Aite Novarica

OCTOBER 2021

MAXIMIZING THE POTENTIAL OF CNP

COLLABORATION VIA 3-D SECURE IS KEY

JULIE CONROY
DAVID MATTEI
RON VAN WEZEL

This report provided compliments of:

OUTSEER
An RSA Company

IMPACT REPORT

IMPACT REPORT

OCTOBER 2021

MAXIMIZING THE POTENTIAL OF CNP

COLLABORATION VIA 3-D SECURE IS KEY

JULIE CONROY
DAVID MATTEI
RON VAN WEZEL

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

IMPACT POINTS

- As the global card payment ecosystem evolved over the past 20 years to protect card-present payment transactions with chip cards, card-not-present (CNP) transactions have seen a significant increase in fraud as fraudsters shifted their attack strategies. As a result, merchants, issuers, payments networks, and governments across the globe are looking for ways to stem the rising tide of CNP fraud. A key tool in their arsenals is 3-D Secure (3DS).
- In this research, sponsored by Outseer, an RSA company, Aite-Novarica Group interviewed 34 large issuers and issuing processors in North America, Europe, and the Asia-Pacific, and deployed a quantitative survey of 756 midsize and large e-commerce merchants in those same geographic regions during Q2 and Q3 2021.
- The U.S. has seen a steady rise in CNP fraud losses, which now represent the vast majority of card fraud. Aite-Novarica Group estimates U.S. CNP fraud losses will total a whopping US$7.9 billion by the end of 2021, while the global impact of CNP fraud will be US$15.3 billion.
- In regions like the EU, India, and Australia, where either governmental or payment network mandates for multifactor authentication (MFA) are in effect, the stronger security has been a very effective deterrent to fraud. The widespread requirement for strong customer authentication (SCA) in the EU is already showing its ability to deter CNP fraud. Just as when countries across the globe upgraded to EMV and the fraud attacks migrated to those countries wherein chip cards had not yet been deployed, fraudsters will follow a similar pattern in the CNP environment.
- Overall, 82% of issuers and processors interviewed said that 3DS is as effective or more effective for fraud detection when compared to other fraud solutions. Issuers' perspectives regarding the effectiveness of 3DS relative to other CNP fraud mitigation techniques vary widely based on geography. In Europe and parts of the Asia-Pacific wherein MFA for CNP transactions is mandated, 100% of issuers view it as effective or highly effective. In North America, where there is no 3-D Secure mandate, the effectiveness is not viewed as favorably. The disparity largely lies in the fact that in countries where MFA for CNP transactions is not mandated, many merchants cherry-pick the transactions they send via 3DS, sending primarily their highest-risk transactions.

- One of the clear findings of the research is the critical importance of having the vast majority of the card payment ecosystem participating in 3DS. A rising tide carries all boats, and benefits accrue to all participants when there is widespread participation. In those regions such as the EU where there is widespread participation from issuers and merchants alike, net CNP fraud is at a very manageable 7 basis points (bps). Non-3DS net card fraud in Europe is around 12 bps, while net 3DS CNP fraud is around 4 bps. By contrast, net CNP card fraud in the U.S. market averages 17 bps among the issuers and processors interviewed, while net fraud on fully authenticated 3DS transactions averages 63 bps. This underscores the importance of creating an ecosystem of full participation by both issuers and merchants not only to more effectively tackle the fraud but also to enable robust data sharing to help improve authorizations and reduce false declines.
- One of the primary drivers for merchants to use 3DS is the desire to improve CNP authorization rates. 3DS is successful in achieving this promise. 3DS transactions see higher authorizations across all noted regions:
  - **North America:** Fifty-three percent of merchants report authorization approval rates of 85% or higher for non-3DS transactions, while 62% of merchants see authorization approval rates of 85% or higher for transactions that ride the 3DS rails.
  - **Europe:** Forty-one percent of European merchants report authorization rates of 85% or greater for non-3DS transactions, while 77% of merchants see 3DS transactions with authorization rates of 85% or more.
  - **Asia-Pacific:** Forty-five percent of merchants in Australia, India, and Japan see authorization rates of 85% or greater for non-3DS transactions, while 66% of merchants see authorization rates of 85% or more for 3DS transactions.

INTRODUCTION

CNP transaction volume has been steadily growing at double-digit rates for years, as an increasingly digital-first customer base gravitates toward online and mobile channels. The global COVID-19 pandemic only accelerated this trend, with CNP transaction volume increasing 25% to 30% from 2019 to 2020 as a result of the pandemic.

Good customers are not the only ones who have recognized the ease and convenience of digital channels. Even prior to the pandemic, fraudsters focused heavily on CNP transactions as an easy avenue for fraud attacks. As the global card payment ecosystem evolved to protect card-present payment transactions with chip cards, CNP transactions have seen a significant increase in fraud attacks.

As a result, merchants, issuers, payments networks, and governments across the globe are looking for ways to stem the rising tide of CNP fraud. A key tool in their arsenals is 3DS. While 3DS version 1 (3DS1) had a rough initial launch in the early 2000s, the subsequent improvements and iterations have resulted in this protocol becoming the cornerstone of CNP risk mitigation for issuers and merchants around the globe.

This Impact Report delves deeply into large issuers' and merchants' strategies with regard to 3DS and CNP fraud, and examines the successes as well as the opportunities for future improvement and evolution.

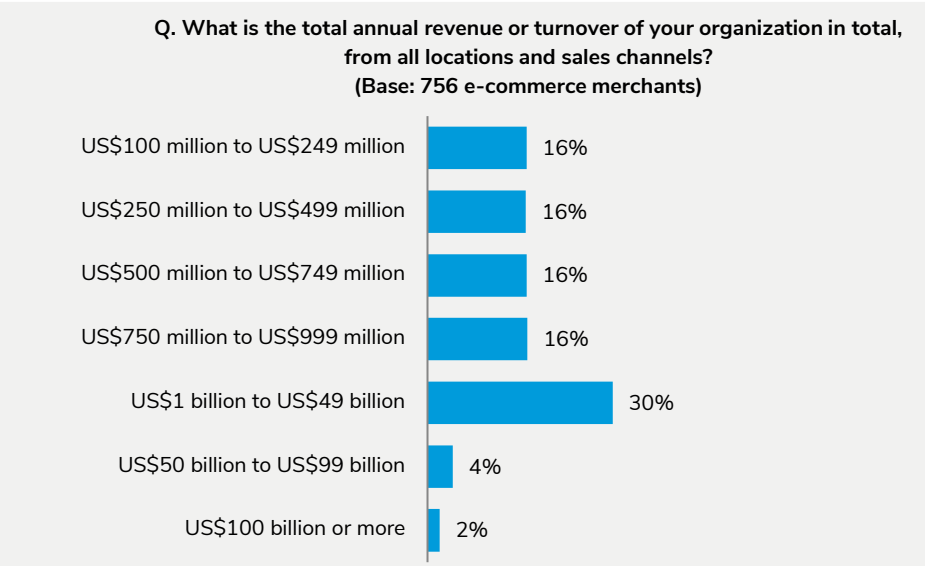
METHODOLOGY

For this research, sponsored by Outseer, an RSA company, Aite-Novarica Group interviewed 34 large issuers and issuing processors in North America, Europe, and the Asia-Pacific, and deployed a quantitative survey of 756 executives responsible for e-commerce payments or loss prevention strategies at midsize and large e-commerce merchants. The quantitative survey was conducted in the same geographic regions during Q2 and Q3 2021. The geographic distribution and interview composition on the issuing side is as follows:

- **North America:** Eleven issuers and two issuing processors in the U.S. and Canada
- **Europe:** Twelve issuers and three issuing processors in the U.K., Italy, Turkey, France, Spain, and Germany
- **Asia-Pacific:** Six issuers in Australia, India, and Japan

The merchant survey population was equally distributed across the three geographic regions. The size of merchants by annual turnover is shown in Figure 1, and the categories of goods that these merchants sell are shown in Figure 2. The data for the full merchant sample has a margin of error of 4 points at the 95% level of confidence; statistical tests of significance were conducted at the 95% level of confidence.

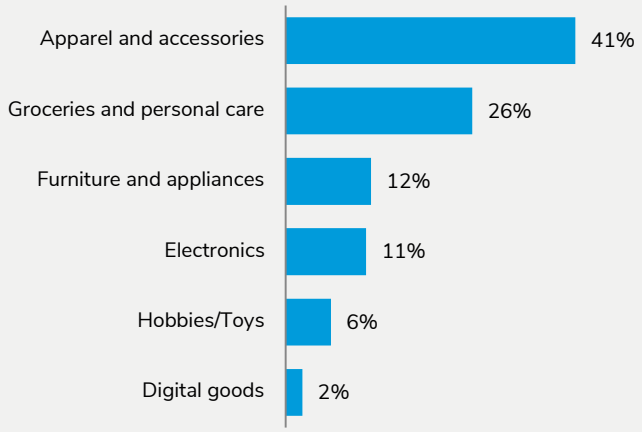
FIGURE 1: ANNUAL TURNOVER OF PARTICIPATING MERCHANTS



Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q3 2021

FIGURE 2: CATEGORY OF GOODS SOLD BY PARTICIPATING MERCHANTS

Q. What is the primary type or types of products your company sells through e-commerce?
(Base: 718 e-commerce merchants)

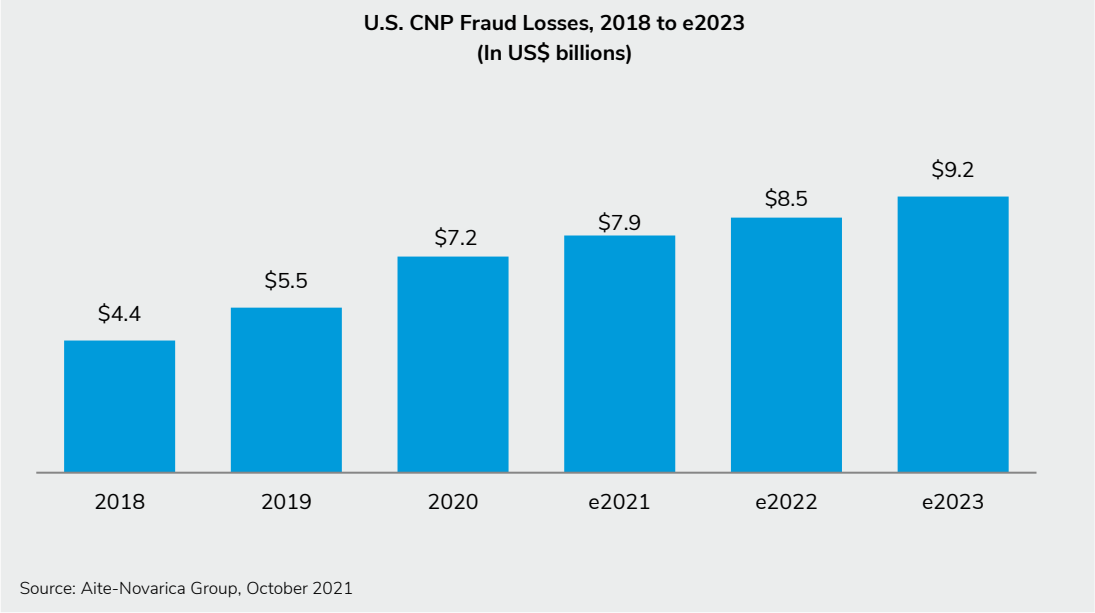


Source: Aite-Novarica Group survey of 756 midsize and large ecommerce merchants, Q3 2021

CNP FRAUD: RAPIDLY RISING

CNP fraud has long been a pain point for merchants and financial institutions (FIs). Organized crime rings use breached data to perpetrate a variety of attacks, often assisted by sophisticated automation tools that facilitate speed and scale. Opportunistic fraudsters are also active with friendly fraud, which has also been steadily rising for years. In the U.S., the result has been a steady rise in CNP fraud losses, which now represent the vast majority of card fraud in the U.S. Aite-Novarica Group estimates U.S. CNP fraud losses will total a whopping US$7.9 billion by the end of 2021 (Figure 3).

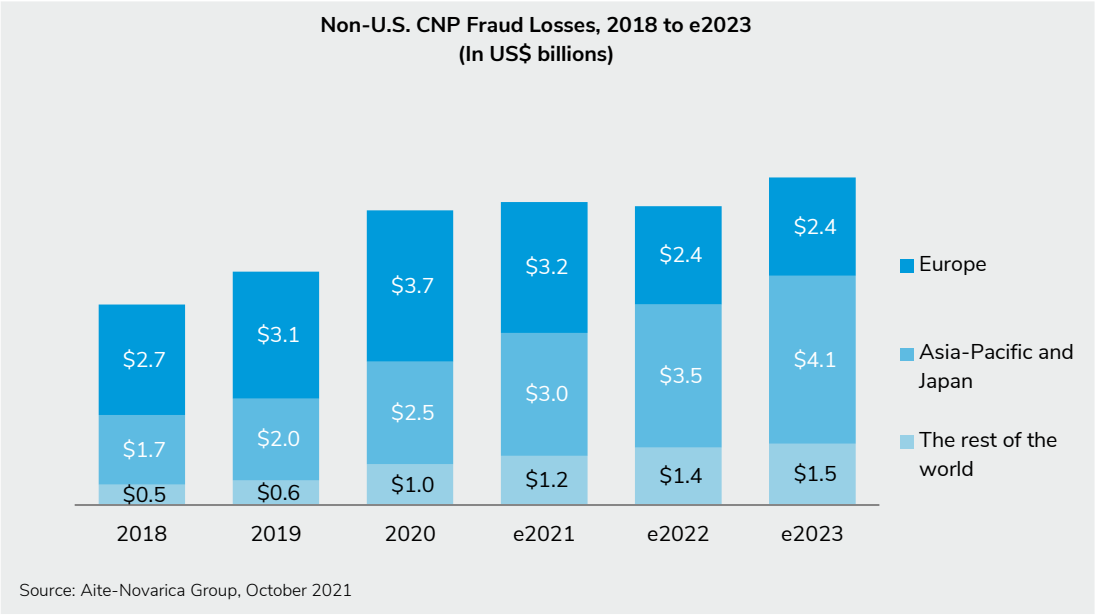
FIGURE 3: U.S. CNP FRAUD LOSSES, 2018 TO E2023



Source: Aite-Novarica Group, October 2021

Not every geography is seeing the same steady rise of CNP fraud as the U.S., however. In regions like the EU, India, and Australia, where either governmental or payment network mandates for MFA are in effect, the stronger security has been a very effective deterrent to fraud. As shown in Figure 4, the widespread requirement for SCA in the EU is already showing its ability to deter CNP fraud. Just as when countries across the globe upgraded to EMV and the fraud attacks migrated to those countries in which chip cards had not yet been deployed, fraudsters will follow a similar pattern in the CNP environment.

FIGURE 4: NON-U.S. CNP FRAUD LOSSES, 2018 TO E2023



Source: Aite-Novarica Group, October 2021

THE CNP CONTROL FRAMEWORK

The layered approach to fraud mitigation has long been a best practice, and CNP fraud is no exception. There is no silver bullet when it comes to fighting fraud, and issuers and merchants use a variety of tools.

Issuers

Issuers are at a bit of a disadvantage when it comes to combating CNP fraud, since they get very little in the way of contextual data coming through the authorization message. Many of the issuers interviewed use some combination of scoring models provided by their authorization system, homegrown fraud models, rules, and scores provided by the payment networks to detect anomalous activity. Their primary method of detecting CNP fraud is whether the transaction is in pattern or out of pattern with prior spending behaviors.

The beauty and the promise of 3DS2 is that it gives issuers much more to work with, within the contextual data set, to the extent that merchants send the data. With the enhanced data that gives context regarding the device attributes, the longevity of the merchant's relationship with the client, the email address of the user, and the type of

goods/services purchased, issuers have the opportunity to make a much more informed decision about both authentication and authorization.

Merchants

Merchants have much more data at their disposal when risk-assessing CNP transactions, given they have the vast amount of digital metadata available as well as internal knowledge of their history (or lack thereof) with the customer. Device fingerprinting, email tenure and reputation, behavioral analytics, and internal hot files represent the first steps in customer risk assessment for many merchants, although some merchants in geographies where 3DS is mandated have found that they can pare back some of these tools and rely more heavily on 3DS.

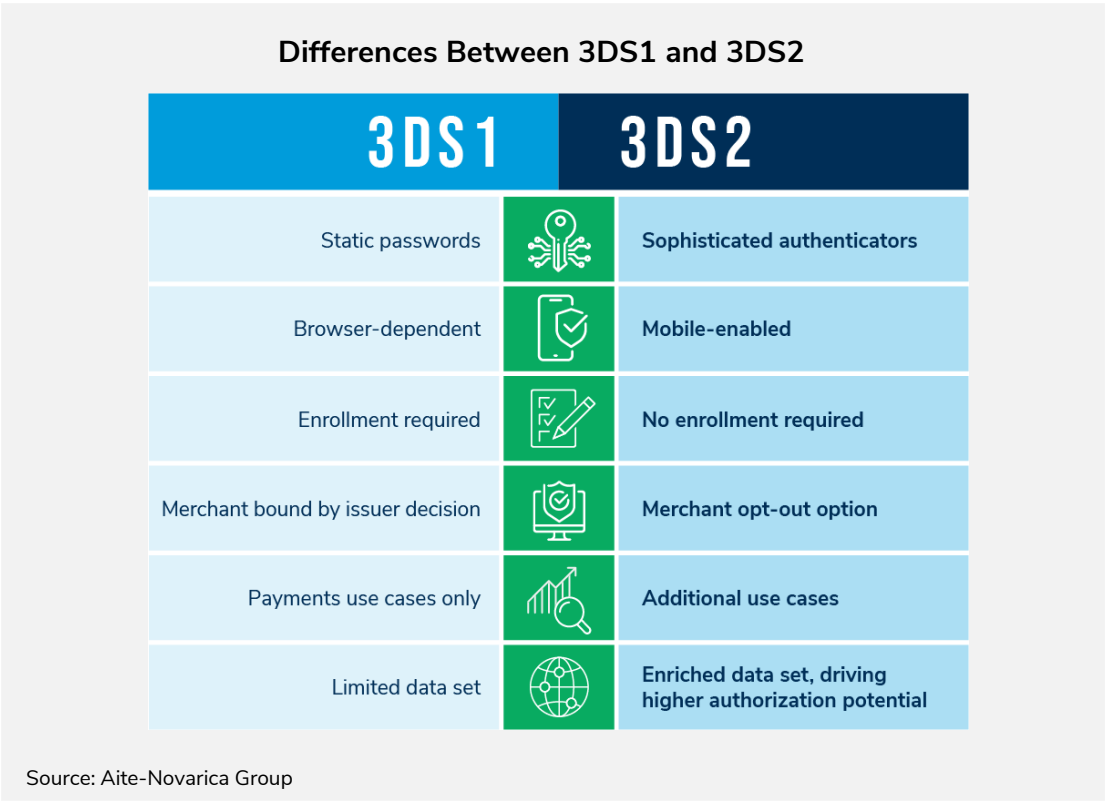
3-D SECURE: A PRIMER

3DS is a protocol that enables issuers to perform additional risk assessment at the time of an e-commerce transaction and prompt the customer for additional authentication if the transaction appears risky. 3DS is a common communication protocol across the card networks, which have separately branded programs and rules structures—for example, Visa Secure (formerly known as Verified by Visa), Mastercard Identity Check (formerly known as SecureCode), American Express SafeKey, Discover ProtectBuy, and JCB J/Secure.[1]

In its initial incarnation in the early 2000s, 3DS was viewed by many merchants and issuers as an obstacle to sales rather than as a fraud prevention solution due to its user experience. Over time, the card networks and enabling vendors made substantial changes to improve the user experience, which in 2016 culminated in the development of a new and enhanced specification, 3-D Secure 2 (also known as EMV 3-D Secure or 3DS2). The key differences between 3DS1 and 3DS2 are summarized in Figure 5.

1. The name 3DS refers to the three domains that add the additional layer of data transfer and security, including the acquirer/merchant domain, the issuer domain, and the interoperability domain, which facilitates the communication.

FIGURE 5: DIFFERENCES BETWEEN 3DS1 AND 3DS2



Source: Aite-Novarica Group

3DS2 contains the following enhancements:

- **Sophisticated authenticators:** Not only are static passwords ineffective and often compromised, but they're also not particularly user-friendly. This can lead to high rates of transaction abandonment and loss of revenue. 3DS2 moves the protocol from static passwords to more robust authenticators, such as biometrics and one-time passwords (OTPs).
- **Mobile-enabled:** The smartphone had not yet been invented when the first version of 3DS was released, so the original protocol was entirely browser-based. 3DS2 is capable of seamlessly integrating with mobile apps as well as browser-based environments.
- **No enrollment required:** 3DS2 eliminates the requirement for consumers to actively enroll. Many of the vendors' risk-based authentication access control server solutions had already introduced this enhancement, so it was available to many issuers on 3DS1. But going forward, it has been formalized within the protocol.

- **Merchant opt-out option:** Many merchants would like the ability to turn on 3DS in nonchallenge mode so they can feed those results into their own risk models and use that to inform their own approve/decline decisions (understanding that they wouldn't benefit from the liability shift). 3DS2 provides this ability.
- **Additional use cases:** While 3DS1 was designed around the payment transaction, 3DS2 supports additional use cases, such as account updates, verification, and token provisioning.
- **Enriched data set:** The 3DS1 protocol supported the transfer of 15 data elements. The 3DS2 data set has significantly expanded, with more than 150 data elements—some of which are required while others are optional or conditional. The enriched data set has the potential to provide a significant performance boost. The current CNP decisioning environment for issuers and merchants is akin to two people dividing a box of puzzle pieces and separately trying to put together the puzzle. Merchants have valuable data about the customer's behavior but currently have no way to share those insights to help inform the issuer's authorization and authentication decisions. 3DS2 provides the mechanism for merchants to share this data with issuers in order to reduce false declines and increase authorization rates, while also better detecting fraud and ensuring friction is minimized in order to maintain a positive customer experience.

Regulatory Compliance

In response to rising fraud, many countries either have already mandated or are in the process of mandating MFA for CNP transactions. 3DS2 provides compliance with the majority of these mandates, as described in Table A.

TABLE A: MFA MANDATES

COUNTRY/ REGION	MANDATING ENTITIES	DESCRIPTION
Global	Visa and Mastercard	Effective October 16, 2021, Visa will continue to support 3DS 1.0.2 transaction processing, including the 3DS 1.0.2 Directory Server (DS), but will stop support of 3DS 1.0.2 Attempts Server for nonparticipating issuers. If an issuer continues to support 3DS 1.0.2 after October 15, 2021, it will be able to respond to merchants with a fully authenticated response and Cardholder Authentication Verification Value, and merchants will obtain fraud liability protection. These transactions will be blocked from fraud-related disputes in Visa Resolve Online. Issuers wishing to stop support of 3DS 1.0.2 must request that their bank identification number (BIN) ranges be removed from the Visa Secure DS.[2] Effective October 15, 2022, Visa and Mastercard will discontinue support for 3DS 1.0.2 altogether.
Australia	Visa	Merchants must process an e-commerce transaction using Visa Secure if it is assigned any of the following merchant category codes (MCCs): 4722 (travel agencies and tour operators), 4816 (computer network/ information services), 4829 (wire transfer money orders), 5085 (industrial supplies), 5311 (department stores), 5399 (miscellaneous general merchandise), 5411 (grocery stores and supermarkets), 5661 (shoe stores), 5691 (men's and women's clothing stores), 5699 (miscellaneous apparel and accessory shops), 5722 (household appliance stores), 5732 (electronics stores), 5733 (music stores—musical instruments, pianos, and sheet music), 5734 (computer software stores), 5912 (drug stores and pharmacies), 5943 (stationery stores, office and school supply stores), 5944 (jewelry stores, watches, clocks, and silverware stores), 5999 (miscellaneous and specialty retail stores), 6211 (security brokers/dealers), 7011 (lodging—hotels, motels, resorts, central reservation services), 7832 (motion picture theaters), 7995 (betting, including lottery tickets, casino gaming chips, off-track betting, and wagers at race tracks), 8999 (professional services), or 9402 (postal services—government only).

[2] "Visa Business News," Visa, February 4, 2021, accessed October 5, 2021, https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-will-discontinue-support-of-3d-secure.pdf.

COUNTRY/ REGION	MANDATING ENTITIES	DESCRIPTION
		If a merchant is not enrolled in Visa Secure and is identified by the Visa Fraud Monitoring Program, it will be subject to the high-risk MCC timeline, as outlined in the Visa Fraud Monitoring Program.
	Mastercard	All transactions over US$200 require 3DS.
Bangladesh	Mastercard	All acquirers and merchants must support 3DS 2.0.
Brazil	Visa	Issuers must ensure that debit and electronic BINs participate in Visa Secure.
Canada	Visa and Mastercard	Issuers must ensure that Visa debit category cards participate in Visa Secure.
China	Visa	Issuers' Visa Secure program must use dynamic authentication.
Europe	European Commission	The second Payment Services Directive (PSD2) mandates SCA to be implemented for electronic transactions. Payment service providers, which include banks, e-money providers, and payment institutions, must apply SCA for all electronic payments initiated by the payer (such as card payments and credit transfers) unless the payment qualifies as low risk and falls within a set of specified exemptions.
	Mastercard	3DS is required for all online gaming transactions. On a staggered basis (timelines coinciding with the PSD2 regulatory technical standard effective dates), Mastercard will require European issuers, acquirers, and merchants to support 3DS 2.0 on e-commerce transactions. In select markets, issuers will also be required to enable biometric authentication on mobile devices that support the technology.
	Visa	Issuers that submit secure e-commerce transactions must support Visa Secure. Acquirers must ensure that all high brand-risk merchants and high brand-risk sponsored merchants process e-commerce transactions using a Visa-approved payment authentication method.

COUNTRY/ REGION	MANDATING ENTITIES	DESCRIPTION
India	Reserve Bank of India	Dual-factor authentication is required for all card transactions above 2,000 rupees.[3] The latter threshold was introduced recently to reduce payment friction and respond to the needs of e-commerce firms, online ticket booking companies, and taxi-hailing apps.
	Mastercard	All acquirers and merchants must support 3DS 2.0.
Japan	Japan Online Game Association	All association members are required to implement 3-D Secure.
Malaysia	Mastercard	All acquirers and merchants must support 3DS 2.0.
	Visa	E-commerce merchants must use 3-D Secure 2.0,1 if it is assigned any of the following MCCs: 4511 (Airlines and Air Carriers), 5977 (cosmetic stores), 5999 (miscellaneous and specialty retail stores), or 7011 (lodging—hotels, motels, resorts, central reservation services).
New Zealand	Visa	All Visa credit, debit, and reloadable prepaid cards must be enrolled in Visa Secure. Virtual accounts associated with Visa commercial cards are excluded from this requirement. A merchant must support Visa Secure if the merchant's fraudulent Visa e-commerce transaction volume is US$25,000 or higher and exceeds 0.25% of the merchant's overall e-commerce transaction volume, or if the merchant's fraudulent Visa e-commerce transaction volume is US$250,000 or higher and exceeds 0.025% of the merchant's overall e-commerce transaction volume. In addition, e-commerce merchants must use Visa Secure or an equivalent Visa-approved authentication method if the merchant exceeds US$10,000 in Visa transaction volume in any quarter or is assigned one of the following MCCs: 4814 (telecommunication services), 5499 (miscellaneous food stores,

3. "Card Not Present Transactions—Relaxation in Additional Factor of Authentication for Payments up to ₹ 2000/- for Card Network Provided Authentication Solutions," Reserve Bank of India, December 6, 2016, accessed October 17, 2017, https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=10766.

COUNTRY/ REGION	MANDATING ENTITIES	DESCRIPTION
		convenience stores, and specialty markets), 5732 (electronics stores), 5734 (computer software stores), 5941 (sporting goods stores), 5944 (jewelry stores and watches, clocks, and silverware stores), 5947 (gift, card, novelty, and souvenir shops), 6300 (insurance sales, underwriting, and premiums), 7399 (business service not elsewhere classified), or 9399 (government services not elsewhere classified).
	Mastercard	All transactions over US$200 require 3DS.
Nigeria	Visa	Nigerian issuers must ensure each cardholder is enrolled in Visa Secure and only authorize domestic e-commerce transactions for which the acquirer has requested Visa Secure authentication, except for transactions processed under the International Airline Program.
	Mastercard	All acquirers and merchants must support 3DS 2.0.
Singapore	Monetary Authority of Singapore	All online transactions must be authenticated via a dynamic OTP via 3DS.
	Visa	An e-commerce merchant must process an e-commerce transaction using Visa Secure with 3-D Secure 2.0,1 if it is assigned any of the following MCCs: 4511 (airlines and air carriers), 4722 (travel agencies and tour operators), 5815 (digital goods media—books, movies, music), 5816 (digital goods—games), 5817 (digital goods—applications), 5818 (digital goods—large digital goods merchant), 5968 (direct marketing—continuity/subscription merchant), or 8999 (professional services).
South Africa	Payment Association of South Africa	All issuers and e-commerce merchants must support 3DS.
	Mastercard	All acquirers and merchants must support 3DS 2.0.

COUNTRY/ REGION	MANDATING ENTITIES	DESCRIPTION
South Korea	Financial Supervisory Service	MFA is required for e-commerce transactions.
	Visa	Ensure that its Electronic Commerce Merchant processes an Electronic Commerce Transaction using Visa Secure with 3-D Secure 2.0,1 if it is assigned either of the following MCCs: I MCC 5968 (direct marketing—continuity/subscription merchant) or I MCC 5999 (miscellaneous and specialty retail stores).
Taiwan	Taiwanese government	A government directive set forth a recommendation for 3DS adoption that has been interpreted as a mandate by Taiwanese banks.
	Visa	An e-commerce merchant must process e-commerce transactions using Visa Secure with 3-D Secure 2.0,1 if it is assigned any of the following MCCs: 4112 (passenger railways), 4722 (travel agencies and tour operators), or 7372 (computer programming, data processing, and integrated systems design services).

Source: Aite-Novarica Group, Visa, Mastercard

Table B summarizes the key market trends and their implications relative to the evolution of 3DS in the global market.

TABLE B: MARKET TRENDS AND IMPLICATIONS

MARKET TRENDS	MARKET IMPLICATIONS
CNP transaction volume is rapidly rising.	Migration from in-person to digital interactions will only continue to accelerate. This transition is particularly notable in geographies such as Latin America and the Asia-Pacific, where many consumers were thrust into the digital channels by the pandemic.

MARKET TRENDS	MARKET IMPLICATIONS
Fraudsters follow the money, and CNP fraud is also on the rise.	There is little in the way of deterrent for organized crime rings to perpetrate fraud, and the industry has seen an industrialization of fraudsters' enabling infrastructure over the past decade, fueled by data breaches and sophisticated, automated attack methods.
Regulators in many jurisdictions are recognizing the risk and requiring more stringent controls.	Mandates for MFA for CNP transactions are becoming more prolific. All eyes are on the EU, which is the largest card market to enact such a mandate to date. If the results show this to be effective, then many other countries are likely to follow suit.
Merchants are still wary of potential attrition associated with inserting authentication into the transaction flow.	In regions without mandates for MFA for CNP transactions, the ability to demonstrate higher authorization rates for CNP transactions will be an important way to encourage merchants to use 3DS to a greater degree.

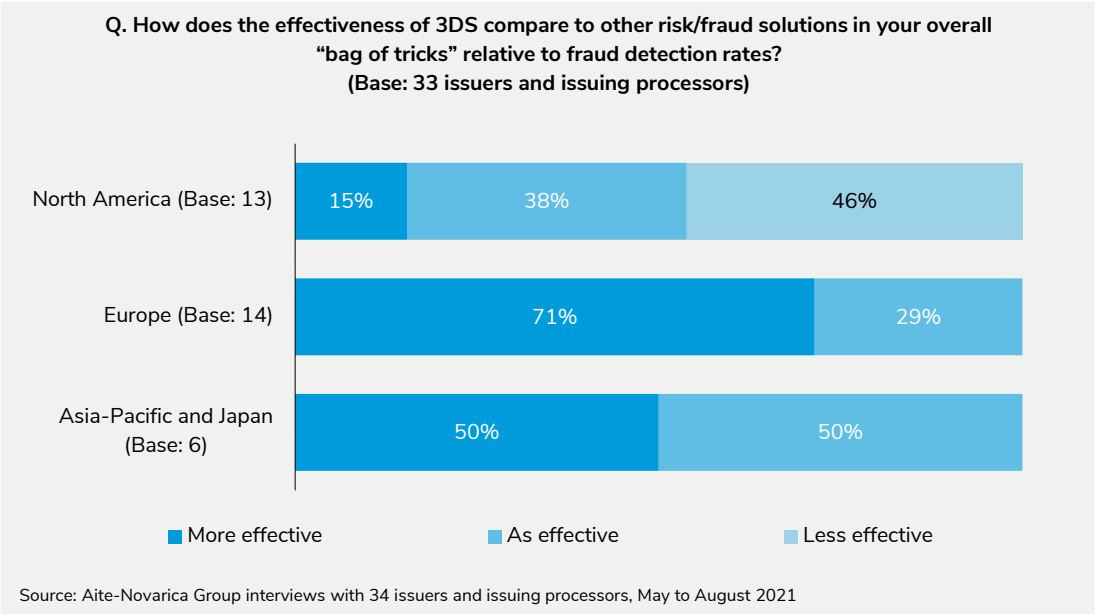
Source: Aite-Novarica Group

3DS: ISSUER PERSPECTIVES

Since the 3-D Secure is successful only when both issuers and merchants can support the protocol concurrently, the good news is that 100% of the issuers interviewed for this research will have the ability to support 3DS2 in 2021. Thirty-two of the issuers and processors were already fully enabled, while two were in the final stages of testing and moving 3DS2 into production. Among the issuing processors surveyed, more than half of their issuing bank clients have also upgraded to 3DS2, although a number are still in the process of enabling 3DS2.

Overall, 82% of issuers and processors interviewed said that 3DS is as effective or more effective for fraud detection when compared to other fraud solutions. Issuers' perspectives regarding the effectiveness of 3DS relative to other CNP fraud mitigation techniques vary widely based on geography. In Europe and parts of the Asia-Pacific where MFA for CNP transactions is mandated, 100% of issuers view 3DS as effective or highly effective. In North America, where strong CNP authentication controls are not mandated, the effectiveness is not viewed as favorably (Figure 6). The disparity largely lies in the fact that in countries where MFA for CNP transactions is not mandated, many merchants cherry-pick the transactions that they send via 3DS, sending primarily their highest-risk transactions. In countries where merchants send the majority of their CNP volume, issuers are able to make more informed authentication and authorization decisions.

FIGURE 6: EFFECTIVENESS OF 3DS RELATIVE TO OTHER CNP FRAUD SOLUTIONS

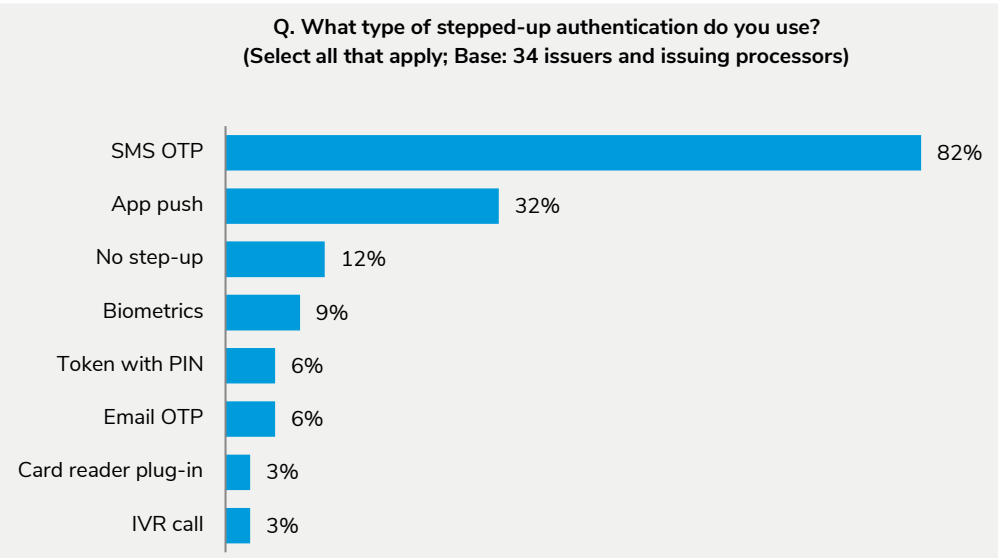


Source: Aite-Novarica Group interviews with 34 issuers and issuing processors, May to August 2021

The approach to authentication methods differed somewhat by geography. Overall, SMS OTP is the most ubiquitous authenticator and the primary mechanism for issuers in the U.S. By contrast, most of the issuers in Europe use mobile app push as their primary authentication mechanism, with SMS OTP as a backup for those consumers who don't have their FI's mobile app. A handful of issuers also include other options, such as biometrics, a card-reader plug-in, or a token (Figure 7). In the U.K., a number of issuers plan to embark on a strategy that combines SMS OTP with behavioral biometrics. The U.K. Information Commissioner's Office has set forth that behavioral biometrics can be used without asking for explicit consent from the customer, which is very attractive in terms of removing points of friction.

While many of the issuers in the U.S. expressed the desire to move to a more secure means of authentication, given the vulnerability of SMS OTP to compromise and social engineering, none of these issuers has yet been able to get its business case to add additional authentication mechanisms funded.

FIGURE 7: STEPPED-UP AUTHENTICATION CAPABILITIES



Source: Aite-Novarica Group interviews with 34 issuers and issuing processors, May to August 2021

UNIVERSAL ADOPTION IS A CRITICAL FACTOR

One of the clear findings of the research is the critical importance of having the vast majority of the card payment ecosystem participating in 3DS. A rising tide carries all boats, and benefits accrue to all participants when there is widespread participation. In those regions such as the EU where there is widespread participation from issuers and merchants alike, net CNP fraud is at a very manageable 7 bps.[4] Non-3DS net card fraud in Europe is around 12 bps, while net 3DS CNP fraud is around 4 bps (Table C).

By contrast, net CNP card fraud in the U.S. market averages 17 bps among the issuers and processors interviewed, while net fraud on fully authenticated 3DS transactions averages 63 bps. The higher rate of overall CNP fraud is due to the fact that a very small proportion of total CNP transactions are sent along the 3DS protocol in nonregulated markets (2% to 5%, as shown in Table D). And the high rate of fraud on 3DS transactions in nonregulated markets is attributable to the fact that many merchants cherry-pick and send only the highest-risk transactions via 3DS. These transactions are often higher dollar value as well, which also augments the fraud rate. A number of the issuers interviewed also see a high rate of first-party fraud that adds to their 3DS fraud rate. One large U.S. issuer has performed forensic analysis into its 3DS losses and found

[4] A basis point is the common unit of measurement for card fraud, equivalent of.01%.

that 70% of its cryptocurrency disputes from 3DS transactions are first-party fraud (buyer's remorse).

TABLE C: CNP FRAUD RATES BY REGION

REGION	OVERALL NET CNP FRAUD (BPS)	NET NON-3DS CNP FRAUD (BPS)	NET 3DS CNP FRAUD (BPS)
U.S.	8 to 35	8 to 35	13 to 175
Canada	1 to 2	1 to 2	40 to 50
Europe	7	12	4

Source: Aite-Novarica Group interviews with executives at 34 issuers and processors, May to August 2021

TABLE D: PERCENTAGE OF CNP PROTECTED BY 3DS BY COUNTRY

COUNTRY	PERCENTAGE OF CNP PROTECTED BY 3DS
U.S.	2%
Canada	5%
France	70%
Germany	90%
Italy	20%
Spain	80%
Turkey	70%
Australia	80%

COUNTRY	PERCENTAGE OF CNP PROTECTED BY 3DS
India	100%
Japan	2% to 3%

Source: Aite-Novarica Group interviews with 34 issuers and issuing processors, Q2 and Q3 2021

Not only are the fraud rates much lower in regions that see a substantial proportion of their CNP traffic use 3DS, but the abandonment rates when stepped-up authentication is invoked are also lower in many of these countries, since customers become habituated to expect authentication prompts. Table E shows the percentage of transactions in which stepped-up authentication is invoked, by country, as well as the associated abandonment rate. When consumers become accustomed to being prompted for stepped-up authentication, attrition rates are reduced. And some level of abandonment will also be present, since as fraudsters are tripped up by the 3DS authentication prompt, the result will be 3DS having its designed deterrent effect and stopping the fraudulent transaction.

TABLE E: PERCENTAGE OF 3DS TRANSACTIONS INVOKING STEPPED-UP AUTHENTICATION

COUNTRY	PERCENTAGE OF 3DS TRANSACTIONS WITH STEPPED-UP AUTHENTICATION, AS REPORTED BY ISSUERS/PROCESSORS	ABANDONMENT RATES WHEN STEPPED-UP AUTHENTICATION IS INVOKED, AS REPORTED BY ISSUERS/PROCESSORS
U.S.	15% to 75%	10% to 30%
Canada	10% to 12%	Less than 5%
Europe	40% to 82%	5% to 50%
Asia-Pacific Japan	1% to 38%	5% to 30%

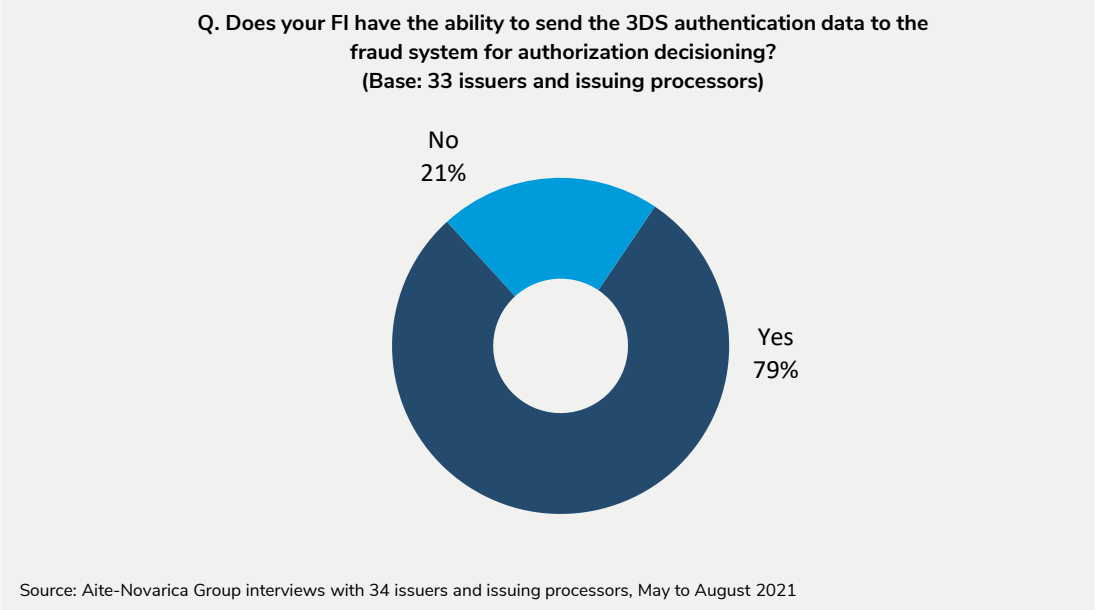
Source: Aite-Novarica Group interviews with executives at 34 issuers and processors, May to August 2021

MOVING THE NEEDLE ON AUTHORIZATION

One of the key areas of promise with the advent of 3DS2 is the ability to reduce CNP false declines by providing enhanced data that can help inform the authorization decision. In the card-present environment, more than 96% of transactions are authorized, while in CNP, authorization rates are only around 85%. The provision of more complete and enriched data to inform the authorization has the potential to reduce the false declines, which are the bane of many e-commerce merchants' existence.

Seventy-nine percent of the issuers and processors today have the ability to send data from their 3DS authentication service to their decisioning engine to help inform the authorization decision (Figure 8).

FIGURE 8: ABILITY TO SEND 3DS AUTHENTICATION DATA/RESULTS TO THE AUTHORIZATION SYSTEM



Source: Aite-Novarica Group interviews with 34 issuers and issuing processors, May to August 2021

That said, many of the issuers indicate that there is still a lot of room for improvement. One of the large issuing processors says that many merchants are still not sending much of the enhanced data set available with 3DS2, and even when they do send that data, the data hygiene is often poor, thus providing little assistance in making a more informed authentication or authorization decision.

3DS: MERCHANT PERSPECTIVES

Merchant fraud executives are challenged to create the optimal control framework to maximize revenue and minimize losses due to fraud and chargebacks. Forty-five percent of merchants surveyed say their company's guiding principal for fraud mitigation is striking that optimal balance between maximum sales and minimum fraud losses. Another 29% of executives surveyed say that their firm's priority with regard to fraud strategy is to minimize friction, maximize sales, and/or minimize false declines. Only one in four of the respondents say fraud mitigation is a key priority, which underscores why the ability to balance risk assessment with friction is so very important in e-commerce (Figure 9).

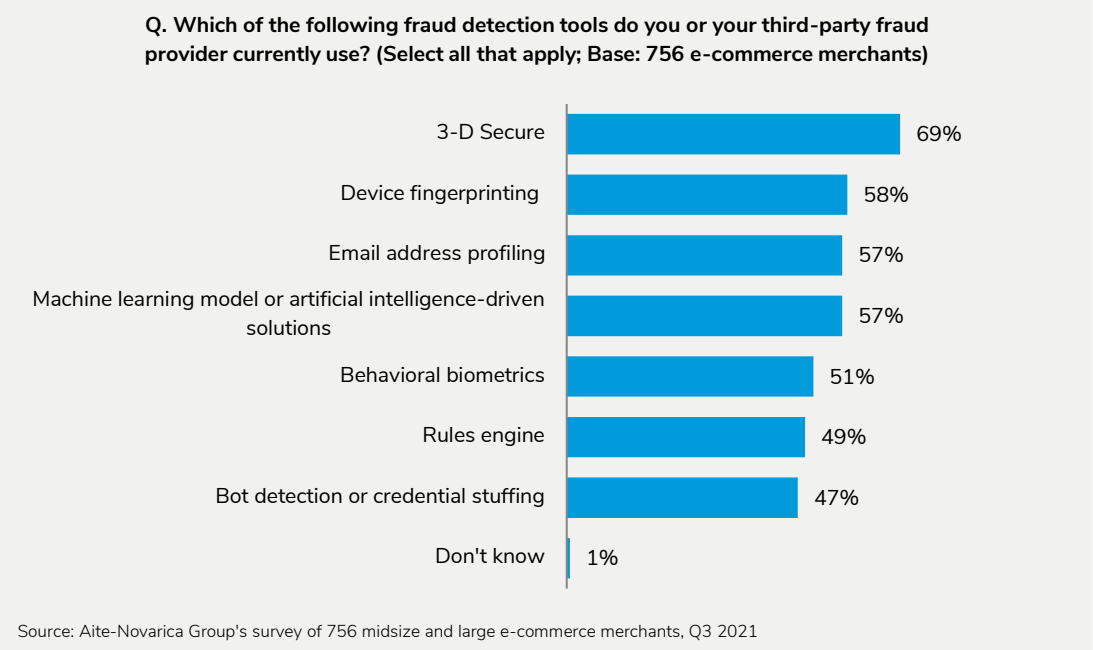
FIGURE 9: MERCHANTS' FRAUD MITIGATION STRATEGIES

Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q3 2021

Among the solutions that merchants employ to mitigate CNP fraud, 3DS leads the pack, with 69% of merchants using 3DS. This is not surprising, given that there are many mandates for MFA for CNP across the globe, and 3DS is the key means of compliance for most issuers and merchants in jurisdictions with mandates (Figure 10). And as shown in the overall CNP fraud rates provided by issuers, 3DS is also very effective at reducing fraud rates. When the data is segmented for countries that have an MFA mandate versus those that do not, 72% of merchants headquartered in regulated

countries enable 3DS, while 65% of merchants headquartered in nonregulated countries do so today.[5]

FIGURE 10: MERCHANTS' CNP FRAUD MITIGATION TOOLS

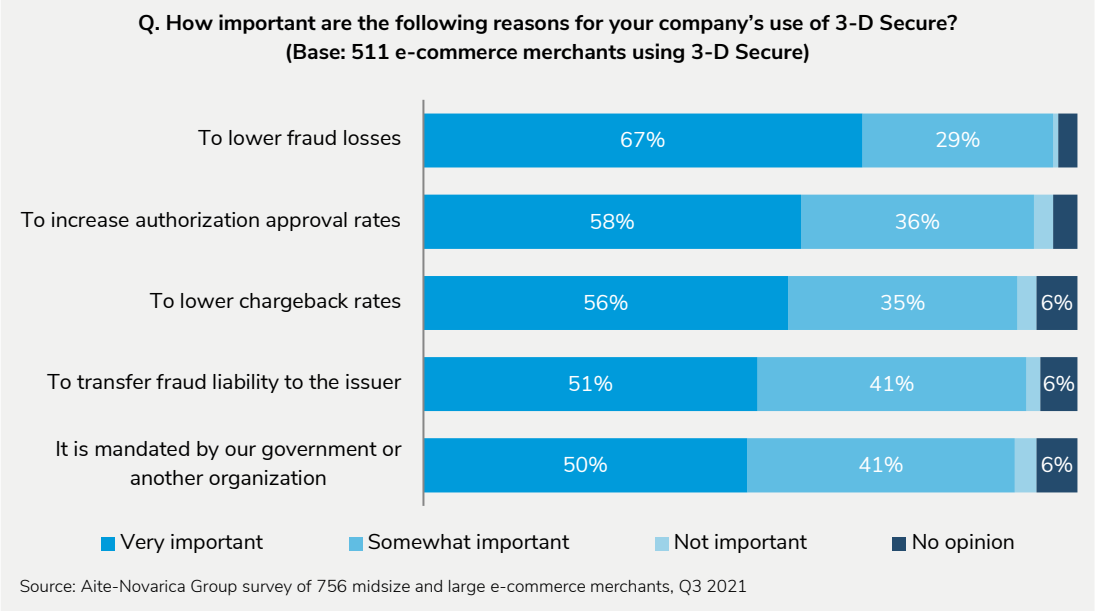


Source: Aite-Novarica Group's survey of 756 midsize and large e-commerce merchants, Q3 2021

When asked about the drivers of 3DS usage, 67% of merchants say lowering fraud losses is a key driver, and 58% say increasing authorization approval rates is very important, while 56% are seeking to lower chargeback rates (Figure 11).

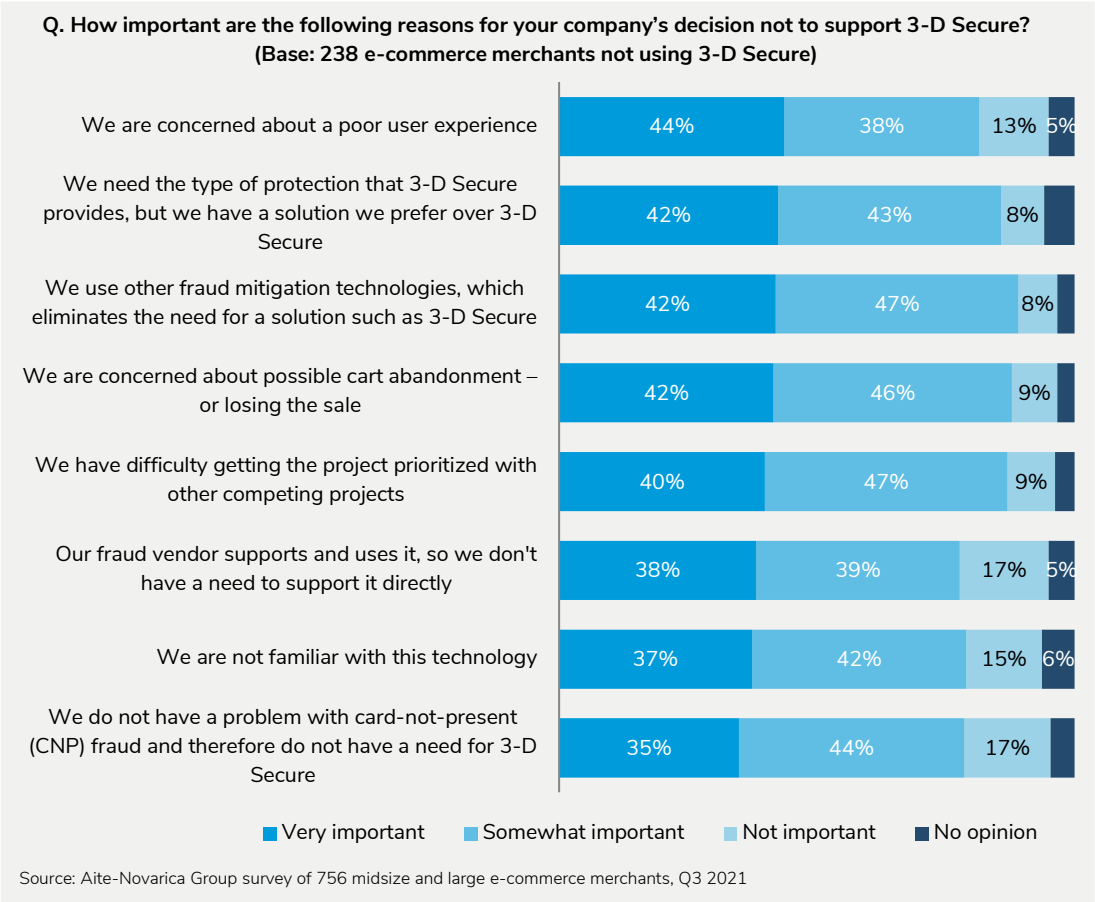
[5] U.K. merchants are included in the "regulated" segmentation, given that there is a pending requirement for SCA, effective March 2022.

FIGURE 11: DRIVERS OF MERCHANT USE OF 3DS



For those merchants not using 3DS, concern over user experience and cart abandonment were among the top reasons, along with the use of alternative risk mitigation technologies (Figure 12). Interestingly, 37% of merchants surveyed say that they are not familiar with 3DS. This education gap is not wholly unusual, especially in highly fragmented markets such as the U.S. In a merchant survey conducted by Aite Group in October 2014, 34% of merchants were unaware of the need to migrate to EMV by October 2015, so effective dissemination of knowledge among the merchant community is by no means a new challenge in card payments.

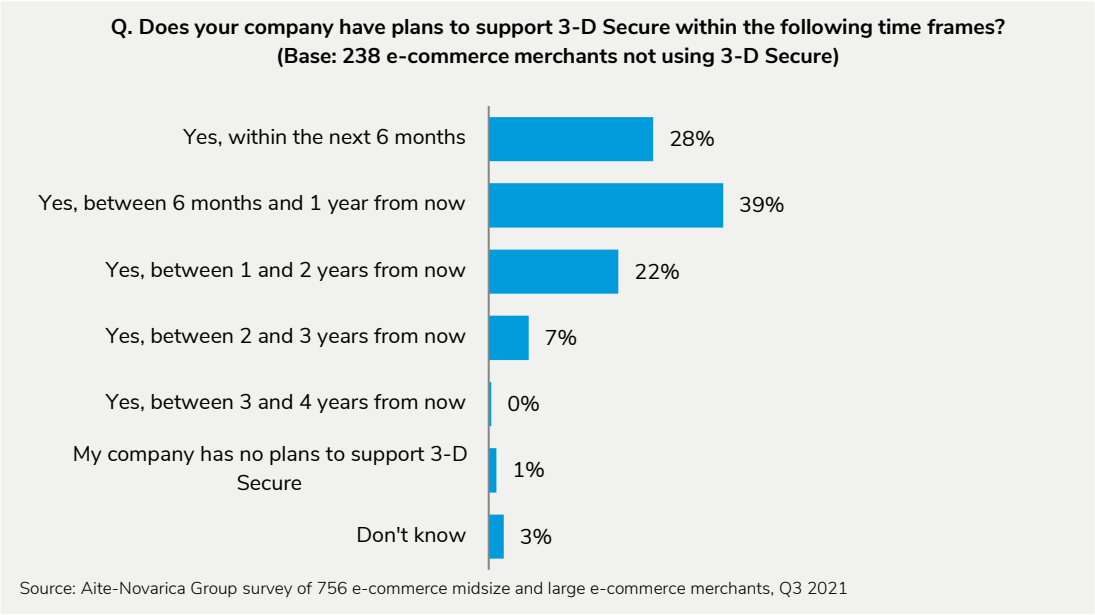
FIGURE 12: REASONS WHY MERCHANTS DO NOT USE 3DS



Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q3 2021

Of the merchants that do not support 3DS today, 67% plan to support it within the next 12 months. The big question for global merchants is the extent to which they decide to extend 3DS into their nonregulated markets (Figure 13). Any merchant with a global presence or aspirations must have 3DS support, since so many countries now have an MFA mandate in place for at least a portion of CNP transactions. To that end, 73% of merchants in unregulated countries that do not currently support 3DS say they intend to do so within the next year.

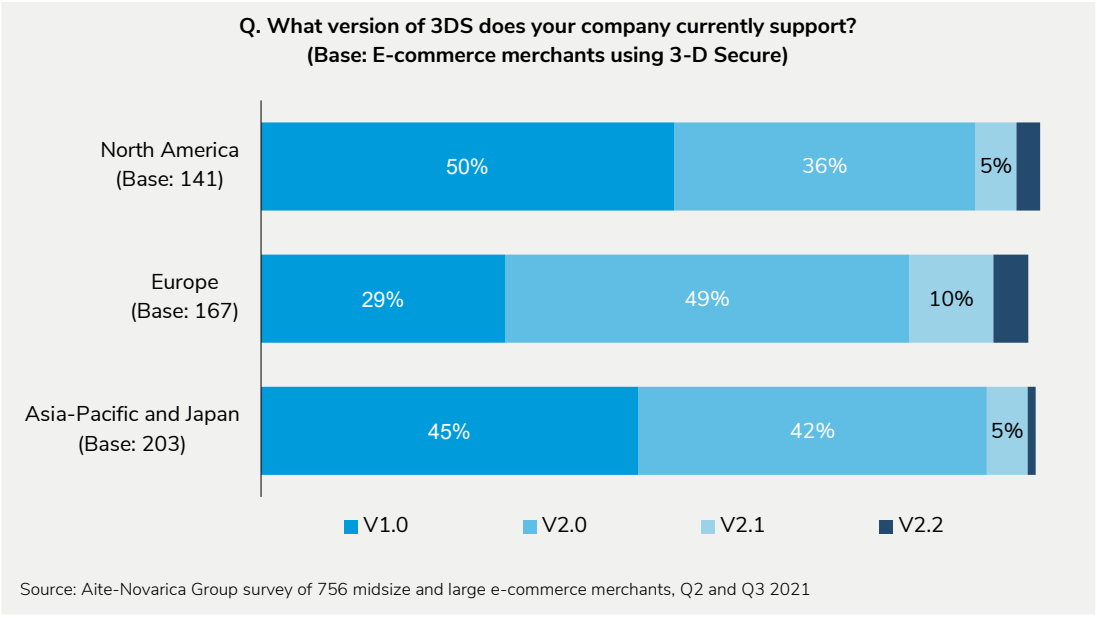
FIGURE 13: PLANNED SUPPORT FOR 3DS AMONG NONPARTICIPATING MERCHANTS



Source: Aite-Novarica Group survey of 756 e-commerce midsize and large e-commerce merchants, Q3 2021

Approximately half of merchants in the Asia-Pacific and North America are still using 3DS1, while far more European merchants have already upgraded to 3DS2; just 29% of European merchants are still on 3DS1 (Figure 14).

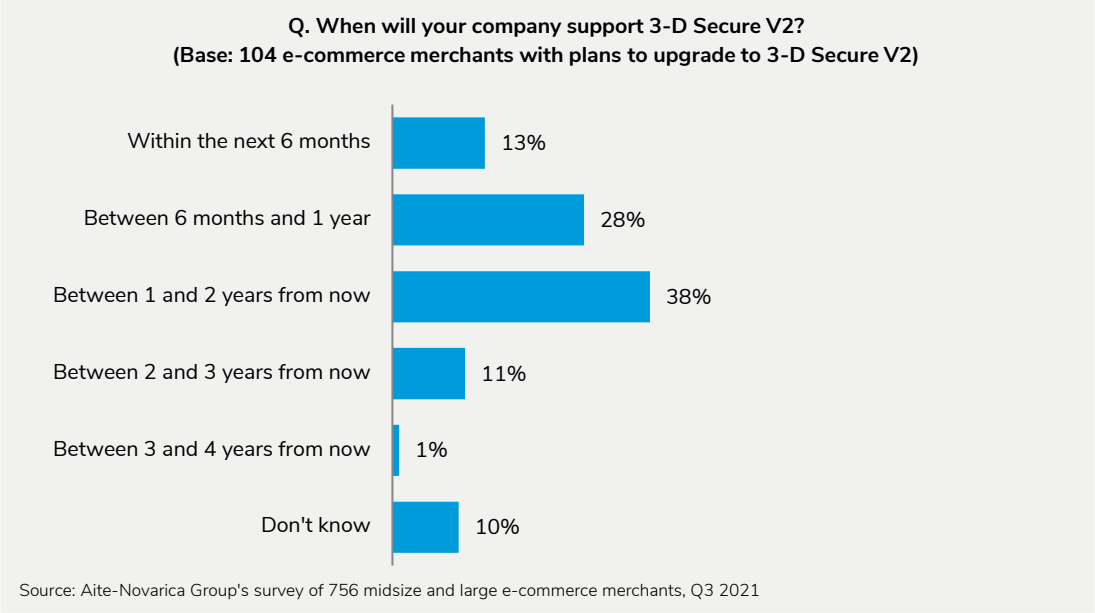
FIGURE 14: VERSION OF 3DS IN USE BY MERCHANTS



Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q2 and Q3 2021

When asked about their planned time frame to support 3DS2, 41% of merchants plan to do so within the next year, and 38% plan to do so within one to two years, while 22% of merchants plan to upgrade in more than two years or don't yet know (Figure 15). This further emphasizes the education gap among the merchant community since payment network support for 3DS1 will be sunset by October 2022.

FIGURE 15: TIMELINE TO SUPPORT 3DS2

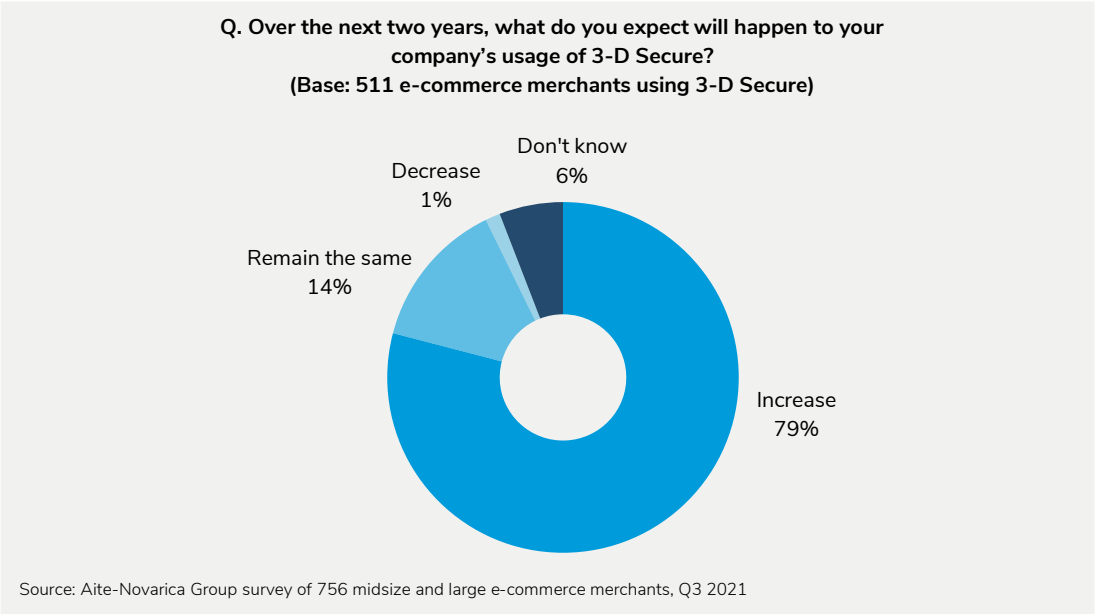


Source: Aite-Novarica Group's survey of 756 midsize and large e-commerce merchants, Q3 2021

INCREASING USE OF 3DS

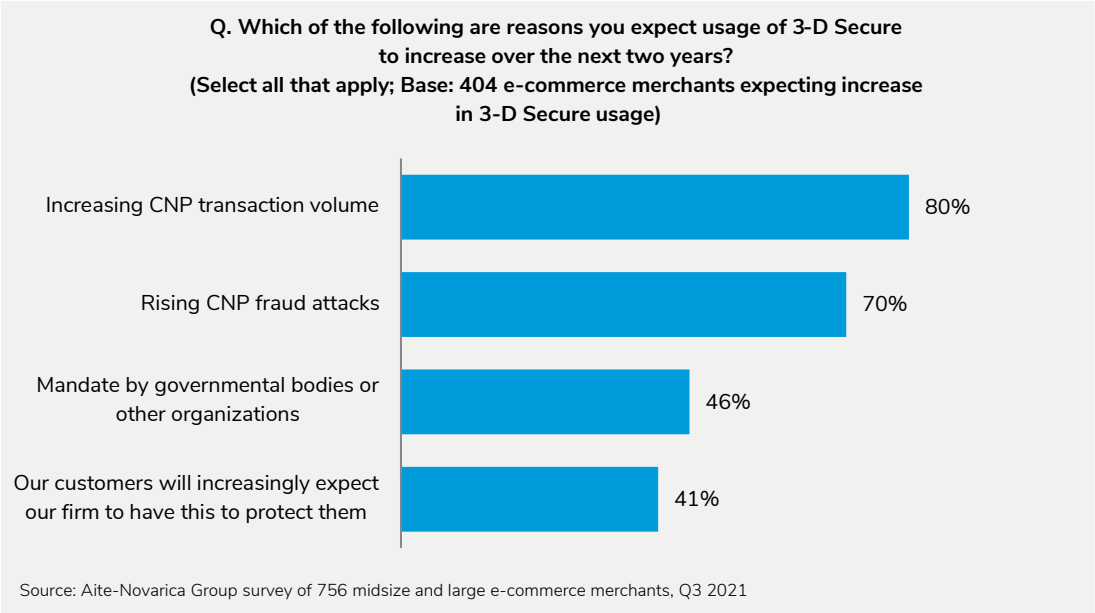
Seventy-nine percent of merchants expect to see their company's use of 3DS increase over the next two years (Figure 16). Primary drivers of the increased usage will be increasing CNP transaction volume and the rising CNP threat landscape (Figure 17).

FIGURE 16: MERCHANTS' PROJECTED USE OF 3DS



Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q3 2021

FIGURE 17: DRIVERS OF INCREASED 3DS USAGE

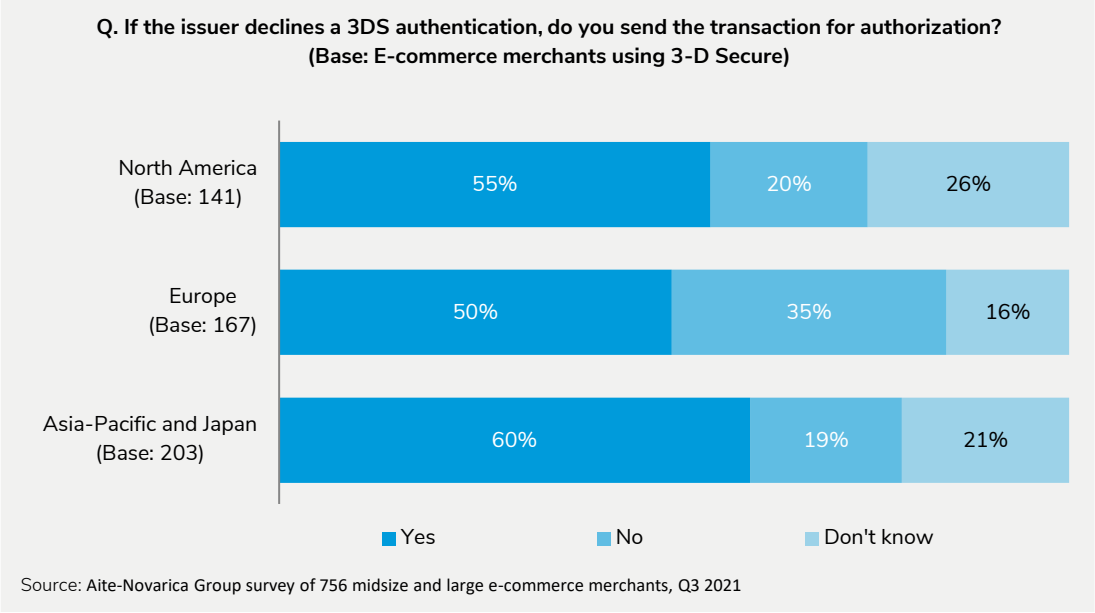


Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q3 2021

IF AT FIRST YOU DON'T SUCCEED...

Many issuers said that they often see merchants submit transactions for authorization even if they have failed 3DS authentication. This practice appears to be widespread, with at least half of merchants in all of the regions saying that they do this (Figure 18).

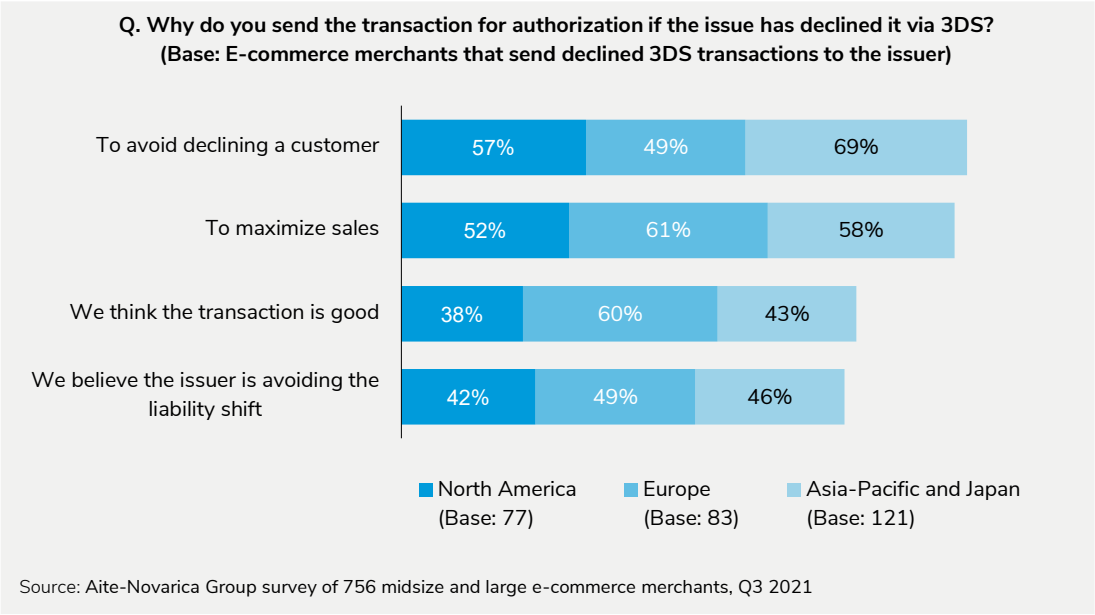
FIGURE 18: SUBMISSION OF 3DS DECLINES FOR AUTHORIZATION



Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q3 2021

When asked about their rationale, 59% of merchants overall surveyed cited their desire to avoid declining the customer, while 57% are trying to maximize sales. These drivers vary somewhat by geography, as shown in Figure 19. Many merchants also believe that the transaction is legitimate and think that the issuer's decline of the original transaction is driven by a desire to avoid the liability shift.

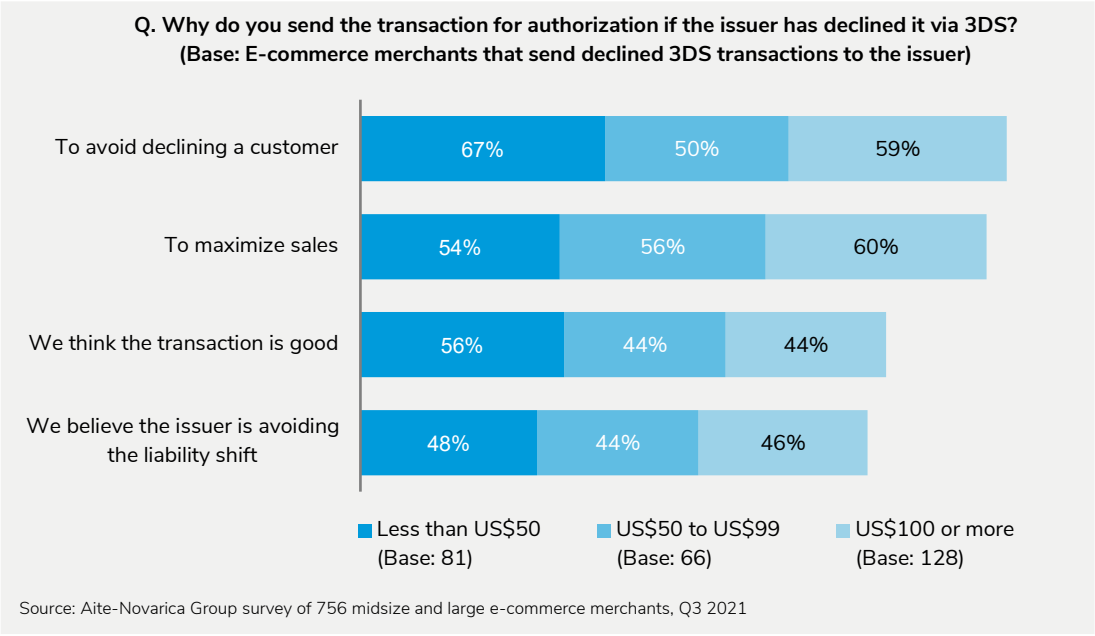
FIGURE 19: REASONS FOR SUBMISSION OF 3DS DECLINES FOR AUTHORIZATION



Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q3 2021

The rationale changes depending on the avg ticket size. Sixty-seven percent of merchants that have smaller average tickets (under US$50) cite interest in their ability to avoid declining a customer, while merchants with higher average tickets are more inclined to send the transactions in order to maximize sales (Figure 20).

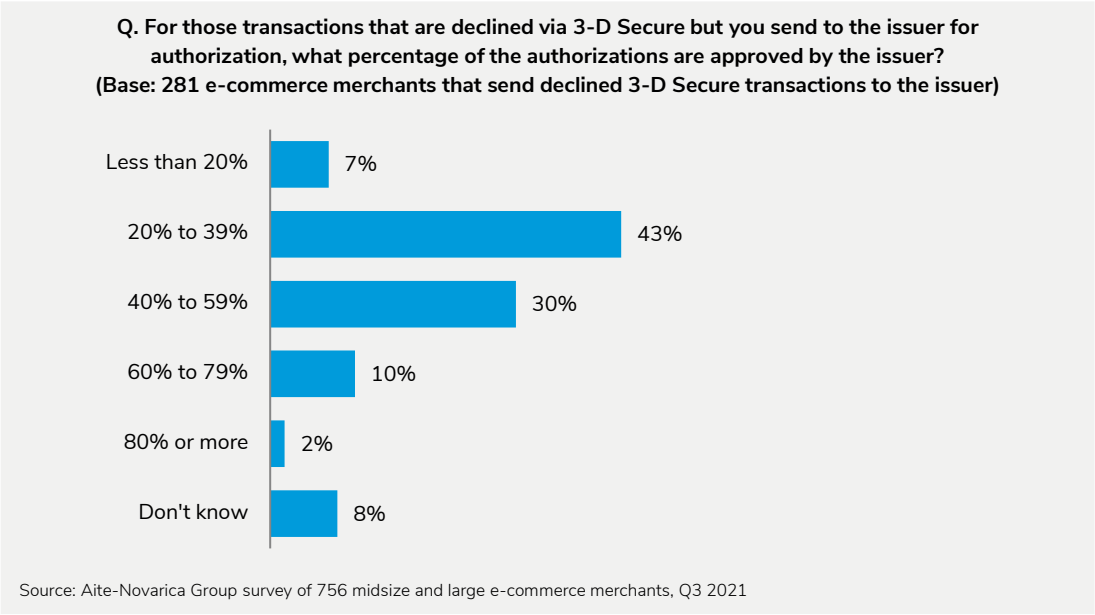
FIGURE 20: REASONS FOR SUBMISSION OF 3DS DECLINES FOR AUTHORIZATION BY AOV



Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q3 2021

The strategy is often successful. Forty-three percent of merchants say that when they take this approach, between 20% and 39% of transactions are approved, while 42% of merchants say that 40% or more of these transactions are approved (Figure 21).

FIGURE 21: EXTENT TO WHICH TRANSACTIONS WITH 3DS DECLINES ARE AUTHORIZED BY THE ISSUER



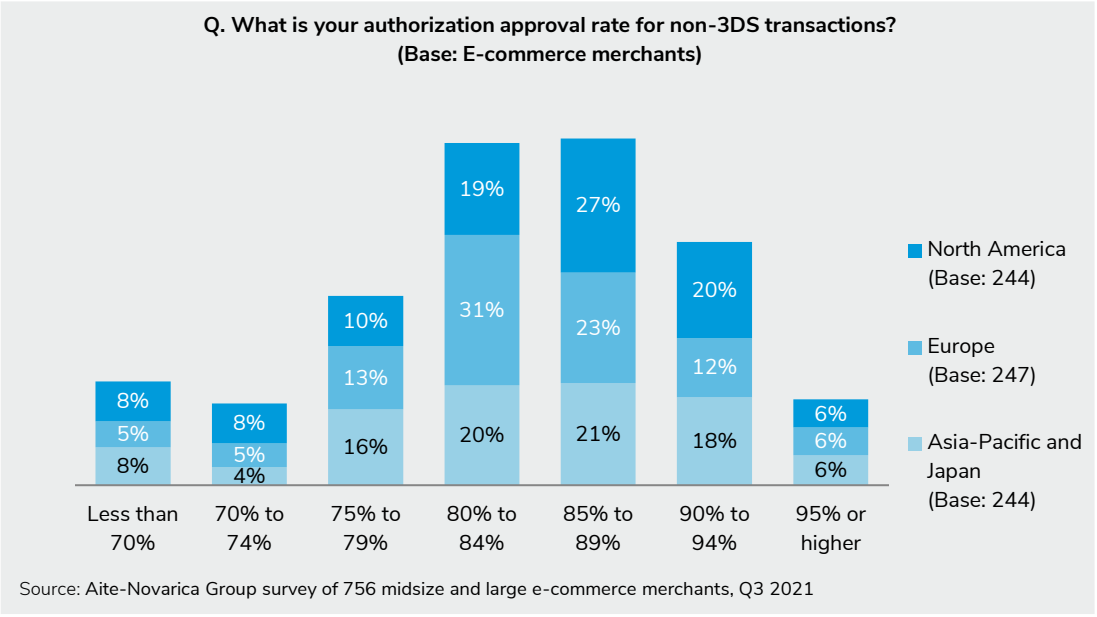
Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q3 2021

3DS TRANSACTIONS HAVE HIGHER AUTHORIZATION RATES

One of the primary drivers for merchants to use 3DS is the desire to improve CNP authorization rates. 3DS is successful in achieving this promise. As shown in Figure 22 and Figure 23, 3DS transactions see higher authorizations across all regions, as follows:

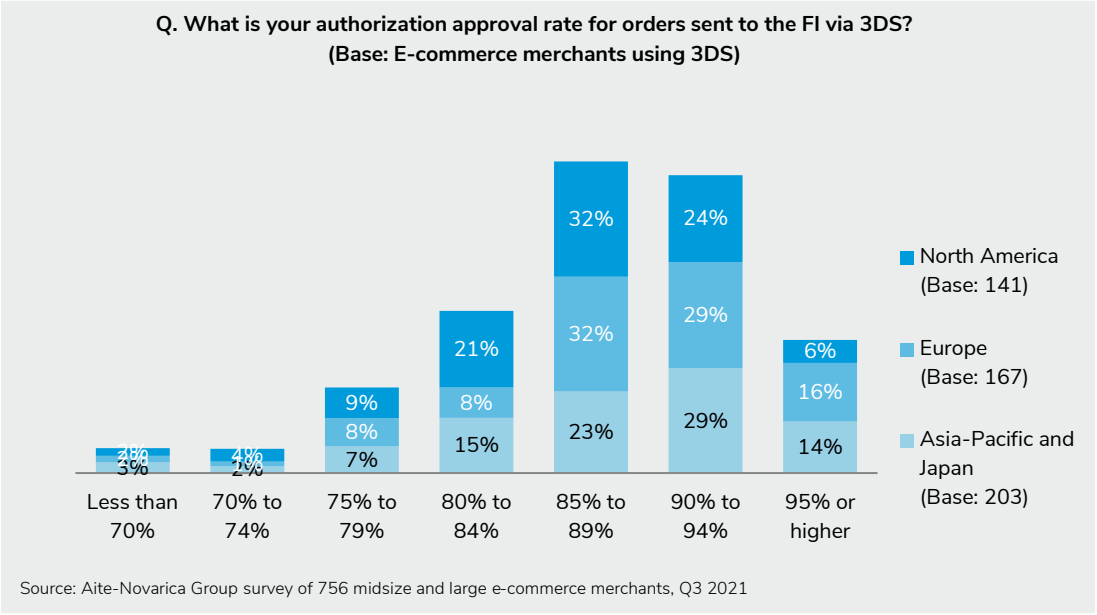
- **North America:** Fifty-three percent of merchants report authorization approval rates of 85% or higher for non-3DS transactions, while 62% of merchants see authorization approval rates of 85% or higher for transactions that ride the 3DS rails.
- **Europe:** Forty-one percent of European merchants report authorization rates of 85% or greater for non-3DS transactions, while 77% of merchants see 3DS transactions with authorization rates of 85% or more.
- **Asia-Pacific:** Forty-five percent of merchants in Australia, India, and Japan see authorization rates of 85% or greater for non-3DS transactions, while 66% of merchants see authorization rates of 85% or more for 3DS transactions.

FIGURE 22: AUTHORIZATION APPROVAL RATE FOR NON-3DS TRANSACTIONS



Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q3 2021

FIGURE 23: AUTHORIZATION APPROVAL RATE FOR 3DS TRANSACTIONS



Source: Aite-Novarica Group survey of 756 midsize and large e-commerce merchants, Q3 2021

CONCLUSION

The industrialization of fraud is here to stay. Fueled by data breaches and sophisticated automated tools readily available in the dark web, the CNP fraud landscape will only continue to escalate. 3DS is a key tool in the arsenal for issuers and merchants worldwide. Here are a few recommendations for issuers and merchants as they map their strategies relative to 3DS:

- **Holistic participation is key.** Like so many things in payments (e.g., the deployment of chips), 3DS works best on a level playing field with equal participation by merchants and issuers. Europe provides a great example of this: Merchant and issuer participation in 3DS is high, and as a result, overall CNP fraud rates are low; CNP authorization on 3DS transactions is significantly higher than on non-3DS transactions; and attrition rates in response to stepped-up prompts trends lower than nonregulated markets like the U.S. If merchants in nonregulated jurisdictions begin sending more volume, rather than cherry-picking the highest-risk transactions, the same benefits in terms of higher authorization rates are likely to accrue. And as consumers become trained to expect occasional friction, attrition rates will also decrease.
- **Upgrade the authenticators.** A fraud system is only as strong as its weakest link. SMS OTP, with its susceptibility to SIM swapping and social engineering, is increasingly that weak link, and authenticators such as mobile app push and biometrics provide better security as well as a positive user experience.
- **Merchant education about 3DS is lacking.** With many merchants indicating they don't have awareness of 3DS, and another significant cohort of merchants not aware of the requirement to sunset 3DS1 by October 2022, it is apparent that there is still an education gap.
- **Data is king.** To achieve the promise of 3DS2 to help reduce false declines, merchants need to make more use of the enhanced data sets and ensure the data that is sent has a good level of data hygiene.

RELATED AITE-NOVARICA GROUP RESEARCH

Aite Matrix: Global Chargeback Guarantee Vendors, November 2020

Improving the Dispute Experience: Transparency Is Power, May 2020

3DS2 and Fraud Prevention: Decision Drivers in the European Marketplace, May 2020

Disputes Upheaval: The Merchant Perspective on Pre-Dispute Solutions, May 2020

Strong Customer Authentication: Friend or Foe?, January 2020

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
jconroy@aite-novarica.com

Contributing authors:
David Mattei
dmattei@aite-novarica.com

Ron Van Wezel
rvanwezel@aite-novarica.com

Research Design & Data:
Judy Fishman
jfishman@aite-novarica.com

Sonia Kundal
skundal@aite-novarica.com