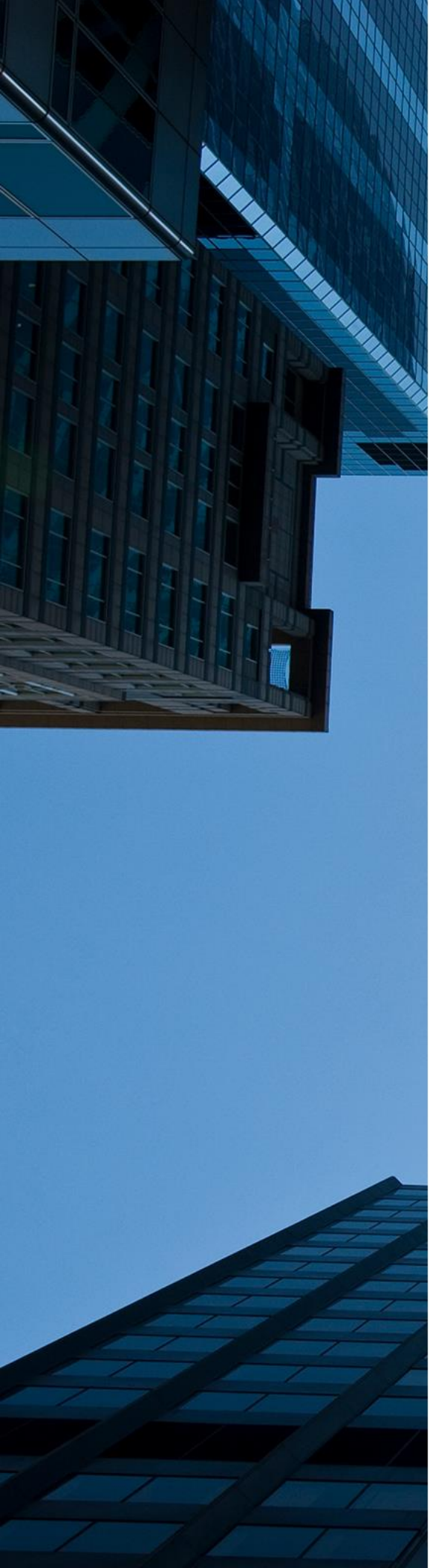


Aite Novarica

OCTOBER 2021

Fraud in Commercial Banking

STRIKING THE BALANCE BETWEEN DETECTION AND THE CUSTOMER EXPERIENCE

Prepared For:

Bottomline

OCTOBER 2021

Fraud in Commercial Banking

STRIKING THE BALANCE BETWEEN DETECTION AND the Customer eXperienceTRIKING THE BALANCE BETWEEN DETECTION AND CX

Table of Contents

List of Figures

List of Tables

Executive Summary

Commercial banking fraud mitigation is seeing a new wave of investment among financial institutions (FIs). These firms are seeking to stave off the wave of fintech firms seeking to encroach into their territory while at the same time combating escalating and highly sophisticated attack vectors from organized crime rings. The good news is that by effectively leveraging the vast amount of data at firms' disposal and applying analytics, financial services firms can walk the tightrope between detection and the customer experience (CX). Key takeaways from this white paper include the following:

- One executive interviewed for this study, whose team studiously tracks fraud attack rates at their institution, reports that attack rates have been growing by 17% per year for the past 10 years.
- Navigating the escalating threat landscape continues to be challenging. At the same time, FI fraud executives are under intense pressure to ensure that their compensating controls do not impinge upon the CX. As fraud mitigation frameworks evolve, FIs are prioritizing controls that improve the CX and facilitate seamless client onboarding and money movement while enhancing the FI's security posture.
- Anti-money laundering (AML) is a key concern in onboarding new commercial banking clients and ongoing transaction analysis. Failure to appropriately flag a transaction that has potential money-laundering implications carries the potential for steep fines and hefty reputational risk. On the flip side, needless interdiction of transactions can have significant adverse impacts on a bank's relationship with its business clients, especially when it comes to time-sensitive wire and faster-payments transactions. Many FIs have adopted integrated data strategies that help bridge the gap between the organizational silos of fraud and AML.
- Continued investment in and evolution of a robust fraud and authentication stack are now competitive issues. Firms on the leading edge will have a greater ability to acquire new customers, enable robust digital transactional functionality, and manage risk in an efficient and compliant manner. Conversely, those that lag in their investments will see their ability to acquire and keep customers wane in this increasingly digital age.

Introduction

In commercial banking, the appetite to invest in robust anti-fraud controls has experienced pendulum swings over the years in response to prevailing attack patterns and regulatory concerns. In the 2000s, investment in the digital fraud control framework focused on retail banking, given its greater volume and the easy vulnerabilities exposed at the outset of internet banking. As FIs fortified their retail defenses, attackers shifted their focus to commercial banking in the early 2010s, with a spate of high-impact corporate account takeover attacks. As the industry adjusted in the mid-2010s, imposing more stringent multifactor controls on commercial banking activity, organized crime pivoted to focus intensely on retail banking. These attackers brought to bear a formidable quantity of breached personally identifiable information and compromised credentials, combined with automation and social engineering.

Now, these organized crime rings recognize that this same combination of data resources, automation, and social engineering tactics can be applied to perpetrate commercial banking fraud, often with significantly higher rewards. This white paper looks at key trends driving loss mitigation strategies for commercial banking firms and how their defensive plans will evolve over the next one to two years.

Methodology

Between April and June 2021, Aite-Novarica Group interviewed fraud executives at 11 large North American FIs and two fintech firms that focus on the commercial banking space to understand the trends and business-case drivers for evolving their control frameworks. In addition, this white paper includes insights from a survey of fraud executives at 32 financial services firms conducted in September and October 2021. Given the size and structure of the research sample, the data reported provide a directional indication of market conditions.

Escalating Attack Vectors

"Fraud Incorporated" is a fully industrialized adversary. It has developed a highly efficient and lucrative approach to committing fraud at scale, combining its vast amount of breached data with sophisticated automation and social engineering techniques. Once funds have been stolen, crime rings use well-developed mule networks to exit the funds from the system, often taking advantage of faster payment rails to move money multiple times quickly, obfuscating the trail. Table A elaborates some of the leading attack vectors targeting commercial banks and their business clients.

TABLE A: LEADING COMMERCIAL BANKING ATTACK VECTORS

Attack Vector	Definition
Account takeover (ATO)	Using compromised credentials or social engineering, attackers log in to an existing customer account to extract some form of monetary benefit.
Business email compromise (BEC)	In BEC attacks, fraudsters trick businesses into initiating funds transfers to accounts under the fraudsters' control. Because these scams result in the responsible party at the organization voluntarily initiating the transaction, most of the usual multifactor authentication controls are not able to detect the fraud. The U.S. FBI estimates US$1.8 billion in BEC losses in 2020,[1] and most FIs interviewed by Aite-Novarica Group believe that statistic to be understated.
Man-in-the-middle (MITM) and remote access trojan (RAT) attacks	MITM attacks occur when an attacker inserts himself into the communication flow, either stealing secrets or altering transaction instructions. RATs are a form of malware that enable attackers to gain unauthorized access to a victim's device.

Source: Aite-Novarica Group

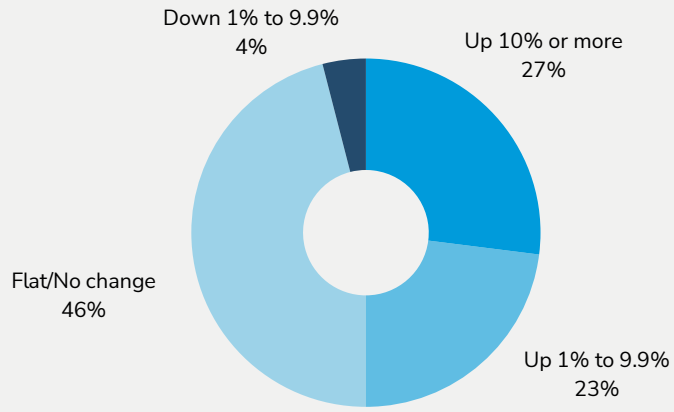
One FI executive interviewed for this study whose team studiously tracks fraud attack rates at their institution reports that attack rates have been growing by 17% per year for the past 10 years. This percentage is consistent with the results of the September and October 2021 survey. BEC has become particularly problematic for commercial

[1] "Internet Crime Report 2020," U.S. Federal Bureau of Investigation, March 17, 2021, accessed September 14, 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

bankers and their customers. Half of FIs have seen BEC increase from the first half of 2020 to the first half of 2021, growing from an already substantial base number (Figure 1).

FIGURE 1: BEC CONTINUES ITS PRECIPITOUS RISE

Q. Please estimate the trend associated with BEC fraud attacks, comparing attack rates between the first half of 2020 and the first half of 2021. (Base: 26 financial services fraud decision-makers)



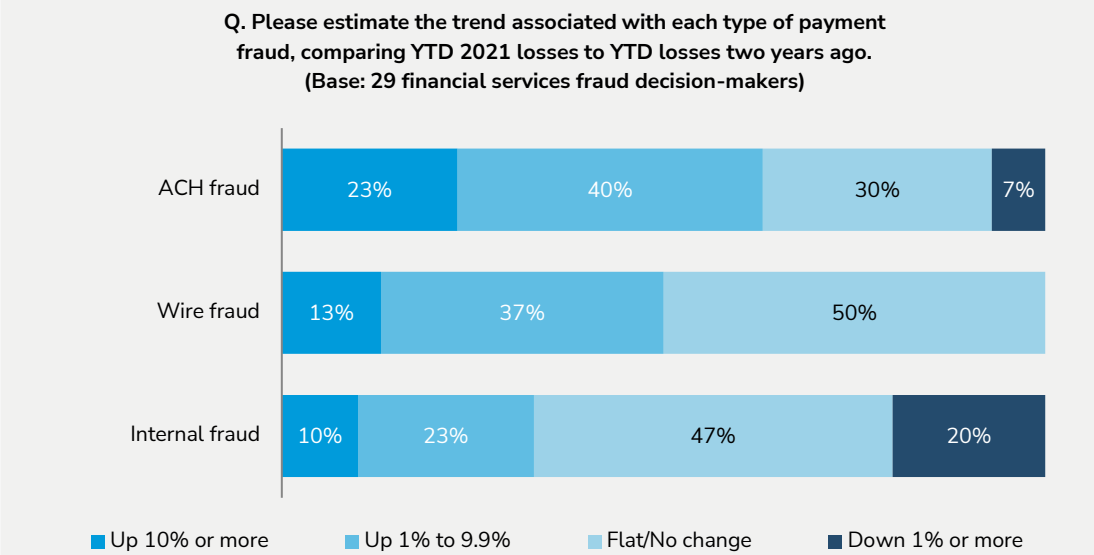
Source: Aite-Novarica Group survey of fraud decision-makers at 32 financial services firms, September to October 2021

As is to be expected, increasing losses accompany rising attack volume. Thirty-four percent of respondents have seen losses due to internal fraud increase from 2020 to 2021. This is not at all surprising, given the rapid shift to working from home in the first half of 2020 as a result of the pandemic; many financial services firms had concerns about the fallout of that sudden change.[2] While much is working well in the pivot to working from home, there are also a number of data compromise risks that FI fraud and information security executives believe have yet to be adequately addressed.

Half of respondents have seen increased wire fraud losses year-to-date in 2021 versus losses year-to-date in 2019 over the past two years, 63% of respondents have seen increased ACH fraud losses, and one-third have seen increased internal fraud losses over the same period (Figure 2). Notably, very few institutions indicate that losses have decreased.

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

FIGURE 2: FRAUD LOSSES ARE INCREASING ON MANY FRONTS



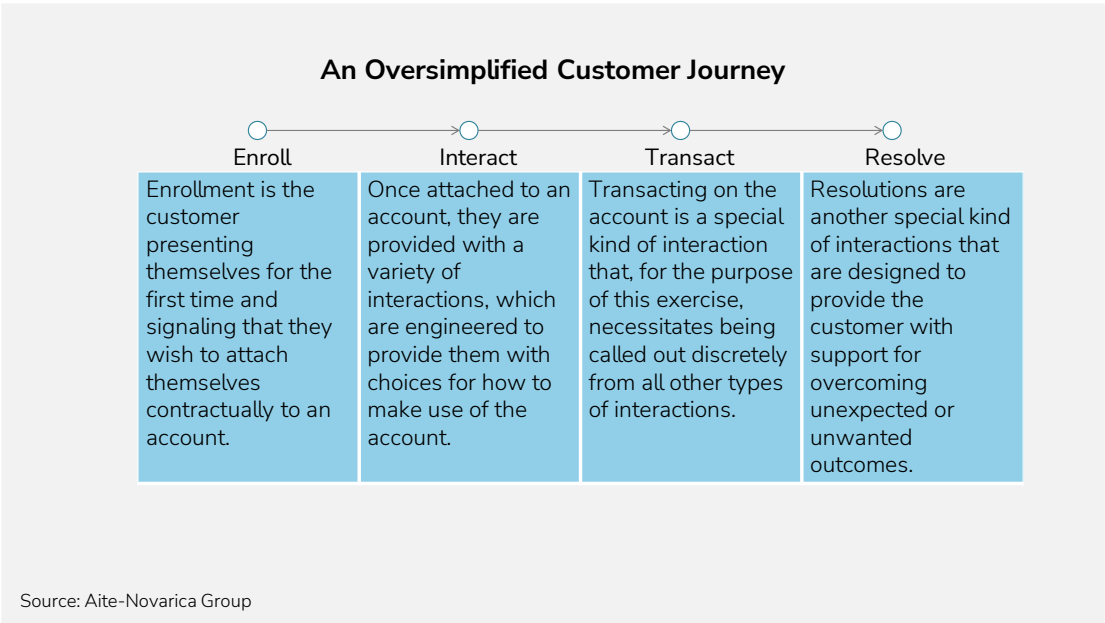
Source: Aite-Novarica Group survey of fraud decision-makers at 32 financial services firms, September to October 2021

Best Practices in Control Frameworks

While the escalating threat landscape continues to be challenging to navigate, FI fraud executives are under intense pressure to ensure that their compensating controls do not impinge upon the CX. Optimally, as those frameworks evolve, controls that improve CX and facilitate seamless client onboarding and money movement, while at the same time enhancing the FI's security posture, will be prioritized. As such, fraud executives today face an incredibly dynamic balancing act among loss prevention, client experience, operational efficiency, and regulatory compliance.

Figure 3 provides a simplified view of the layers of controls required to manage risk and explains how these map to the customer journey. There is a good deal of overlap among the various stages. Many FIs increasingly deploy transaction monitoring across the customer journey to enable a holistic view of customer behavior. This approach facilitates modeling down to a segment of one, rather than solely relying on peer group analysis, which is prone to both false positives and false negatives. Similarly, while identity authentication is a key mechanism to control for ATO, it is also widely used at onboarding to help automate anomaly detection. And in the resolution stage, case management is a critical building block supporting the entire process of fraud identification and mitigation, all the way through to the eventual filing of a suspicious activity report.

FIGURE 3: ALIGNING CONTROLS WITH THE CUSTOMER JOURNEY



Source: Aite-Novarica Group

The Need for Integrated AML Signals

The challenge of risk mitigation in commercial banking is by no means limited to fraud attack vectors. AML is another key concern when it comes to onboarding new commercial banking clients and ongoing transaction analysis. Failure to appropriately flag a transaction that has potential money-laundering implications carries the potential for steep fines and hefty reputational risk. On the flip side, needless interdiction of transactions can have significant adverse impacts on a bank's relationship with its business clients, especially when it comes to time-sensitive wire and faster-payments transactions.

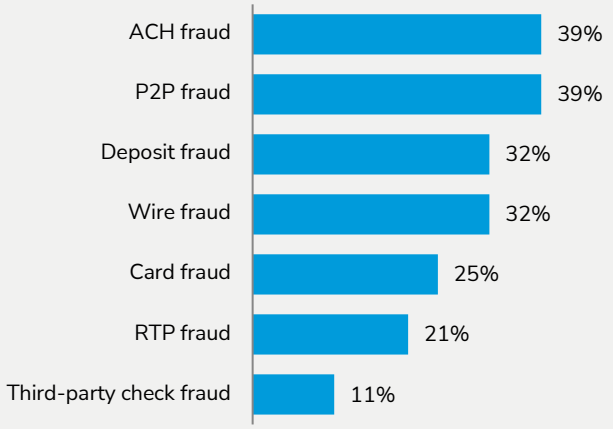
Many FIs have adopted integrated data strategies that bridge the gap between the organizational silos of fraud and AML. These FIs leverage common data lakes and case management functionality and look for opportunities to align detection strategies as appropriate. As faster-payments rails gain traction around the globe, the ability to take an integrated, real-time approach to sanctions screening and fraud detection is particularly important. Done properly, this can help achieve the trifecta of improving detection, enhancing CX, and optimizing operational efficiency.

Evolution of the Control Framework

Among FIs surveyed, the ability of existing control frameworks to control for ACH fraud tops the list as a key concern (Figure 4). When asked about plans to make investments in substantial transformation of the control framework over the next one to two years, 69% of FIs surveyed plan to substantially evolve their ACH/wire controls, 77% plan transformation of real-time payment controls, 57% of respondents plan to make significant changes to their internal fraud detection capabilities, and 54% plan to make substantial investments in their case management systems (Figure 5).

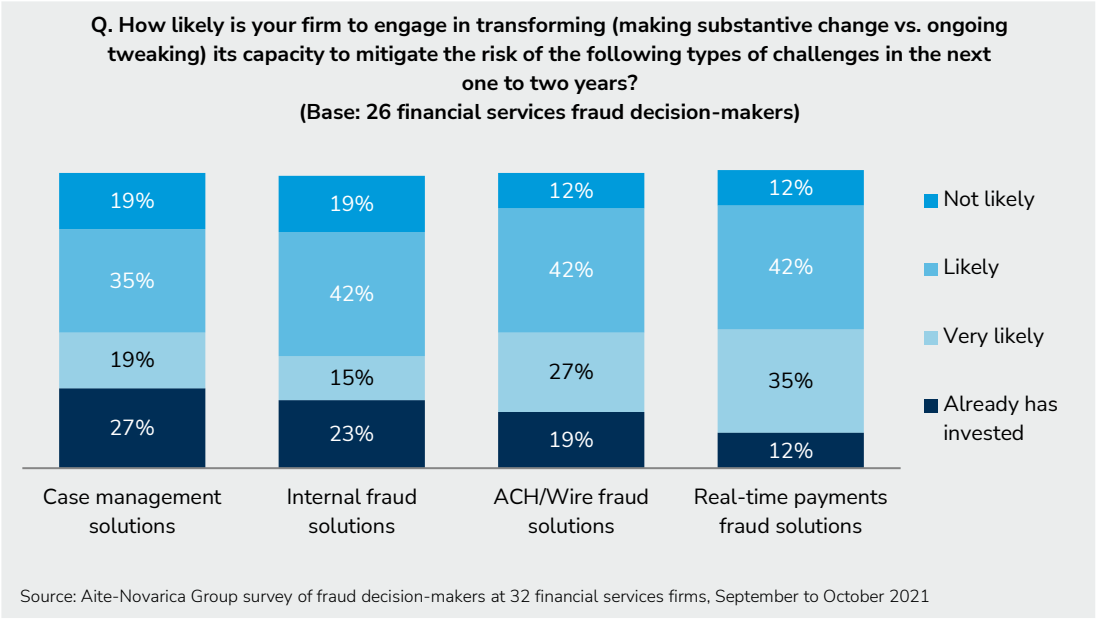
FIGURE 4: ACH FRAUD IS A TOP FRAUD CONCERN

Q. Thinking about the capabilities of your firm's transaction monitoring control framework to adequately detect attacks and prevent losses, which two types of fraud are you most concerned about in 2021?
(Select top two; Base: 28 financial services fraud decision-makers)



Source: Aite-Novarica Group survey of fraud decision-makers at 32 financial services firms, September to October 2021

FIGURE 5: ACH, WIRE, AND RTP CONTROLS WILL SEE SIGNIFICANT INVESTMENT



Source: Aite-Novarica Group survey of fraud decision-makers at 32 financial services firms, September to October 2021

Security as a differentiator

A best-in-class control framework not only protects the bottom line but enables the deployment of differentiating capabilities in digital channels and drives more revenue opportunities. Of the 13 FIs and fintech firms that participated in the qualitative interviews for this white paper, less than half of the 11 FIs enable online onboarding for small and midsize business clients. In every case, those that do not have this capability cited their lack of ability to manage the risk as the driving factor. Both fintech firms enable online onboarding—it's the only means by which they acquire new customers.

This underscores the extent to which continued investment and evolution of a robust fraud and authentication stack are now competitive issues. Firms on the leading edge will have a greater ability to acquire new customers, enable robust digital transactional functionality, and efficiently manage risk in a compliant manner. Conversely, those that lag in their investments will see their ability to acquire and keep customers wane in this increasingly digital age.

Conclusion

The challenges facing fraud executives in commercial banking will not get easier anytime soon. The sophistication of the attack surface shows no sign of abating. At the same time, the imperative of appropriate friction and minimizing false positives, driven by customer expectations, will also only continue to increase. As such, many firms are seeking to reevaluate and enhance their control frameworks for their business clients. Here are a few recommendations for firms as they strive to improve their fraud prevention capabilities:

- **Focus on your data.** Properly leveraged, your data can be your greatest asset. Look for ways collect and analyze customer data and metadata across the customer life cycle to assess both fraud and AML risk.
- **Collaborate with your business partners.** Given the increasing imperative that fraud and authentication solutions must not impinge upon the CX, many fraud executives are collaborating with their business counterparts to help fund solutions that will enhance their security posture and also reduce undue friction in the CX.
- **Ensure your solutions are real time.** With the advent of instant onboarding for small businesses and faster payments, fraud solutions have to analyze and respond in real time. Anything less will expose gaps in the control framework and have adverse impacts on the CX.

About Bottomline Technologies

Bottomline Technologies (Nasdaq: EPAY) makes complex business payments simple, smart, and secure. Corporations and banks rely on Bottomline for domestic and international payments, efficient cash management, automated workflows for payment processing and bill review, fraud detection, behavioral analytics, and regulatory compliance solutions. Thousands of corporations around the world benefit from Bottomline solutions.

Bottomline's Secure Payments solution enables real-time payment fraud protection, continuous risk assessment, and the ability to meet compliance regulations. Leveraging machine learning, rich visualization and forensic tools, the solution can reduce a firm's risk profile. Secure Payments works with multiple banking platforms and payment systems for quick activation and low total cost of ownership.

About Aite-Novarica Group

Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base. The quality of our research, insights, and advice is driven by our core values: independence, objectivity, curiosity, and integrity.

Contact

Research and consulting services:
Aite-Novarica Group Sales
+1.617.338.6050
sales@aite-novarica.com

Press and conference inquiries:
Aite-Novarica Group PR
+1.617.398.5048
pr@aite-novarica.com

For all other inquiries, contact:
info@aite-novarica.com

Global headquarters:
280 Summer Street, 6th Floor
Boston, MA 02210
www.aite-novarica.com

Author Information

Julie Conroy
+1.617.398.5045
jconroy@aite-novarica.com

Research design and data:
Judy Fishman
jfishman@aite-novarica.com