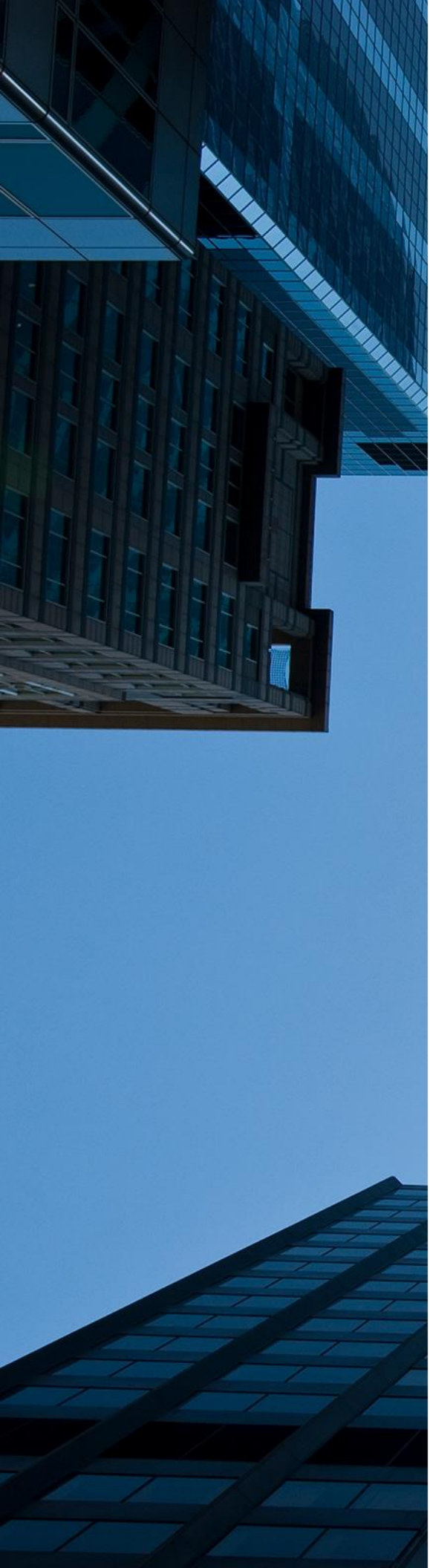


Aite Novarica

OCTOBER 2021

INTEGRATING ATO AND PAYMENT FRAUD SYSTEMS

BUILDING STRONGER DEFENSES FOR FINTECH FIRMS AND THEIR CUSTOMERS

PREPARED FOR:

sift

OCTOBER 2021

INTEGRATING ATO AND PAYMENT FRAUD SYSTEMS

Building Stronger Defenses for Fintechs and Their Customers

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Integrating ATO and Payment Fraud Systems, commissioned by Sift and produced by Aite-Novarica Group, explores the state of fraud management within fintech firms. It examines the extent to which fintech firms share data among their account-level and payment-level fraud systems, common reasons why firms do not share data, and the perceived versus actual benefits of bringing these systems together.

Key takeaways from the study include the following:

- Fintech firms report that managing account takeover (ATO) fraud is their most significant issue (46%), followed closely by handling payment fraud (42%). Managing new account opening fraud is a distant third, at 12%.
- Seventy-five percent of fintech firms manage fraud in-house, with 47% using a multivendor approach and 28% using a single vendor.
- Fifty-three percent of firms share data among their ATO and payment fraud systems, while 46% would like to share data but face obstacles to the practice.
- Fintech firms that share data among their ATO and payment fraud systems are twice as likely to report it is very or somewhat easy to manage fraud.
- Those fintech firms that do not share ATO/payment data consistently underestimate the potential benefits of data sharing compared to the realized benefits among fintech firms that do share data.
- Among all fintech firms, 78% have some preference or a strong preference for an all-in-one solution from one vendor.
- As fraud becomes ever more complex, fintech firms need adaptable strategies and systems that can mitigate fraud losses while also delivering strong customer experiences. By sharing and integrating data among ATO and payment fraud systems, and implementing a multiprong, integrated fraud detection suite from a single vendor, fintech firms can achieve those goals.

INTRODUCTION

Fintech firms live in a digital world where nearly all of their business is conducted online. Not only do they lack face-to-face interactions with their customers, but they also do not have the luxury of directing customers to a branch location for high-risk transactions. They need to excel at opening new accounts and providing superior customer experiences while protecting applicants and existing customers against fraudsters. Their fraud problems do not stop there, though. They also have to guard against online financial transactions, which have higher fraud rates than in-person transactions. And organized crime rings are growing in sophistication, increasingly automating their attacks. This challenges fintech firms to adapt and upgrade fraud systems to stay current with the newest attack vectors.

Fraud systems commonly evolve over time. Point solutions are deployed at different moments to address specific deficiencies in a firm's defenses. Often, these solutions are "islands" that serve a particular function, but they are not integrated and do not share data. As technology-first organizations, fintech firms tend to have newer fraud solution stacks compared to traditional financial institutions. As such, they provide an interesting opportunity to compare the performance of stand-alone fraud tools versus integrated fraud systems. What can be learned from these digital-only firms about fighting fraudsters who continually attack the online channel?

METHODOLOGY

In this research, sponsored by Sift, Aite-Novarica Group conducted a quantitative survey of 110 fintech firms in the U.S. and the U.K. in September 2021 about their approach to protecting users' digital accounts and financial transactions. Survey respondents are influencers or decision-makers in areas such as online payments, digital fraud or loss prevention strategies, or IT security. Two-thirds of the firms are in consumer wealth management (35%), personal finance (20%), and digital wallets (10%). The remaining one-third are in a variety of other fintech businesses.

The data for the full fintech sample has a margin of error of 9 points at the 95% level of confidence; statistical tests of significance were conducted at 90% level of confidence.

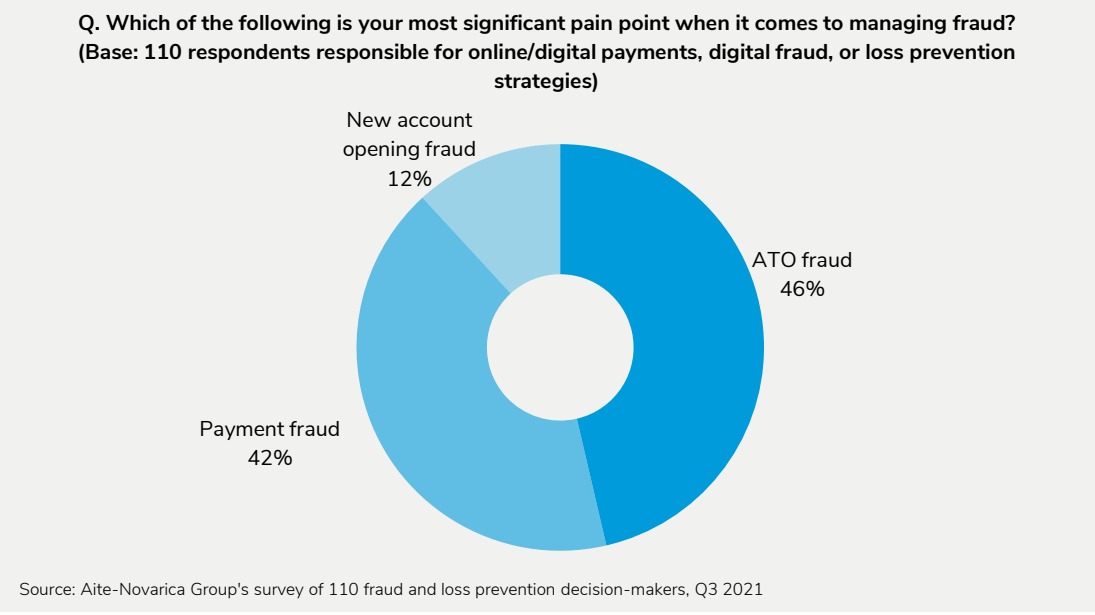
STATE OF FRAUD MANAGEMENT AT FINTECH FIRMS

Any firm conducting business online knows there are three points in a user's digital engagement when fraud commonly occurs:

- Opening a new online account
- Logging in to an existing online account
- Performing a financial transaction

It is no surprise that 46% of fintech firms report that ATO is the most prevalent problem. This is primarily the result of billions of breached accounts containing personally identifiable information and username/password pairs, the high rate at which consumers reuse passwords across multiple websites, and the growing sophistication and prevalence of credential-stuffing tools used by fraudsters to ascertain valid username/password pairs. On the heels of ATO fraud, protecting against payment fraud is fintech firms' next most common concern, at 42% (Figure 1).

FIGURE 1: MOST SIGNIFICANT FRAUD PAIN POINTS TO MANAGE

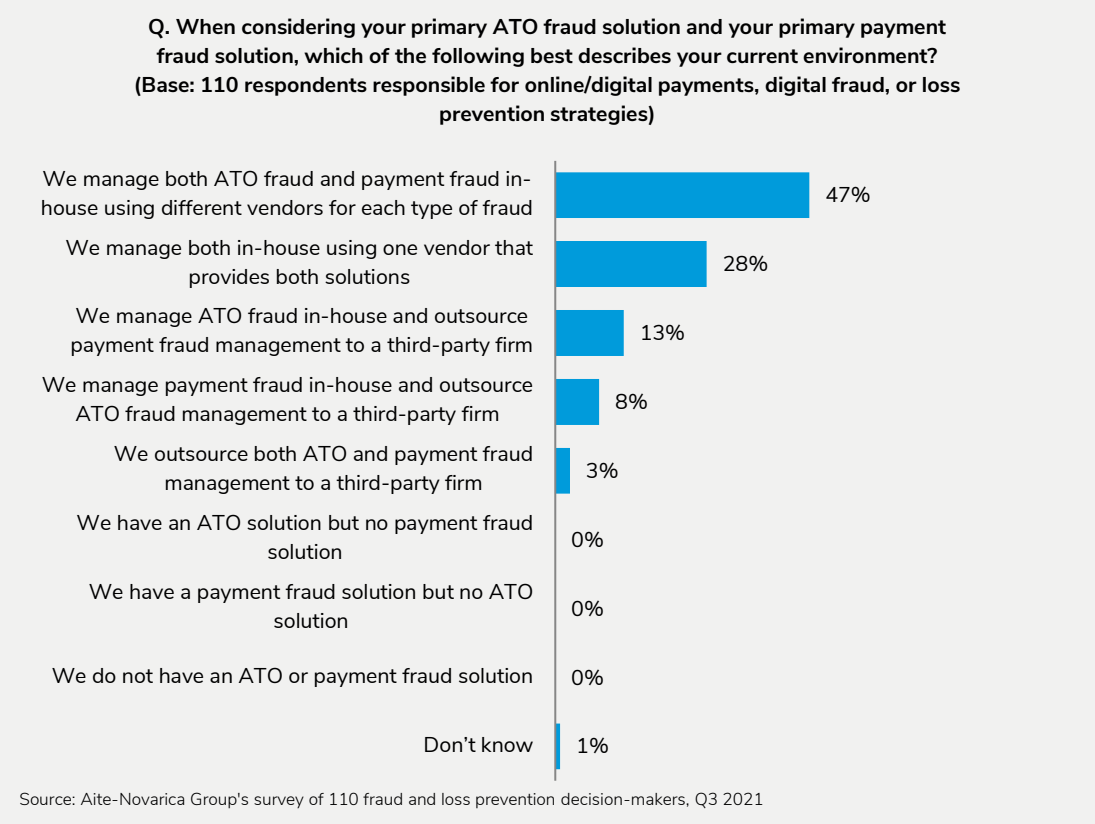


Source: Aite-Novarica Group's survey of 110 fraud and loss prevention decision-makers, Q3 2021

Seventy-five percent of the fintech firms manage ATO and payment fraud in-house using either a multivendor suite of tools (47%) or solutions from a single vendor (28%).

This shows their commitment to deploying resources to actively manage fraud internally. The remaining fintech firms use some combination of in-house and third party to manage ATO and payment fraud (Figure 2).

FIGURE 2: HOW ATO AND PAYMENT FRAUD ARE MANAGED

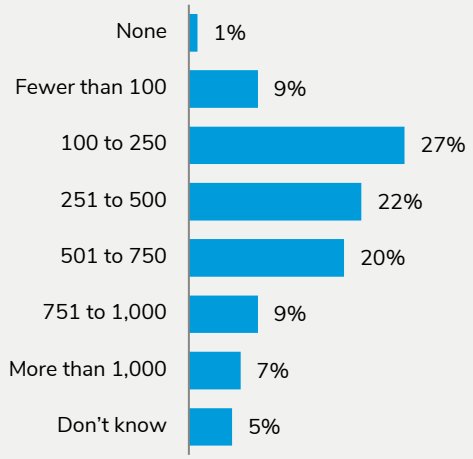


Source: Aite-Novarica Group's survey of 110 fraud and loss prevention decision-makers, Q3 2021

Funding an account via a credit or debit card is a common practice for fintech firms (83%). This is significant since it creates potential financial liability for the fintech firm based on chargeback liability rules defined by the card brands. It also increases operational costs for fintech firms due to the systems and staff required to process chargebacks. And nearly 70% of these firms receive between 100 and 750 chargebacks annually (Figure 3).

FIGURE 3: ANNUAL CHARGEBACK VOLUME FROM CARD-BASED ACCOUNT FUNDINGS

Q. On average, how many chargebacks do you receive annually from credit/debit card account fundings? (Base: 91 respondents responsible for online/digital payments, digital fraud, or loss prevention strategies at fintech firms that allow funding of an account via a credit or debit card)



Source: Aite-Novarica Group's survey of 110 fraud and loss prevention decision-makers, Q3 2021

The next few survey questions relate to the effort required to manage fraud, and realized benefits proves to be key differentiators among fintech firms. When asked whether fintech firms share data across their ATO fraud system and payment fraud system, 53% of the fintech firms say they currently share data, while 47% would like to but currently do not. Forty-one percent of fintech firms share data among their ATO fraud system and chargeback system, while 56% would like to but currently do not (Figure 4). It is also worth highlighting that only two respondents have no interest in sharing data, illustrating the strong interest in and importance of data sharing.

Common reasons for not integrating ATO fraud data with payment fraud and chargeback systems follow:

- High level of IT effort
- Approval of the business case
- Organizational challenges with ATO and other systems managed in different departments

FIGURE 4: PREVALENCE OF SHARING ATO DATA AMONG OTHER FRAUD SYSTEMS

Q. When considering sharing data between your ATO fraud solution and payment fraud solution, which of the following best describes your current environment?
(Base: 110 respondents responsible for online/digital payments, digital fraud, or loss prevention strategies)

Source: Aite-Novarica Group's survey of 110 fraud and loss prevention decision-makers, Q3 2021

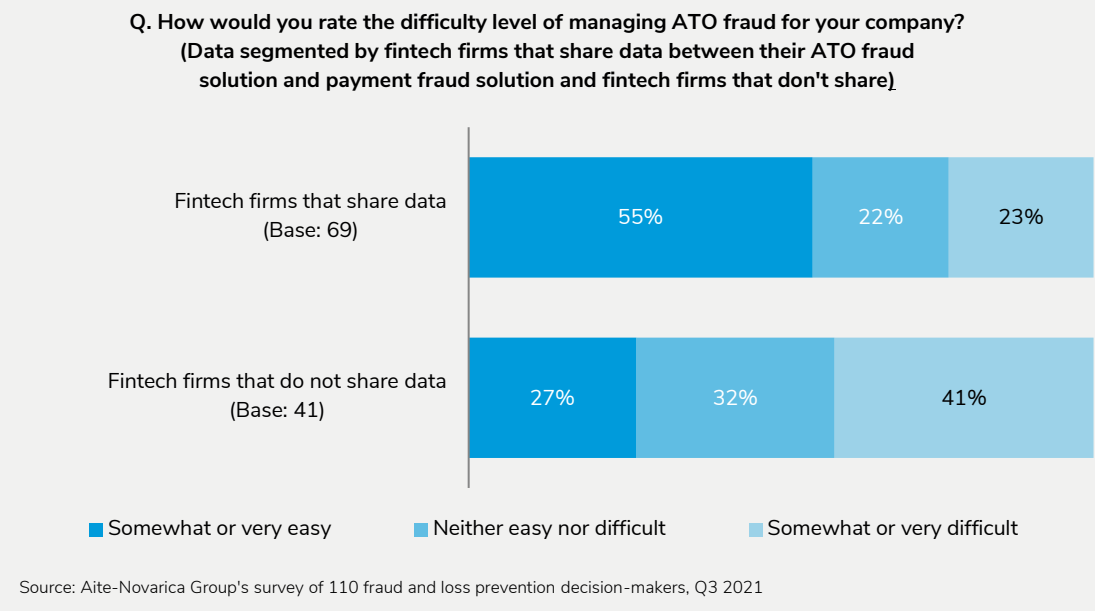
BENEFITS OF INTEGRATED FRAUD MANAGEMENT

Managing fraud is a complex problem, especially as fraudsters evolve and their attacks become more sophisticated. If not done properly, managing fraud can be a significant challenge and a constant source of aggravation.

Fintech firms that share data among their ATO and payment fraud systems report that managing fraud is significantly easier than do those fintech firms that do not share data. Those that share data are twice as likely to say it is somewhat or very easy to manage ATO fraud (55% versus 27%; Figure 5). They are also twice as likely to say it is somewhat or very easy to manage payment fraud (57% versus 27%; Figure 6).

These results clearly demonstrate that fintech firms with integrated ATO and payment fraud systems have a more manageable level of effort. This could be partly due to increased access to and visibility of data to assist fraud teams, eliminating the need for manual searches. Also, ATO fraud systems collect a wealth of information that can be useful to train the machine learning models used in payment fraud systems.

FIGURE 5: EASE OF EFFORT TO MANAGE ATO FRAUD



Source: Aite-Novarica Group's survey of 110 fraud and loss prevention decision-makers, Q3 2021

FIGURE 6: EASE OF EFFORT TO MANAGE PAYMENT FRAUD

Source: Aite-Novarica Group's survey of 110 fraud and loss prevention decision-makers, Q3 2021

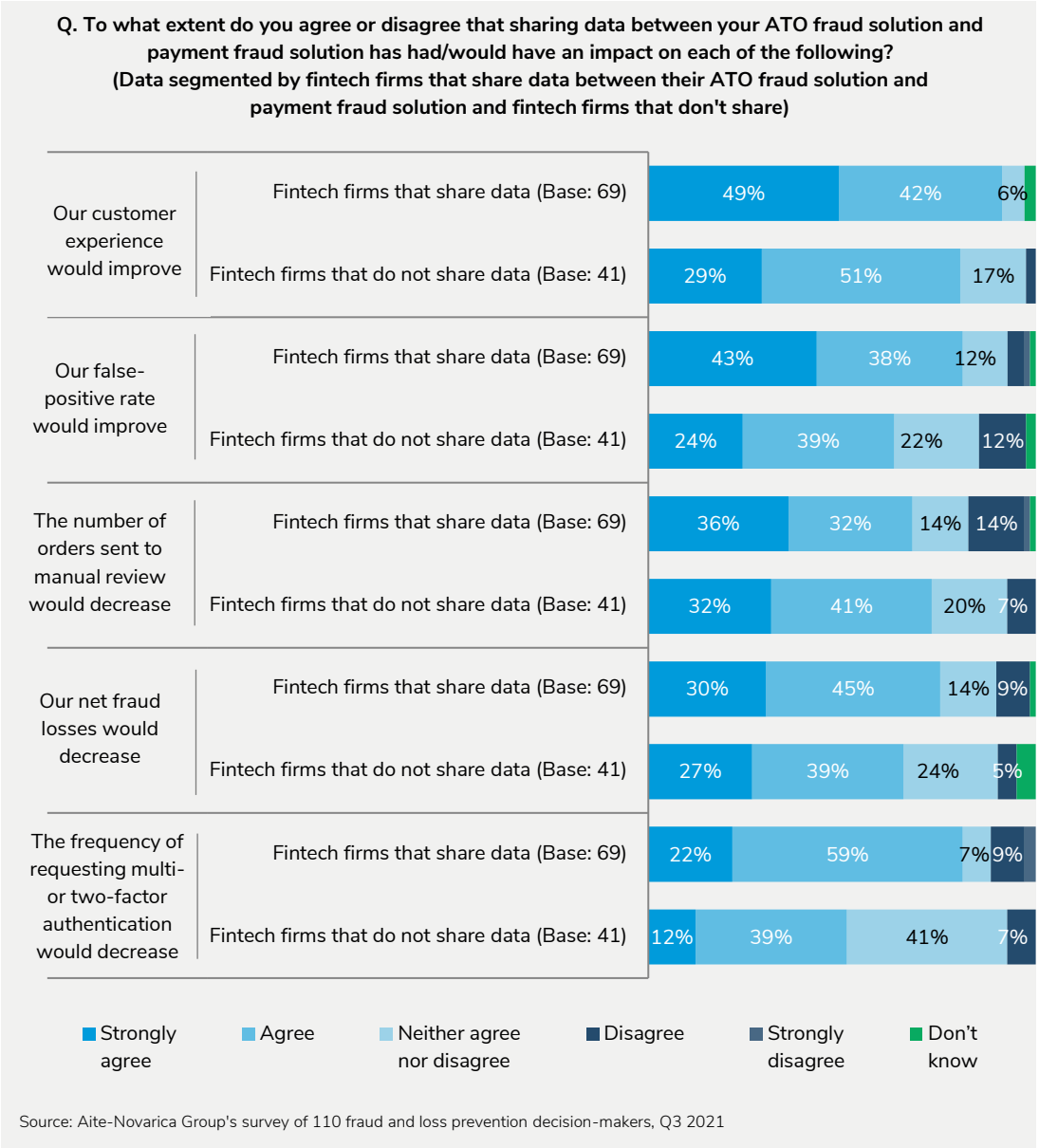
As noted earlier, 28% of the respondents report they manage ATO and payment fraud in-house using a single-vendor solution, yet 53% share data among these two systems. It is safe to say some fintech firms that use a multivendor suite of solutions have taken the effort to integrate their fraud systems. When asked how interested fintech firms would be in using an integrated ATO and payment fraud solution from a single vendor, 72% of those who share data are very or extremely interested in such a system compared to 49% of those that do not share data.

Strong interest in an integrated fraud solution among both groups suggests that there are perceived or actual benefits to be derived from this type of system configuration. Aite-Novarica Group explored to what degree each of these groups believe they would realize benefits in the following five areas:

- Customer experience
- False-positive rate
- Number of orders sent to manual review
- Net fraud losses
- Frequency of requests for multi- or two-factor authentication

Fintech firms that do not share data believe they would derive benefits in all of these areas. However, when compared to the actual benefits that fintech firms that share data realize from their integrated ATO and payment fraud systems, those that do not share data consistently underestimate how much benefit would be achieved (Figure 7).

FIGURE 7: PERCEIVED VS. ACTUAL BENEFITS DERIVED FROM AN INTEGRATED ATO/PAYMENT FRAUD SOLUTION



Source: Aite-Novarica Group's survey of 110 fraud and loss prevention decision-makers, Q3 2021

The starkest contrast between fintech firms that do and don't share data among ATO and payment fraud systems relates to how often multifactor authentication (MFA) is needed to authenticate a user. Eighty-one percent of fintech firms that share data agree or strongly agree that MFA usage has decreased, but only 51% of fintech firms that don't share data believe MFA usage would decrease. The next most significant difference is in false-positive rates. Eighty-one percent of fintech firms that share data agree or strongly agree that their false-positive rates have improved, while just 63% of those that don't share data expect an improvement in false-positive rates. These metrics speak to the imperative of streamlining the user experience and removing friction—common goals across financial services firms. And for those fintech firms that want to share data among ATO and payment fraud systems but cannot build a business case to justify the project, the value of these benefits in those business cases is likely underestimated.

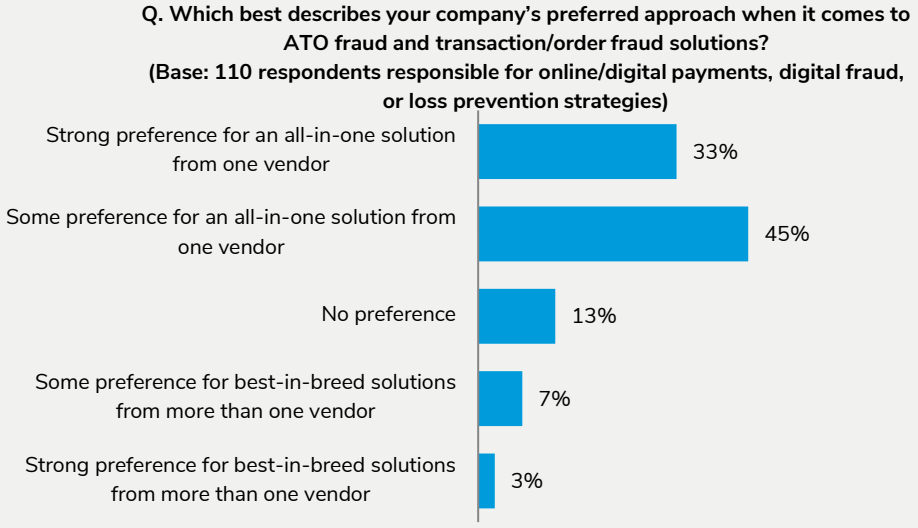
TABLE A: PERCEIVED VS. ACTUAL BENEFITS OF AN INTEGRATED FRAUD SOLUTION

BENEFITS	REALIZED BENEFITS OF FINTECH FIRMS THAT SHARE DATA	EXPECTED BENEFITS OF FINTECH FIRMS THAT DON'T SHARE DATA	DELTA BETWEEN REALIZED AND EXPECTED BENEFITS
Customer experience would improve	91%	80%	11%
False-positive rate would improve	81%	63%	17%
The frequency of requesting multi- or two-factor authentication would decrease	81%	51%	30%
Net fraud losses would decrease	75%	66%	9%
The number of orders sent for manual review would decrease	68%	73%	-5%

Source: Aite-Novarica Group

To realize the benefits of sharing data among ATO and payment fraud systems, a fintech firm needs to either integrate disparate systems from multiple vendors or deploy an integrated solution from one vendor. Since fintech firms' number-one stated reason for not integrating these systems is the level of IT effort required, it is no surprise that 78% of fintech firms have either some or a strong preference for an all-in-one solution from one vendor (Figure 8). This reduces the number of vendors to manage and eliminates the need for fintech firms to expend IT effort to integrate disparate systems, among other benefits.

FIGURE 8: PREFERENCE FOR AN ALL-IN-ONE SOLUTION FROM ONE VENDOR



Source: Aite-Novarica Group's survey of 110 fraud and loss prevention decision-makers, Q3 2021

CONCLUSION

Managing fraud in today's complex and constantly evolving environment is no easy task. As fraudsters become more sophisticated, fintech firms need to adapt to control fraud losses while also providing a good user experience. To achieve these goals, the following recommendations should be embraced by fintech firms:

- Share data among ATO and payment fraud systems to enhance the performance of both systems. This will significantly simplify the effort to manage fraud, which is especially important as this task will become more difficult over time.
- Refine and enrich business cases to reflect the many benefits of data sharing more accurately, especially the reduction in MFA usage and improvements in false-positive rates. Current benefit estimates are likely underappreciated and understated by many fintech firms, especially those that do not share data across diverse fraud systems. With a stronger list of expected benefits, the likelihood your business case will be approved increases.
- Minimize IT effort to integrate disparate systems by considering a multiprong fraud suite from one vendor that has already integrated its solutions. With IT resources at a premium, initial implementation effort and ongoing maintenance will be decreased with an integrated, single-vendor solution.

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, leveraging deep insights developed via our extensive network of clients and other industry contacts.

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

David Mattei
+1.617.398.0908
dmattei@aite-novarica.com

Research Design & Data:
Sarah Fitzsimmons
sfitzsimmons@aite-novarica.com