use in the next one to two years. Forty-seven percent plan to add additional vendors, and 11% plan to replace one or more current vendors with a new vendor.
- Eighty-eight percent of FIs state that improving the customer onboarding experience is very important as they make technology investments. Two categories—cross-channel fraud detection and compliance concerns—tie, with 64% stating that these are very important factors driving technology investments.
- Ninety percent of FIs indicate plans to implement mobile identity document capture and verification solutions within the next two years.

INTRODUCTION

Application fraud continues to be a significant problem for FIs across the U.S. As identity crimes continue to grow, it is increasingly difficult for FIs to determine who they are dealing with in all delivery channels. The prevalence of fake IDs makes proving an individual's identity difficult even in a physical branch; knowing for certain who the applicant is on the other side of a laptop, tablet, telephone, or mobile device is extremely difficult. As a result, these identity crimes are influencing a number of strategies and resulting in FIs planning to make new technology investments to meet both compliance (Know Your Customer) and fraud challenges.

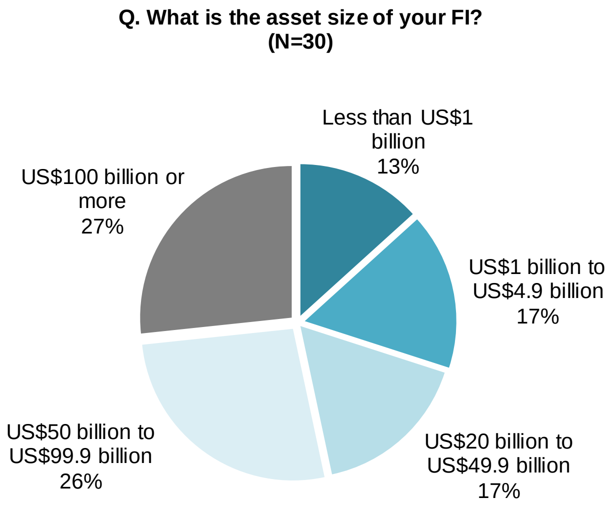
Since identity crimes are so easy to commit in the current environment, fraudsters will increasingly apply for accounts fraudulently (and take over accounts to commit fraud as well). Until safeguards are put in place to stop them, it is just like taking candy from a baby.

METHODOLOGY

Aite Group conducted research using an online survey from March 2018 to June 2018 to better understand application fraud for both DDAs and credit cards. Executives from 30 U.S. FIs completed the online survey; continuing conversations with FI executives supplemented the data gathered via the survey. Asset sizes of the participating FIs range from under US$1 billion to over US$100 billion. Almost half of the FIs had under US$50 billion in assets, while roughly one-quarter of participants had between US$50 billion and US$99.9 billion, and the final quarter had US$100 billion or more (Figure 1). This Impact Report represents a refresh of research previously conducted in late 2015 and a report published in March 2016.[1] 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.

Figure 1: Asset Size of FI Respondents



Source: Aite Group's survey of 30 FIs, March to June 2018

THE MARKET

Application fraud has been a significant challenge for the past few years in the U.S. market. Aite Group research from 2017 revealed that application fraud was second only to account takeover fraud as the biggest challenge for FIs.[2] Many FI executives attribute part of the rise of application fraud to the rollout of EMV—US$4 billion in displaced fraud losses from counterfeit magnetic stripe cards had to be replaced, and application fraud was identified by fraudsters as one method to accomplish that.

Data breaches continue to give fraudsters access to personal information about millions of consumers that fraudsters can readily use to impersonate others. Since 2013, over 13 billion data records have been lost or stolen.[3] Unfortunately, with all the breached data, third-party databases that have been used for decades to verify a consumer's identity are not as effective as they used to be. Phishing attacks continue to plague consumers, and malware use has moved into the mobile channel as well as online. All of these tools are used by fraudsters to make identity crimes easy to commit and hard to detect.

Identity theft is one form of application fraud, but cases of manipulated identities and the use of synthetic or manufactured identities are growing as well.[4] Having no real victim can make it more difficult to determine that the applicant doesn't actually exist in the real world (Table A).

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 continuing 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

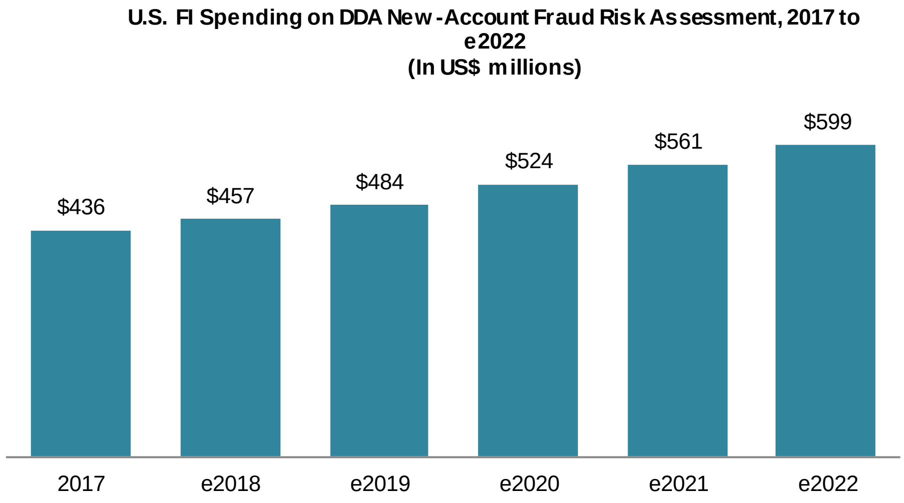
[2] See Aite Group's report *Machine Learning: Fraud Is Now a Competitive Issue*, October 2017.

[3] "Data Breach Statistics," Breach Level Index, accessed November 2, 2018, https://breachlevelindex.com/.

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

Since the application fraud threat will continue to be a major challenge for many FIs to address, losses will continue to be significant. Spending to combat application fraud related to DDAs is projected to increase to US$599 million by 2022 (Figure 2).

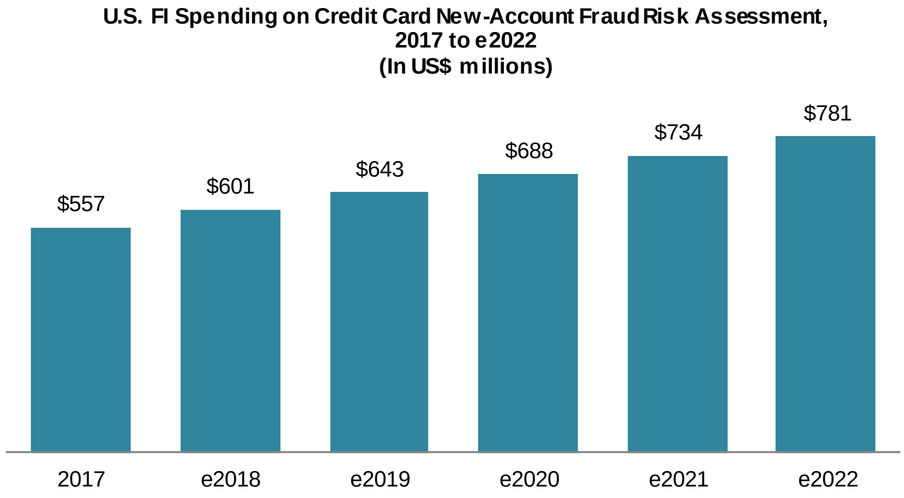
Figure 2: U.S. FIs' Spend on DDA Application Fraud Solutions



Source: Aite Group

Credit card application fraud will result in even higher fraud losses; by 2022, spending to curtail these fraud losses is projected to increase to US$781 million (Figure 3).

Figure 3: U.S. FIs' Spend on Credit Card Application Fraud Solutions



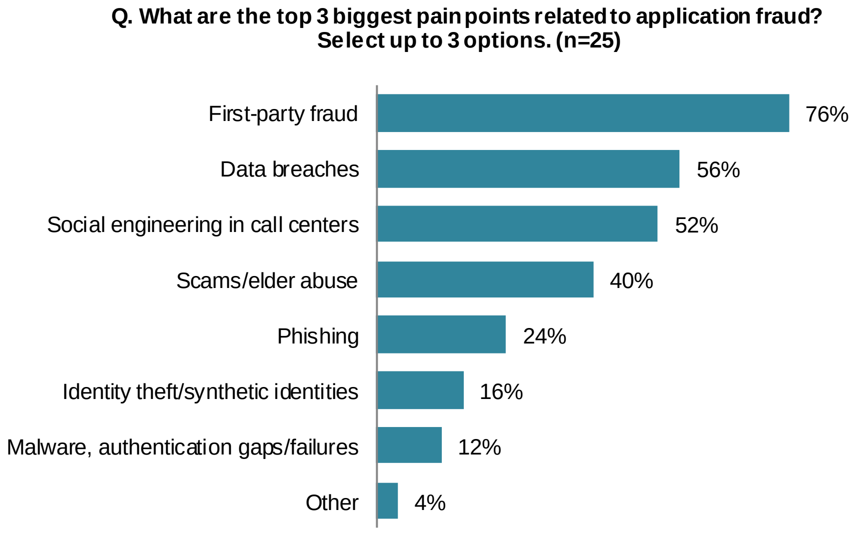
Source: Aite Group

APPLICATION FRAUD'S FI IMPACT

Application fraud is an issue for both DDAs and credit cards; however, they are examined separately in this report since they have a number of differences as well as similarities.

FI executives identify several pain points that lead to successful application fraud. By far the biggest pain point is first-party fraud, which was chosen by 76% of executives as one of their top three challenges. Data breaches are the second-biggest problem FIs face; much of the data breached can be used by fraudsters to impersonate real consumers or to extract data points to create a synthetic identity. Third highest among pain points is the social engineering that occurs in contact centers where fraudsters are able to successfully impersonate existing customers or open new accounts, committing application fraud. Scams and elder abuse come in as the fourth biggest challenge, followed by phishing attacks (Figure 4).

Figure 4: Biggest Pain Points Leading to Application Fraud



Source: Aite Group's survey of 30 FIs, March to June 2018

First-party fraud (i.e., fraud committed by the person who owns the account) is extremely difficult to thwart, particularly if it is the first time the person has committed fraud. Organized fraud rings often recruit and incentivize people to perform certain tasks; in the case of application fraud, they may convince people to allow their personal information to be used to open new accounts or apply for a card. Various groups of people are approached by fraudsters—groups such as those who are young and naive, elderly people who may be easily misled, or people who have been in the country for a specific period of time and are leaving shortly are targeted.

Data breaches have occurred so frequently that people aren't as concerned as they used to be; that is unfortunate, because continuing data breaches refresh the data fraudsters gather about us all, and they are able to use this data to commit their crimes. Unfortunately, there seems to be no end in sight for these breaches, and many experts feel that a dedicated hacker will eventually gain access to any system.

Social engineering in contact centers is a form of attack against an FI. These tactics are used by fraudsters to call in repetitively until they are able to convince an agent that they are the real customer. In the case of application fraud, their job may be easier because they just need to convince the agent that they match the identity they are providing to apply for an account or card. This may be an identity they have created, or they can use data from data breaches, social media, and other sources to represent someone else. In one example, a fraudster called in to an FI's contact centers and opened over 50 DDAs using various identities.

Scams often go hand-in-hand with elder abuse, but people of any age can fall for a scam. Elders are particularly vulnerable because they may be lonely, may be isolated, and may not have anyone who can advise them against falling for the scam in question. Elder abuse is prolific and is expected to grow as the population ages.

Phishing attacks continue to flourish; according to the Anti-Phishing Working Group, in Q2 2018, 36% of phishing targeted payments, and an additional 16% targeted financial institutions.[5] Phishing attacks have grown far more sophisticated, both in their wording and in the methods used to conduct the attacks. In Q2 2018, about 35% of phishing attacks were hosted on websites that had HTTPS and SSL certificates (leading many to think the websites were secure and could be trusted). Most phishing attacks are sent to thousands of people, making even a low percentage of responses highly profitable.

Identity theft and the use of manipulated or synthetic identities are challenges FIs must contend with. Identity theft occurs when someone uses the identity of a consumer without their consent; the true owner of the identity is the victim. When fraudsters use synthetic identities, there is no victim of the crime because the identity does not exist in the real world. Fraudsters are nurturing synthetic or manufactured identities for many months or years, establishing credit bureau reports, obtaining mobile phones, and taking other steps to make such identities extremely difficult to detect.

Malware has been a threat for almost as long as the internet has existed and has spread to mobile devices as well. Many devices have malware, and while not all of it is malicious, FIs have to guard against activity from infected machines.

Authentication failures occur when a method used to authenticate consumers is defeated by fraudsters; as one example, knowledge-based authentication (KBA) questions may be successfully answered by fraudsters based on data from data breaches, information posted on social media, or phishing attacks. Authentication gaps occur when fraudsters figure out a way around a fraud prevention or authentication process (e.g., a fraudster who doesn't want his voice analyzed by contact center technology calls a branch and is transferred directly to an agent, avoiding the voice analysis performed on all incoming contact center calls).

[5] "Phishing Activity Trends Report: Second Quarter 2018," Anti-Phishing Working Group, October 18, 2018, accessed November 22, 2018, http://docs.apwg.org/reports/apwg_trends_report_q2_2018.pdf.

Respondents who chose the “other” category state that business email compromise is one of their top three fraud pain points leading to application fraud.

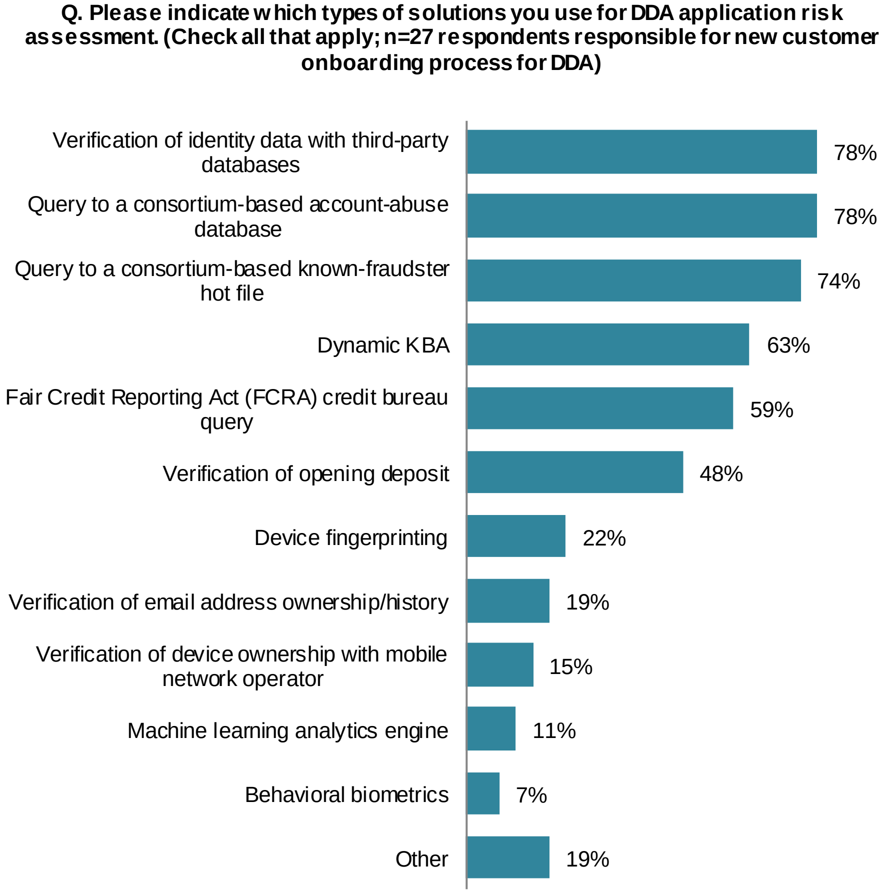
APPLICATION FRAUD: DDA

DDAs are opened by fraudsters for a variety of reasons. Fraudsters may open the accounts planning to commit check fraud, deposit fraud, or kiting; they may use the account as a repository for funds stolen from other FIs; or the DDA may just be an entry point to later apply for credit cards or other loans. Regardless of the reason for the account opening, application fraud is a major problem in new account opening.

FIs use many different types of solutions to understand who is opening new accounts and to prevent application fraud. About three-quarters of FIs use solutions that verify the identity with third-party databases and check with a consortium of databases to detect prior account abuse or fraudulent behavior. Roughly 60% of FIs surveyed also use KBA to determine that the person is who they claim to be and to do a credit bureau query. Unfortunately, while some of these practices are widespread in the industry, the value from a third-party database or credit bureau query has been degraded due to all the data breaches and fraudsters’ practices of nurturing synthetic identities until they are well-represented in both types of databases. Similarly, KBA questions can sometimes be more readily answered by fraudsters than the true individual, thanks to data breaches and information consumers post on social media websites. Many FIs have turned to additional measures to try to defeat fraudsters from opening new DDAs. Almost half (48%) do a verification on the opening deposit made to the DDA. While only 11% indicate they are using a machine learning engine,[6] the use of this technology is expected to grow rapidly. Behavioral biometrics, used by 7% of FIs, is another relatively new technology that can help in identifying human versus nonhuman or bot behavior, as well as normal applicant behavior versus fraudster behavior during the application process. The “other” category includes additional tools, such as IP geolocation comparisons, phone number verifications, one-time passwords, and fraud anomaly detection. The five least used of the tools listed are all completely transparent to the customer and can be used to improve the customer experience while still adding an extra layer of security (Figure 5).

[6] See Aite Group’s report *Machine Learning for Fraud Mitigation: The Substance Behind the Buzz*, April 2017.

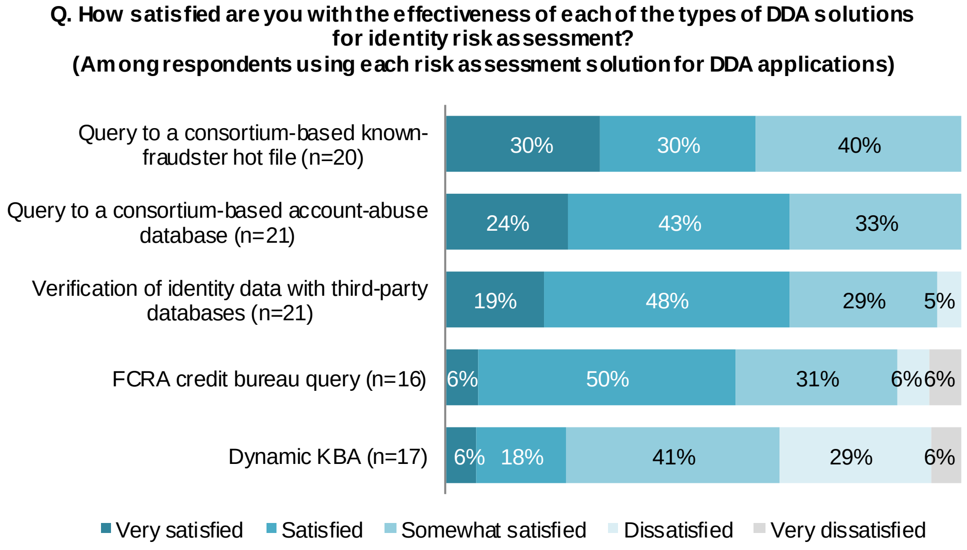
Figure 5: Types of Solutions Used for DDA Application Risk Assessment



Source: Aite Group's survey of 30 FIs, March to June 2018

FIs' satisfaction levels with the most commonly used fraud prevention solutions vary. Queries to consortium databases result in at least "somewhat satisfied" executives across the board. For all other categories, there is some level of dissatisfaction. Some of this dissatisfaction is stemming from the lower reliability of the data than was possible in the past. This is not the fault of solution providers, but is instead due to data breaches, phishing attacks, and other methods fraudsters use to defeat these tools. Interestingly, both credit bureau queries and KBA questions have the same percentage of executives who are very satisfied and very dissatisfied, at 6% each (Figure 6).

Figure 6: Satisfaction Levels With Solutions Used for DDA Application Risk Assessment

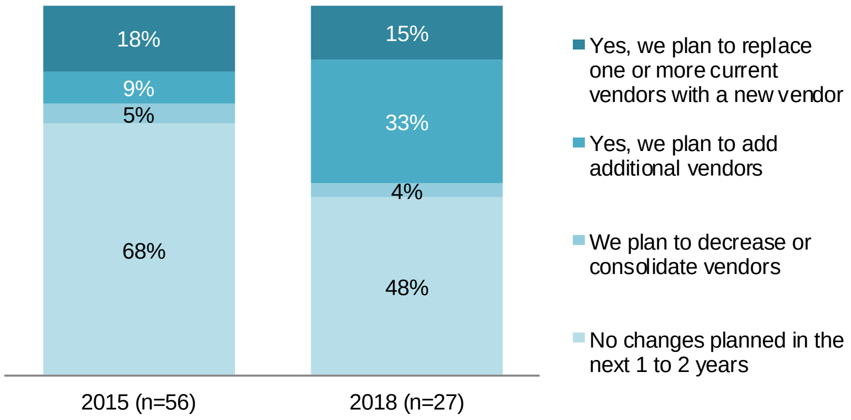


Source: Aite Group's survey of 30 FIs, March to June 2018

FIs don't tend to make rapid changes in vendors they use, because it is often costly to tear out old solutions and implement new ones. Often, these efforts require a major IT project, and those resource allocations can be difficult to obtain. In 2015, 68% of FIs surveyed did not plan any changes in vendors used during the following one to two years. That has changed in the current environment, with slightly over half of FIs surveyed (52%) planning some type of change. A third of FIs plan to add additional vendors, a significant change compared to only 9% that planned to do so in 2015. Current rates of application fraud are likely spurring these technology investments. Only 15% of FIs plan to replace one or more vendors with a new vendor, a slight decrease from 18% in 2015 (Figure 7).

Figure 7: Planned Changes in DDA Application Risk Assessment Vendors

Q. Do you plan to add or change DDA application risk assessment vendors in the next 1 to 2 years?
(Among respondents responsible for new customer onboarding process for DDA)



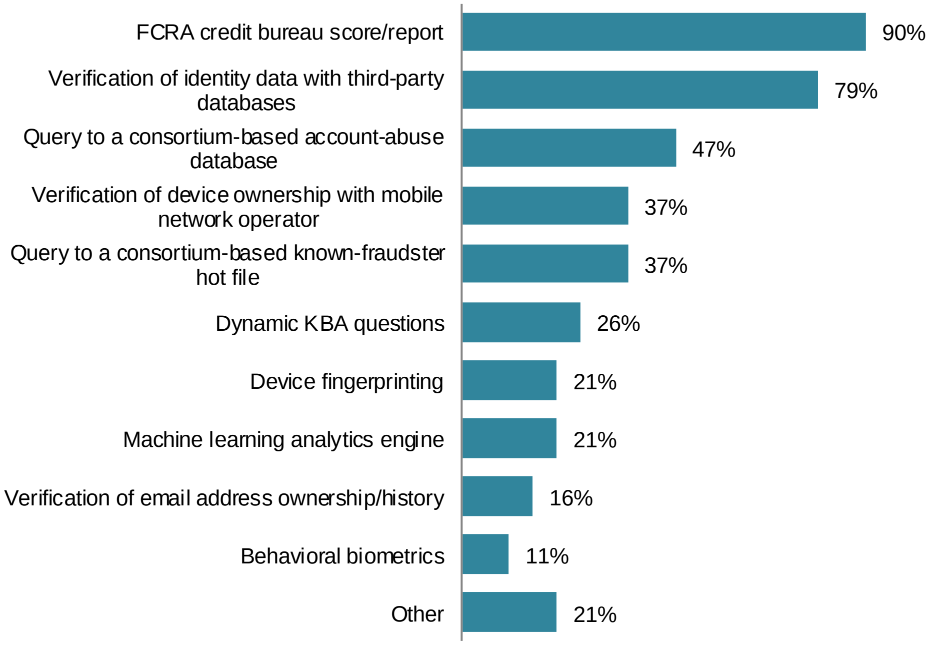
Source: Aite Group's survey of 30 FIs, March to June 2018, and Aite Group's survey of 83 U.S. FIs, November to December 2015

APPLICATION FRAUD: CREDIT CARD

Similar to the DDA opening process, FIs use many different kinds of solutions to prevent and detect fraud in their credit card application process. Ninety percent of the FIs are using credit bureau queries, and 79% are checking third-party databases to try to learn more about applicants. Slightly less than half of issuers (47%) are checking applicant data against a consortium-based database for account abuse. Two solution types are used by 37% of issuers—verification of device ownership with mobile network operators and queries to a consortium-based known-fraudster hot file. A quarter of issuers are using KBA questions to try to determine that the applicant is who he or she claims to be, and 21% or less are using additional tools. Similar to the DDA environment, behavioral biometrics can be used to try to distinguish between human and bot behavior as well as between normal applicant behavior and fraudster behavior (Figure 8).

Figure 8: Types of Solutions Used for Credit Card Application Risk Assessment

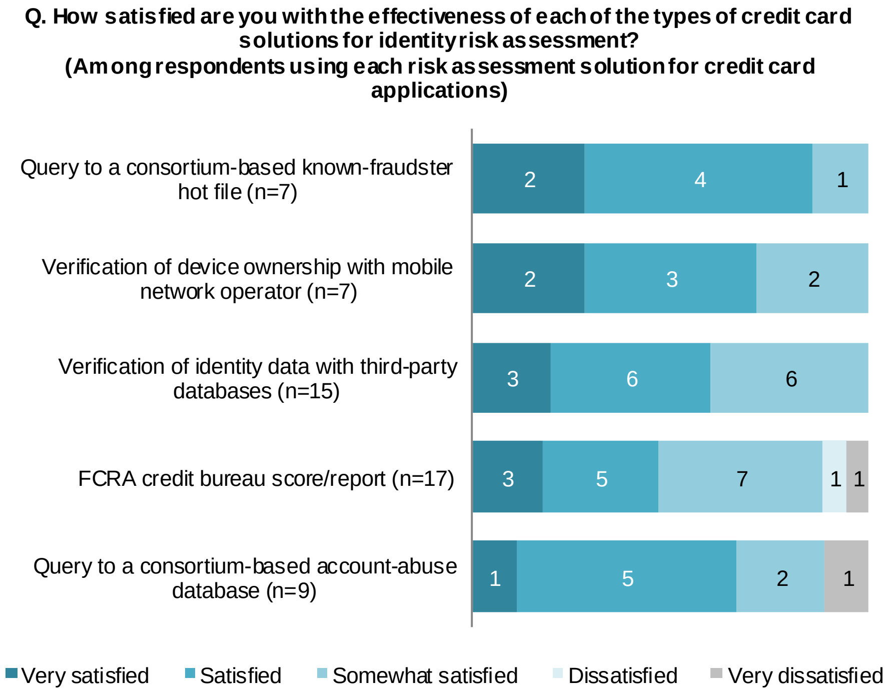
Q. Please indicate which types of solutions you use for credit card application risk assessment. (Check all that apply; n=19 respondents responsible for new customer onboarding process for credit card)



Source: Aite Group's survey of 30 FIs, March to June 2018

While some solutions work well, not all do. Overall, the majority of respondents are at least somewhat satisfied with the tools they rated. Minimally, one issuer was dissatisfied and one was very dissatisfied with the credit bureau query under FCRA; this may be due to the fact that fraudsters have nurtured synthetic identities to the point that they are indistinguishable from real identities in credit bureau queries. Additionally, one issuer was very dissatisfied with the results of queries to a consortium-based account abuse database (Figure 9).

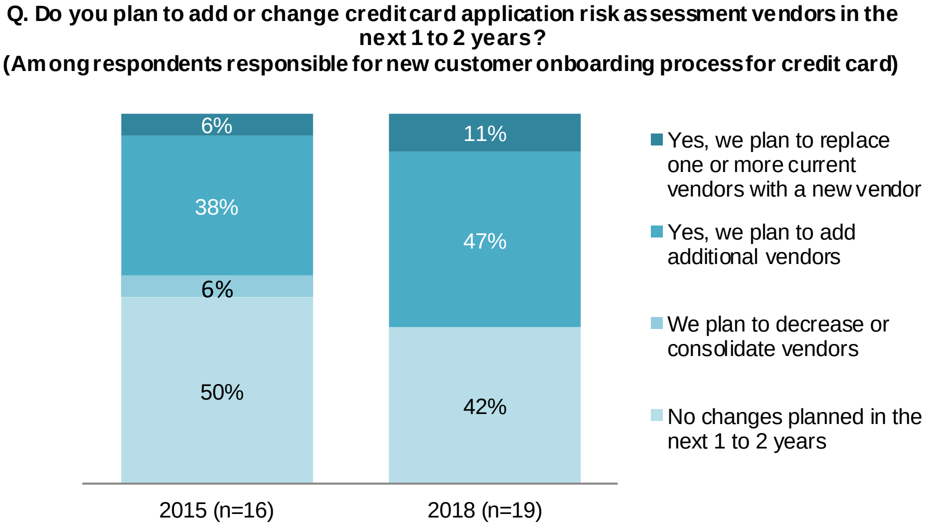
Figure 9: Satisfaction Levels With Solutions Used for Credit Card Application Risk Assessment



Source: Aite Group's survey of 30 FIs, March to June 2018

Over half of respondents plan to make some changes to the vendor solutions they use in the next one to two years. Forty-seven percent plan to add additional vendors, and 11% plan to replace one or more vendors with a new vendor. These percentages are higher than those seen in 2015, when half of issuers planned no changes; this is also indicative of the market environment in which identity crimes continue to represent a major challenge (Figure 10).

Figure 10: Planned Changes in Credit Card Application Risk Assessment Vendors



Source: Aite Group's survey of 30 FIs, March to June 2018, and Aite Group's survey of 83 U.S. FIs, November to December 2015

SOLUTION PROVIDERS

As FIs consider new tools to use to supplement their efforts or consider changing vendors to upgrade current solutions, there are many in the market to choose from. This section will identify some of the vendors that offer solutions in a variety of categories.

In general, behavioral biometrics solutions analyze data points related to how applicants interact with their device, be it a laptop, tablet, or mobile phone. This can include factors such as how data is entered, how applicants move around a form, the angle at which they hold a device, whether they are left- or right-handed, etc. Some of these solutions can differentiate between bot and human behavior; some can differentiate between normal applicant behavior and fraudster behavior. Some vendors who offer behavioral biometrics are listed in Table B.

Table B: Behavioral Biometrics Vendors

Vendors				
ACI Worldwide*	AimBrain	BehavioSec	BioCatch	Kofax
Neuro-ID	NuData Security	OneSpan	SecuredTouch	ThreatMetrix**

Source: Aite Group
**Indicates that the solution is white-labeled and is provided by another vendor*
*** A LexisNexis Risk Solutions Company*

Device identity vendors uniquely identify a specific device used by a consumer; in some cases, the device identity can be associated with the individual. Some vendors do more in-depth device identification than others; Table C lists vendors that offer such solutions.

Table C: Device Identity Vendors

Vendors				
41st Parameter*	BioCatch	Entrust Datacard	InAuth	IdentityMind
iovation	Kount	Neustar	NuData Security	OneSpan
Pindrop Security	RSA Security	ThreatMetrix**		

Source: Aite Group
**An Experian Company*
***A LexisNexis Risk Solutions Company*

One factor that some FIs use to confirm identity is to confirm the ownership of the mobile device used to apply for a new account. Device ownership that matches the information supplied by an applicant is one layer of security to confirm that the person is who he or she claims to be. Vendors that offer these solutions are listed in Table D.

Table D: U.S. Mobile Device Ownership Verification Vendors

Vendors				
Danal	Early Warning Services*	Emailage*	Equifax	Experian
IDology*	LexisNexis Risk Solutions	Neustar	Payfone	Socure
ThreatMetrix* **	TransUnion	TrustID	Zumigo	

Source: Aite Group
**Indicates that the solution is white-labeled and is provided by another vendor*
***A LexisNexis Risk Solutions Company*

"Hot files," or lists of suspicious identities, are tools often used to detect account abuse or fraudster behavior that is likely to occur if a new account is opened for someone appearing in such a database. There is a lot of power in collaborating and sharing such information; by sharing, an FI can avoid losing money to someone who has previously caused a loss at another FI. With many fraud rings being highly organized, an FI has difficulty withstanding attacks alone. Shared data can add tremendous value to fraud prevention efforts. Table E shows vendors that support such collaboration in the industry.

Table E: Consortia-Based Suspicious Identity, Account Abuse, or Known Fraudster Data

Vendors				
Deluxe*	Early Warning Services	Ethoca	Equifax	Experian
FIS	ID Analytics	LexisNexis Risk Solutions	PhishLabs	RSA Security
ThreatMetrix**	Verifi	Visa Issuers' Clearinghouse Service		

Source: Aite Group
**Indicates that the solution is white-labeled and is provided by another vendor*
***A LexisNexis Risk Solutions Company*

Many vendors offer identity verification products; typically, these products validate various data provided by an applicant against third-party databases, and may also incorporate other tests to determine that the person is who he or she claims to be. Many of these solutions are somewhat unique, and some FIs use multiple vendors for identity verification (Table F).

Table F: Identity Verification Vendors

Vendors				
Acxiom	Deluxe	Dragnet Solutions	Early Warning Services	Emailage
Equifax	Experian	FIS	Fiserv	Giact
ID Analytics	IdentityMind	IDology	LexisNexis Risk Solutions	Melissa Data
MicroBilt	Socure	Trulioo	TransUnion	Whitepages Pro

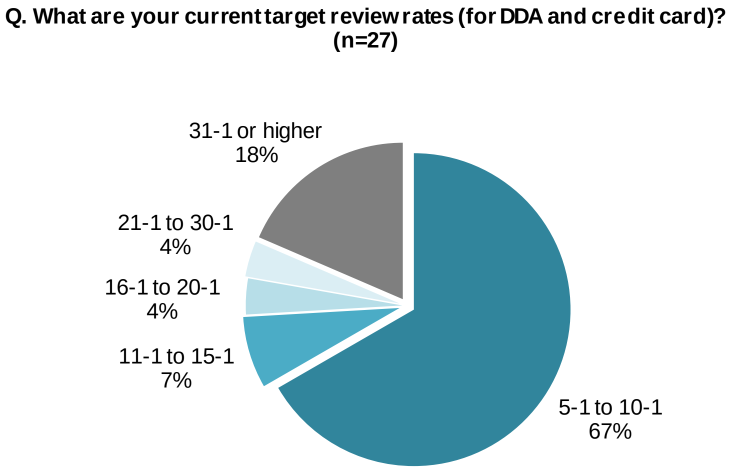
Source: Aite Group

MANUAL REVIEW RATES

One of the biggest challenges in using fraud detection solutions effectively is managing false positive rates. Adjustments to the system must be made to keep the number of alerts generated to a manageable level that can be worked with existing staff while not excluding alerts that indicate fraud. This balance is always the goal, but the correct balance is easier to achieve with some solutions than others.

The majority of FIs (67%) have a target review rate of between the 5-1 and 10-1 range. This means that they will work between five and 10 alerts that are false positives for every alert that actually represents fraud. Amazingly, 18%, or almost one in five, FIs state that their target manual review rate is 31-1 or higher (Figure 11). Some systems produce high false positives, so perhaps these FIs have just resigned themselves to looking for the needles in the haystack. The primary danger of such high false positives becoming a way of life is that analysts may miss the fraudulent items because they find so few of them daily.

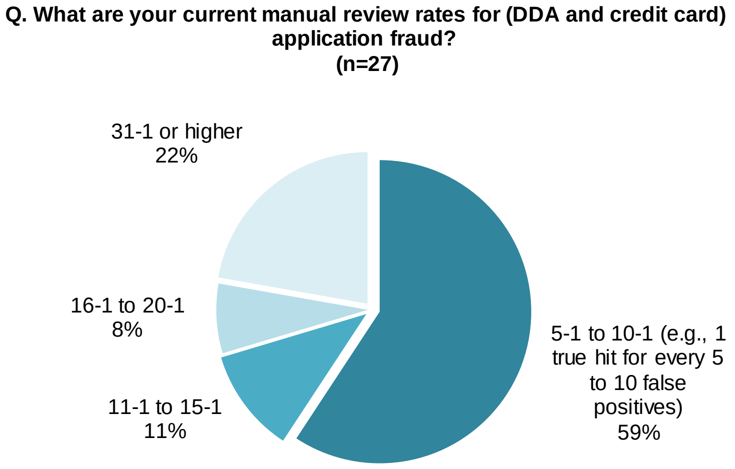
Figure 11: Target Manual Review Rates



Source: Aite Group's survey of 30 FIs, March to June 2018

The bulk of FIs are achieving their targeted review rates. Eight percent of FIs would like to achieve review rates of 10-1 or lower, but are currently realizing higher rates. The bulk of FIs are spot on their targets. Similarly, in the highest range, 4% of FIs are targeting lower ranges than they are achieving (Figure 12). Some FIs are implementing new solutions primarily for the purpose of reducing the output of existing systems and winnowing out the highest risk items. Machine learning models are very helpful in successfully reducing false positives while still detecting fraud successfully.

Figure 12: Manual Review Rates

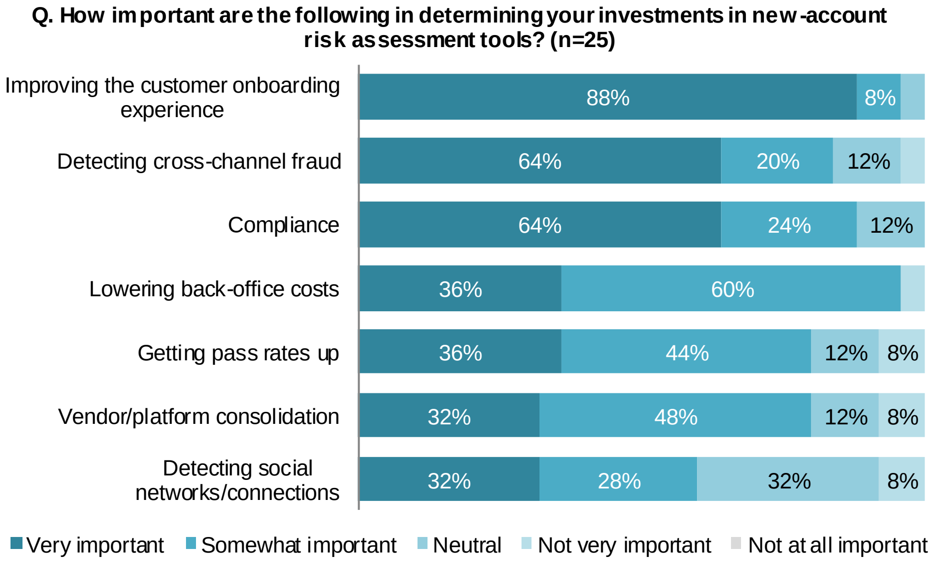


Source: Aite Group's survey of 30 FIs, March to June 2018

INVESTMENT DRIVERS

As FIs continue to focus on moving more activity to digital channels, it is not surprising to see that the most important category driving investments is improving the customer onboarding experience. Consumers are demanding simpler and faster methods to accomplish whatever they want to do online and on mobile devices. Eighty-eight percent of FIs state that improving the customer onboarding experience is very important as they make technology investments. Two categories—cross-channel fraud detection and compliance concerns—tie, with 64% stating these are very important factors driving technology investments. At least a third of FIs also view lowering back-office costs, increasing pass rates, consolidating the vendor platform, and detecting social networks as very important (Figure 13).

Figure 13: Factors Driving Investments

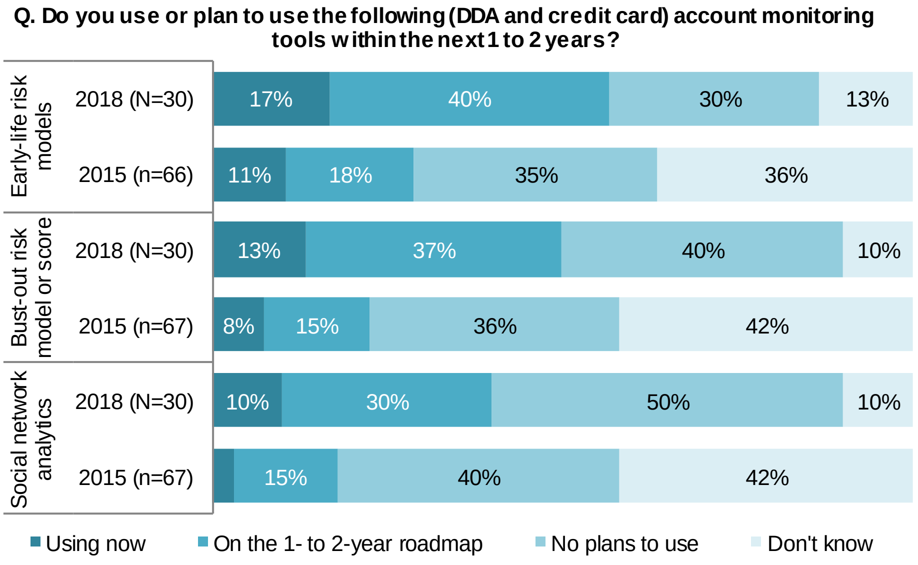


Source: Aite Group's survey of 30 FIs, March to June 2018

USE OF NEW MODELS AND SOLUTIONS

FIs use of a number of predictive models to enable them to best manage their product portfolios. FIs have increased the use of all three models summarized in Figure 14 since 2015, and many more FIs are planning to implement these models in the next one to two years. For example, early risk models are being used by 17% of FIs (up from 11% in 2015), but an additional 40% plan to implement these models in the next one to two years. If those plans come to fruition, over half of U.S. FIs will be using early risk models by the end of 2020. Similarly, if plans to implement bust-out risk models come to fruition, half of FIs will be using them before 2021, and 40% will be using social network analysis models (Figure 14).

Figure 14: Plans to Use Account Monitoring Tools

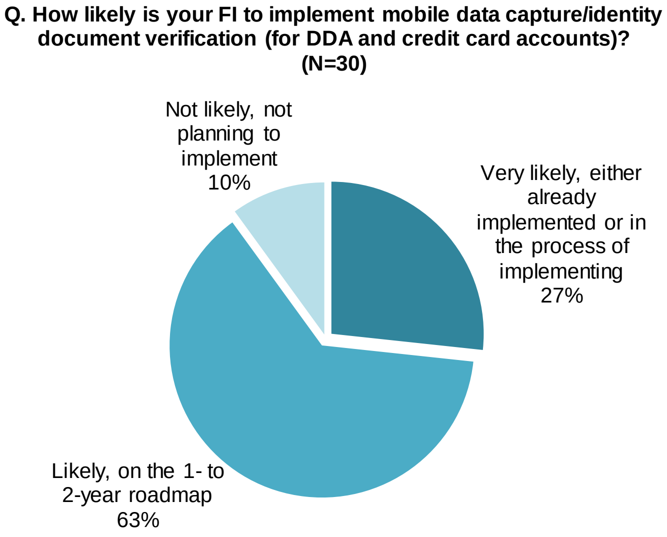


Source: Aite Group's survey of 30 FIs, March to June 2018, and Aite Group's survey of 83 U.S. FIs, November to December 2015

Automated identity document capture and verification is a solution that is relatively new in the market and is gaining traction in many economic sectors. Use of the product is relatively new; it is in use by governmental agencies, telecommunications companies, car rental companies, and many others. In faceless delivery channels, such as online, mobile, and contact centers, using identity document capture and verification can enable a company to ensure that the identity document is legitimate and has not been tampered with, and comparing a selfie to the picture on the document can ensure that the owner of the document is on the other side of the device.[7] This technology replaces methods of referring to printed books to compare the features on a driver's license or passport, and technology can often detect changes that the human eye can miss. Figure 15 shows that 27% of FIs have implemented or are implementing this technology, while an additional 63% of FIs are likely to implement and have the solution on their one- to two-year roadmap. Overall, 90% of FIs indicate plans to implement within the next two years.

[7] See Aite Group's report *AIM Evaluation: Identity Document Capture and Verification*, October 2018.

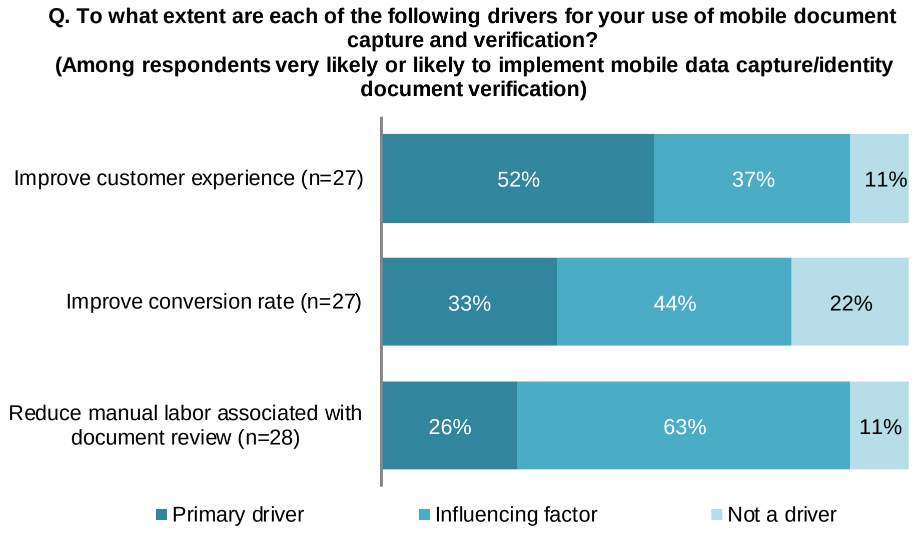
Figure 15: Likelihood of Implementing Identity Document Capture and Verification



Source: Aite Group's survey of 30 FIs, March to June 2018

Although identity document capture and verification solutions are ideal for ensuring you know who is on the other side of a device, tablet, or computer, FIs are choosing to implement them for other reasons. Capturing the data from an identity document enables an FI to use that data to prefill another document, such as a credit card or DDA application. This is much more customer-friendly than having to type all this data via a small mobile keyboard, and it also eliminates many keying errors that normally lead to additional back-office work, thus improving operational efficiency. This back-office process often entails contacting the customer and requiring the customer to mail in copies of documents or bring them into a branch, adding friction to the customer experience. Know Your Customer requirements can be met through this process as well, improving compliance. In over half of FIs, improving the customer experience is the primary driver for implementing identity document verification; 33% of FIs are implementing the solution in order to increase the conversion rate for new accounts in digital channels, and 26% are doing so to reduce the manual labor associated with the document review processes, thus improving operational efficiency (Figure 16).

Figure 16: Drivers for Implementing Identity Document Capture and Verification



Source: Aite Group's survey of 30 FIs, March to June 2018

Many vendors offer identity document capture and verification solutions, which is a relatively new product in the market. Some of the vendors that offer it are highlighted in Table G.

Table G: Identity Document Capture and Verification Vendors

Company	Headquarters	Year founded
Acuant	Los Angeles	1999
Au10tix	Nicosia, Cyprus	2006
AuthenticID	Manchester, New Hampshire	2012
Confirm.io	Boston	2015
Equifax*	Atlanta	1899
Experian*	Dublin	1996
FIS*	Jacksonville, Florida	1968
Fiserv*	Brookfield, Wisconsin	1984
GB Group	Sunbury, United Kingdom	2005
Gemalto	Amsterdam	2006
ID Analytics*	San Diego, California	2002
ID.me	McLean, Virginia	2010
Idemia	Paris	2007
IDology	Atlanta	2003

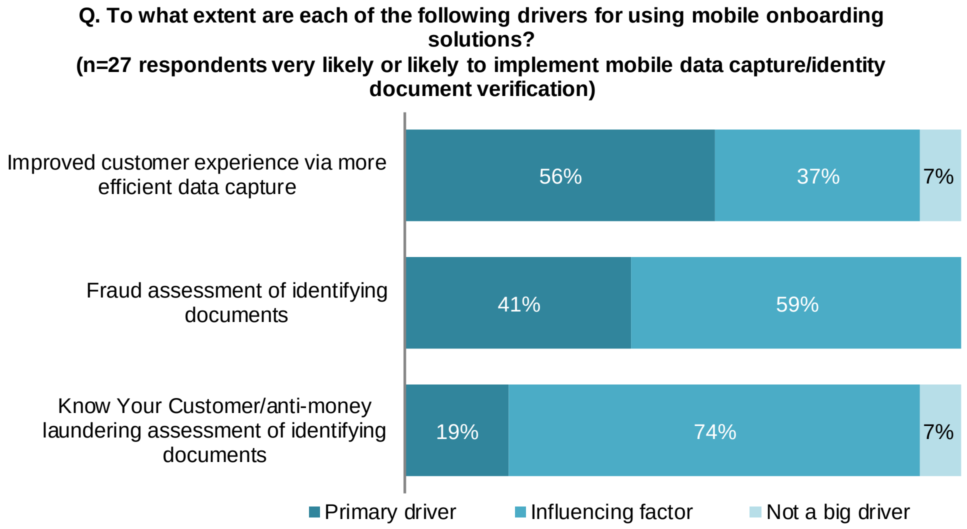
Company	Headquarters	Year founded
Jumio	Palo Alto, California	2010
Kofax	Irvine, California	1985
LexisNexis Risk Solutions*	Alpharetta, Georgia	2000
Lexmark	Lexington, Kentucky	1991
Mitek Systems	San Diego, California	1985
OneSpan*	Chicago	1991
Onfido	London	2012
Paycasso	London	2012
Signicat*	Trondheim, Norway	2007
TransUnion*	Chicago	1968
Trulioo	Vancouver, Canada	2011
Zoot*	Wilmington, Delaware	2009

Source: Aite Group
**Indicates that the solution is white-labeled and is provided by another vendor*

Mobile onboarding solutions also make opening new accounts or applying for cards and other products easier for consumers. Often, they incorporate the identity document capture and verification process mentioned previously and take additional steps, such as capturing digital signatures and using the customer's preferred methods of communication. Mobile onboarding solutions can automate the entire process and integrate with internal bank systems so that all manual processes are eliminated.

The primary reason to implement a mobile onboarding solution is to improve the customer experience via the automated capture of data, followed by the fraud assessment of identifying documents. Achieving compliance with Know Your Customer regulations is a distant third in terms of primary drivers, but its importance is clear, with 74% of FIs stating that it is an influencing factor (Figure 17).

Figure 17: Drivers for Mobile Onboarding Solutions

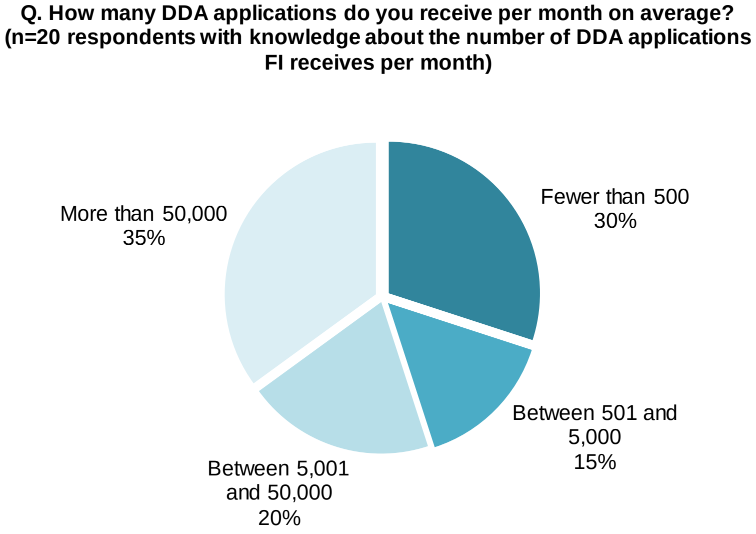


Source: Aite Group's survey of 30 FIs, March to June 2018

APPLICATION VOLUME

Application volume can vary broadly based on the size of an FI, the marketing campaigns it is running, any new account incentives it may offer, etc. The FIs that participated in this research have a broad range of DDA application volumes. Thirty percent receive fewer than 500 applications per month, while 55% receive over 5,000 per month. Clearly, automating the onboarding process saves manual effort in all FIs, but the FIs processing a higher volume can likely better afford automated processing. Thirty-five percent process over 50,000 applications per month (Figure 18).

Figure 18: DDA Application Monthly Volume

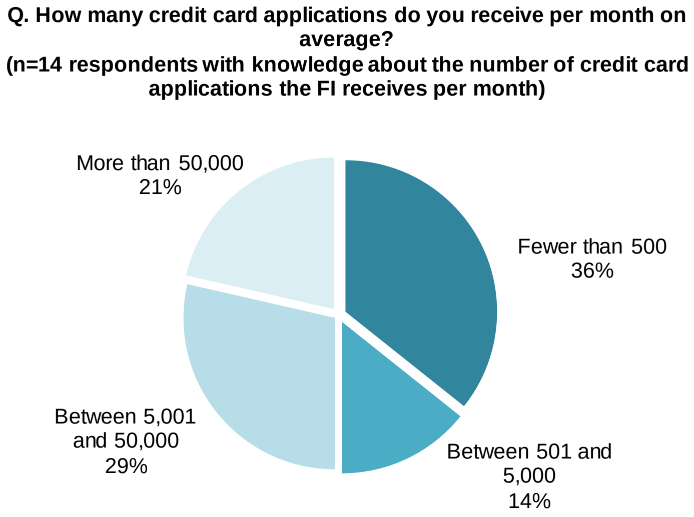


Source: Aite Group's survey of 30 FIs, March to June 2018

Licensed for external distribution by: NuData Security, a Mastercard company.

Fewer FIs responded with credit card application volume in this research, and some small FIs may not issue cards at all. Only three FIs process over 50,000 credit card applications per month, while four process between 5,001 and 50,000. The other seven FIs each process fewer than 5,000 credit card applications per month (Figure 19).

Figure 19: Credit Card Application Monthly Volume



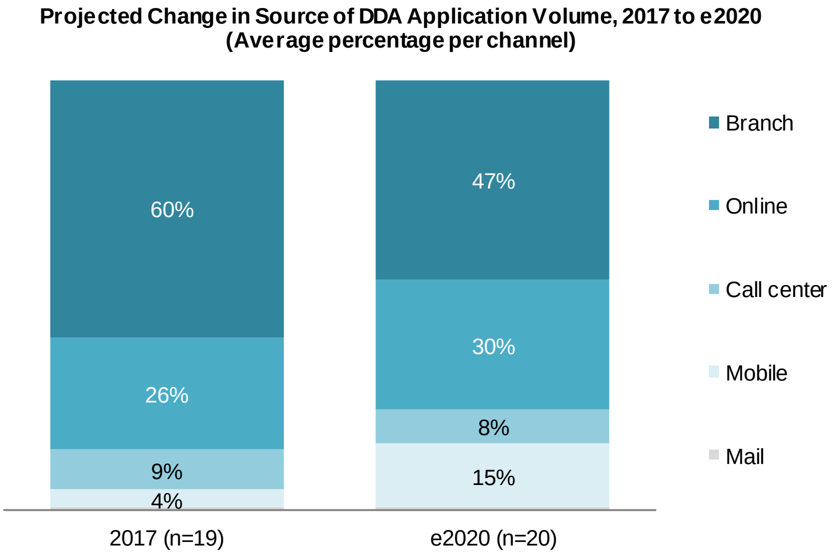
Source: Aite Group's survey of 30 FIs, March to June 2018

ONBOARDING CHANNELS

In the past few decades, FIs have had a strong desire to move application volume online (and later to mobile) due to the lower cost of these delivery channels. Digital channels offer tremendous cost savings, and now that consumers seem to prefer a mobile-first approach to everything, win-wins should easily be achievable.

In 2017, 60% of DDA applications were still submitted in branches, and 26% were submitted via the online channel. Nine percent were submitted via contact centers, and only 4% were submitted via mobile. By 2020, FI executives project that less than half (47%) of DDA applications will be submitted in branches, and submissions through online and mobile channels will grow to 45%, with contact center volume changing only slightly (Figure 20).

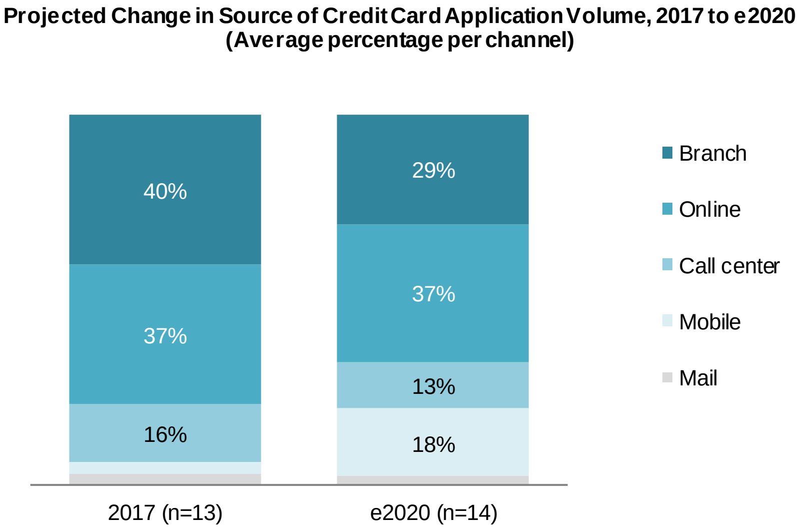
Figure 20: Projected DDA Application Volume by Channel



Source: Aite Group's survey of 30 FIs, March to June 2018

Credit card applications have been moved out of branches much more successfully to date than DDAs, with only 40% being accepted in branches in 2017; that percentage is projected to drop to 29% by 2020. Online volume in 2017 was at 37%, with no change predicted. Call center application volume is projected to drop slightly, and the big change is that the mobile channel is projected to grow to 18% of credit card application volume by 2020 (Figure 21).

Figure 21: Projected Credit Card Application Volumes by Channel

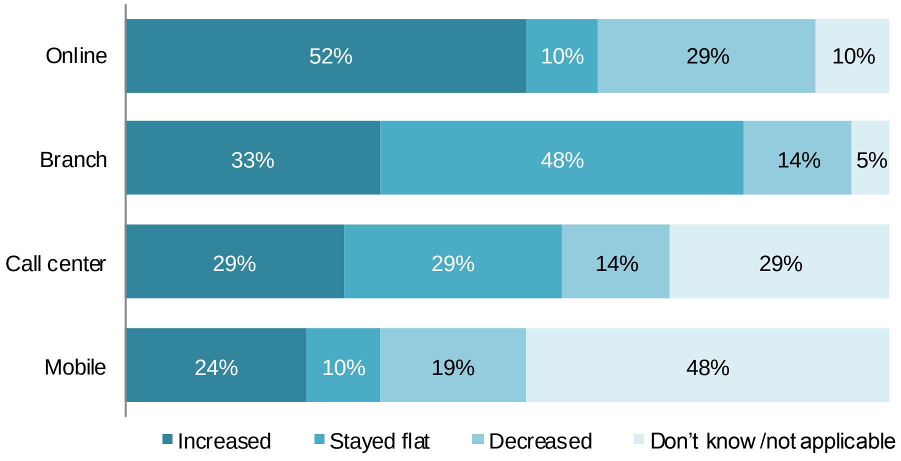


Source: Aite Group's survey of 30 FIs, March to June 2018

Organized criminal rings vary their attack methods over time; as a result, application fraud rates change in different delivery channels based on that and other factors (e.g., new capabilities rolled out for online or mobile). Over the course of the past two years, application fraud has increased in many FIs in all delivery channels to varying degrees. Over half the FIs state that this type of fraud grew online; a third saw growth in branch-originated fraud, and 24% and 29% saw growth in mobile and call center fraud, respectively. Interestingly, some FIs also saw decreases in application fraud over this period of time; 29% saw decreased application fraud in the online channel. Quite a few executives don't know whether application fraud has grown, particularly in the mobile channel. This is likely because they don't track fraud by channel or they haven't begun tracking mobile fraud separately from online fraud (Figure 22).

Figure 22: Application Fraud Trends by Channel for DDA

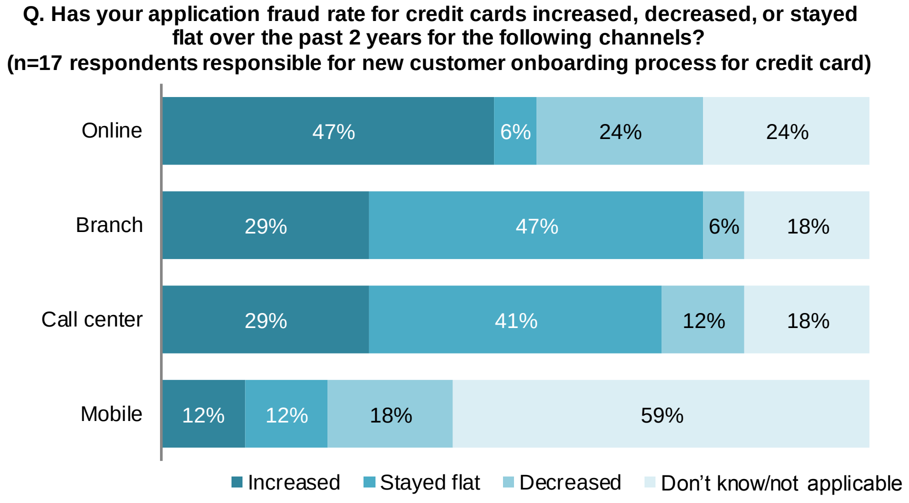
Q. Has your application fraud rate for DDA increased, decreased, or stayed flat over the past 2 years for the following channels?
(n=21 respondents responsible for new customer onboarding process for DDA)



Source: Aite Group's survey of 30 FIs, March to June 2018

Almost half (47%) of FIs experienced increased application fraud for credit cards via the online channel compared to 29% each for branch and contact centers. Twelve percent saw increased application fraud via the mobile channel. Almost half (47%) of FIs state that application fraud was flat in branches, and 41% state it was flat in call centers. The biggest decrease was in the online channel, in which 24% saw application fraud decline, and 18% saw a decline in the mobile channel (Figure 23).

Figure 23: Application Fraud Trends by Channel for Credit Card



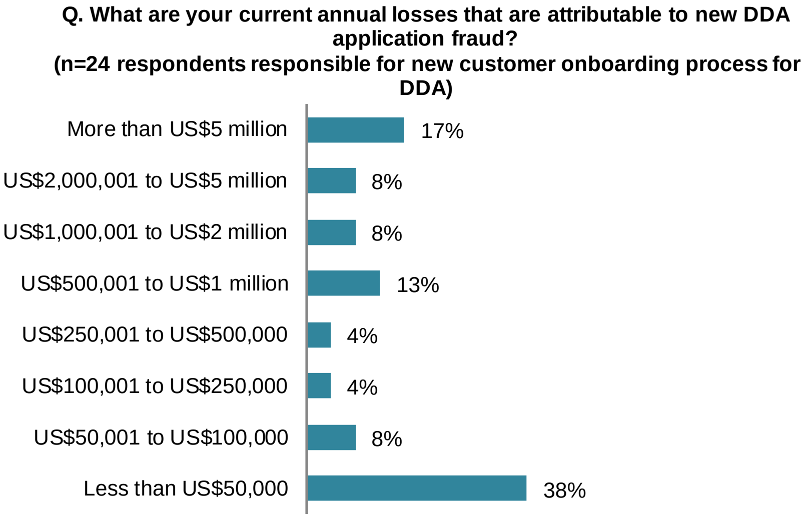
Source: Aite Group's survey of 30 FIs, March to June 2018

APPLICATION FRAUD LOSSES

FIs take many steps to detect application fraud to avoid incurring losses, but their efforts aren't always successful. Despite FIs using many systems and processes, fraudsters are still able to succeed in committing application fraud.

Seventeen percent of FIs incur more than US$5 million annually in DDA application fraud losses, while an additional 16% incur between US$1 and US$5 million. Thirty-eight percent incur less than US$50 thousand in losses (Figure 24). These findings are logical based on the fact that FIs of all sizes participated in the research.

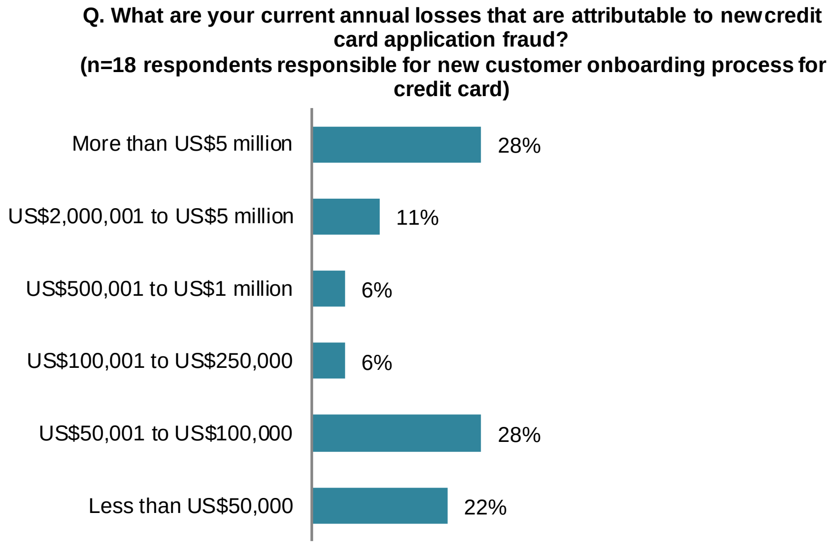
Figure 24: DDA Application Fraud Losses



Source: Aite Group's survey of 30 FIs, March to June 2018

For credit cards, application fraud is even more costly than for DDAs. Twenty-eight percent of respondents incur more than US$5 million in application fraud losses annually; an additional 11% incur between US$2 and US$5 million in losses. While 50% of FIs state they incur less than US$100,000 in application fraud losses (Figure 25), these figures may well be understated. Based on comments from more than one FI executive, a significant percentage of loan losses on credit cards have been determined to be due to the use of synthetic identity fraud, realized when collection efforts determined that there was no person in the physical world to collect from. Application fraud losses may actually be much higher than stated as a result of this insight.

Figure 25: Credit Card Application Fraud Losses

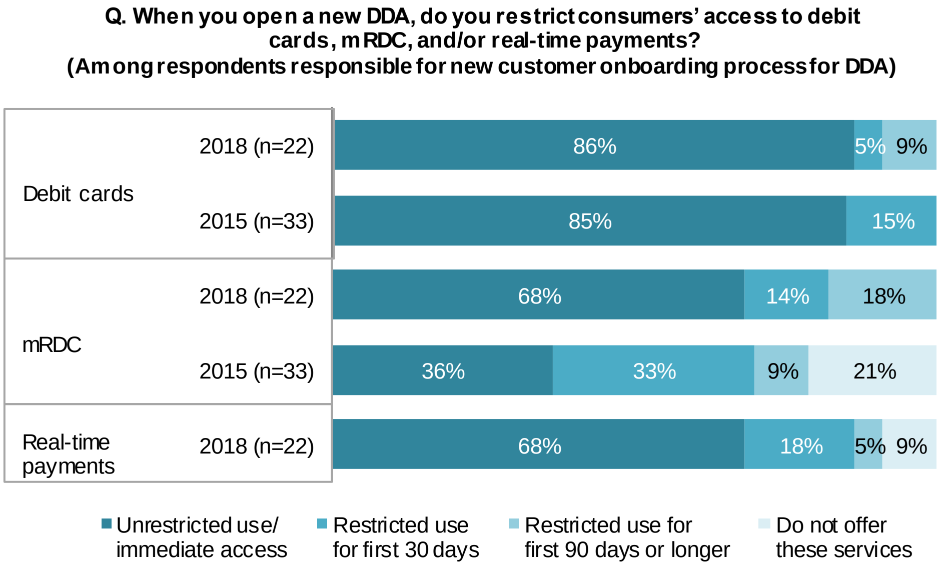


Source: Aite Group's survey of 30 FIs, March to June 2018

FRAUD MITIGATION TACTICS: POST-ACCOUNT OPENING

Many FIs take steps to reduce fraud on new accounts by restricting access to certain products until they can get to know the new customer and their normal behavior. This also allows time to pass to ensure that the account wasn't opened purely to commit fraud. In 2015, 15% of FIs restricted the use of debit cards in the first 30 days after new DDA opening. In 2018, 5% of FIs continue to do this, but 9% have increased the restriction period to 90 days. Conversely, in 2015, only 36% of FIs allowed immediate use of mobile remote deposit capture (mRDC), compared to 68% that allow immediate use in 2018. Real-time payments are new in 2018, so there is no comparative 2015 data; 68% allow new accounts immediate access to using real-time payments, while 18% restrict use for the first 30 days, and 5% restrict use for the first 90 days (Figure 26).

Figure 26: Restrictions to Curb Fraud on New Accounts



Source: Aite Group's survey of 30 FIs, March to June 2018, and Aite Group's survey of 83 U.S. FIs, November to December 2015

CONCLUSION

Application fraud will continue to be a significant challenge until solutions are implemented that enable the identity of a person to be verified reliably. Through no fault of their own, many of the existing methods of determining identity are compromised and often prove unreliable when dedicated fraudsters attack. FIs should take this into consideration moving forward.

- The bottom line is that application fraud (as well as other identity crimes) will not go away; they are far too lucrative. Unless changes are made to address these crimes, they will continue to grow, as will the resultant fraud losses.
- Try to fully understand the cost of application fraud. If some DDAs or credit card accounts are determined to be due to identity theft or synthetic identities during post-charge-off collection efforts, have a feedback loop to collect that data. Problems that are not accurately sized are difficult to address.
- Review authentication processes throughout the organization. While many FIs are still relying on third-party databases or credit bureau queries to verify identity information, this cannot be relied upon alone. Third-party databases' information is often known to fraudsters who use the data, and synthetic identities are often nurtured with a credit bureau file being created.
- Consider using a mobile identity document capture and verification solution that can be used in all delivery channels throughout the life of the new account. These solutions can help combat fraud and achieve compliance for Know Your Customer during the application process.
- While it is always difficult to stop using any solution that adds value, scrutinize existing solutions to ensure they are still providing adequate value in light of the market environment and the challenges to come. Determine if it is time to replace some solutions or whether they can be shored up with additional processes.
- If false positives (and the staff required to work alerts) are driving up operational costs, consider using machine learning models to vastly reduce the alert volume while still retaining the fraud prevention benefit.
- Delight your customers. Many new fraud solutions can detect fraudsters at work without impacting customers negatively or at all. Transparent solutions can help improve the customer experience while improving the security of the bank and its customers.

RELATED AITE GROUP RESEARCH

AIM Evaluation: Identity Document Capture and Verification, October 2018.

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

Digital Channel Fraud Mitigation: Evolving to Mobile-First, November 2017.

Financial Institution Fraud Trends: ATO and Application Fraud Rising Rapidly, May 2017.

Machine Learning for Fraud Mitigation: The Substance Behind the Buzz, April 2017.

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

Shirley Inscoe
+1.617.398.5050
sinscoe@aitegroup.com

CONTACT

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

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

ABOUT NUDATA SECURITY

NuData Security is a Mastercard company that helps businesses identify users based on their online interactions and stops all forms of automated fraud. By analyzing over 350 billion events annually, NuData harnesses the power of behavioral and biometric analysis, enabling its clients to identify the human behind the device accurately. Its award-winning technology allows clients to verify users before a critical decision, block new account or application fraud, stop automated attacks, and reduce customer insult. NuData's products are used by some of the biggest brands in the world to prevent fraud while offering a great customer experience.