datos INSIGHTS

November 2023

CNP Fraud and the Role of 3-D Secure: The Tale of Different Countries

David Mattei
Julie Conroy

This report provided compliments of:

OUTSEER

November 2023

CNP Fraud and the Role of 3-D Secure: The Tale of Different Countries

David Mattei
Julie Conroy

Table of Contents

List of Figures

List of Tables

Summary and Key Findings

E-commerce continues its upward climb as customers increase their propensity for digital commerce. However, once chip cards very effectively addressed counterfeit fraud at the point-of-sale, e-commerce struggled to find a similar solution to mitigate card-not-present (CNP) fraud. 3-D Secure (3DS) is one of the more promising solutions, but usage is inconsistent globally and thus has varying results.

This Datos Insights research study, sponsored by Outseer, entails a survey of 20 fraud executives at large financial institutions (FIs) in Q3 2023 in Australia, Canada, Germany, the U.K., and the U.S. Given the size of these countries and their varying regulatory landscapes, the results provide a directional indicator of the trends in these markets. The key findings from this report follow:

- **Location matters for higher authorization rates:** Many jurisdictions have regulatory requirements or payment network mandates for strong customer authentication (SCA) on e-commerce transactions. Jurisdictions with such mandates have better outcomes for CNP authorization approval rates than in non-mandated geographies. For example, FIs in the U.K. report average authorization rates for 3DS-protected transactions of 93% versus 86% for U.S FIs.

- **As 3DS usage increases, CNP fraud losses decrease substantially in regulated markets:** In unregulated markets such as North America, 3DS usage averages 2.7% of all CNP transactions, yet fraud rates on 3DS-protected transactions are nearly six times higher than for all CNP transactions. This is largely because the majority of merchants in unregulated markets send only high-risk transactions across the 3DS rails, which in turn prompts issuers to employ more draconian authorization strategies, which also adversely impact authorization rates. The inverse is true in regulated markets such as Europe and Australia, in which 25% to 50% of CNP transactions are protected by 3DS, and fraud rates are three times to six times lower than for all CNP transactions.

- **U.S. CNP fraud losses are on the rise:** Datos Insights estimates U.S. CNP fraud losses will exceed US$9 billion in 2023 and approach nearly US$13 billion by 2026, as fraudsters continue to heavily target CNP, particularly in markets that do not require strong authentication for e-commerce transactions. For example, U.S. e-commerce sales averaged an annual increase of 19% over the past six years whereas CNP fraud losses grew faster at a rate of 21% over the same time period. On the other hand, in

markets like the U.K., which have been steadily preparing for SCA for many years, the CNP fraud losses have been steadily declining while e-commerce sales have been growing.

- **3DS is highly rated as one of the better CNP risk mitigation tools available:** Half of the FIs interviewed say that 3DS is better than other CNP fraud controls they have in place. Reasons include enhanced data not available in the authorization message, risk-based assessments leveraging machine learning (ML) models, and ability for user authentication. North American FIs in particular have better perceptions of 3DS compared to two years ago when half of them indicated it was worse than other CNP fraud detection controls. Among the North American FIs interviewed in 2023, 70% of the FIs interviewed believe 3DS to be as effective or more effective at fraud detection than their other CNP tools.

- **FI attitudes toward user authentication methods have changed dramatically:** In 2021 only 24% of FIs had or were planning to make changes to how they authenticate a user, with a one-time password (OTP) via text message or email being the predominant method. In 2023, 94% of FIs have recently or are planning to make changes to their authentication method. FIs are realizing the heightened susceptibility of OTP interception via text and email.

- **3DS data is useful in authorization fraud systems:** Seventy-five percent of FIs surveyed in 2023 currently support or plan in the next one to two years sending 3DS data to their transaction authorization fraud platforms. The additional intelligence provided by 3DS systems will enable improved FI authorization decisioning to positively impact approval rates and false declines.

- **Many issuers would welcome a 3DS mandate in North America:** While FIs tend to shy away from increasing regulation, several North American FIs would welcome a mandate by the government or card brands that would increase the number of 3DS-protected CNP transactions. One U.S. FI said, "It would be great if merchants and FIs played more nicely together. That could drive 3DS adoption." In a similar vein, a Canadian bank said, "The card brands need to work with merchants to get them to adopt and use 3DS more. While mandates have worked in other markets, I don't think it's going to happen in North America."

Introduction

E-commerce is alive, well, and growing, fueled by consumers' appetites for buying online. E-commerce sales continue to increase annually, and billions of dollars are lost each year to CNP fraud. EMV chip cards have significantly reduced in-store fraud losses, thus driving fraudsters to the online channel in which chip technology does not offer protection. Mitigating this form of fraud is a concern for merchants and FIs alike. As FIs work to limit these losses, unintended consequences from aggressive fraud strategies include lower CNP authorization approval rates, false declines, poor consumer experiences, lower card interchange income, and higher operational costs.

Fortunately, the 3DS specification, now managed by EMVCo, provides a way to protect e-commerce transactions and increased authorization rates, when used appropriately. 3DS is widely supported globally among issuers, merchants, payment processors, and other industry players. FIs typically work with an access control server (ACS) vendor to procure their 3DS solution that offers a combination of enhanced data, transaction risk assessment, and the ability to authenticate cardholders at the time of purchase, thus lowering CNP fraud losses. While that is how it is supposed to work on paper, the reality is that 3DS benefits depend on what country and region of the world the FI is located, based on the degree to which strong user authentication for e-commerce transactions is mandated, and the extent of merchant participation.

This report explores FI experiences and attitudes with CNP fraud and 3DS, and why an FI's geographical footprint makes a difference in the benefits it derives from this standard. It also looks at those industry forces that may impact this standard and its usage in the future.

Methodology

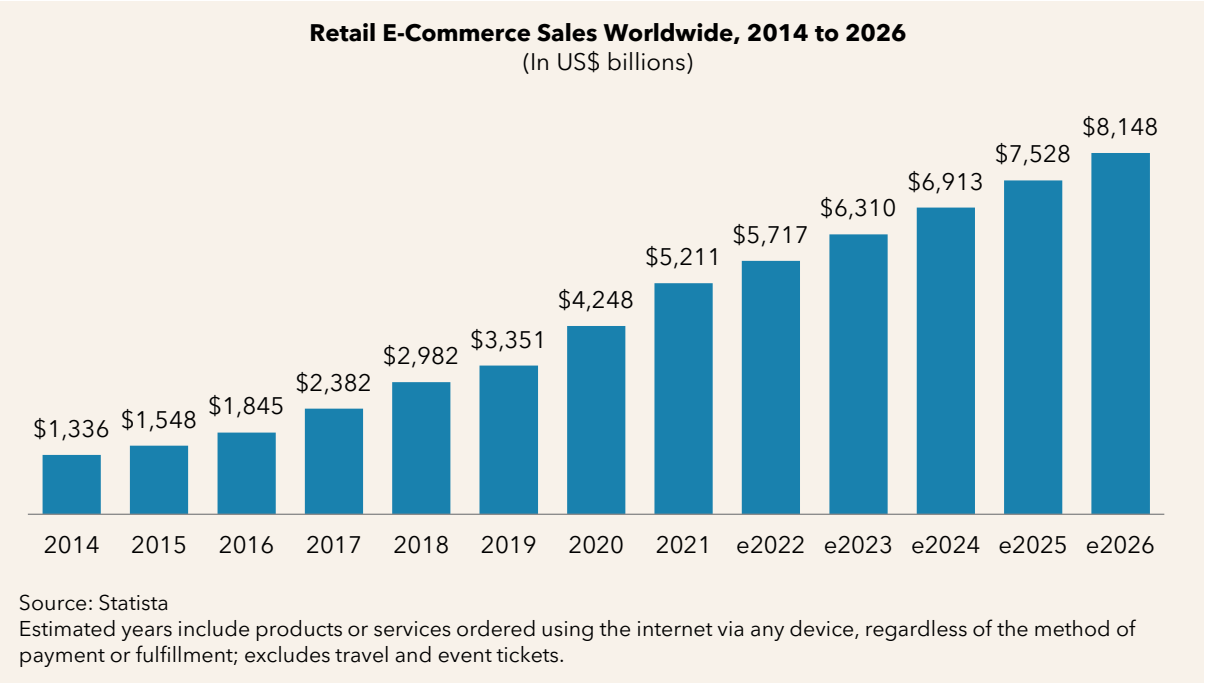
In this research, sponsored by Outseer, Datos Insights interviewed fraud executives at 20 FIs to assess their CNP fraud and 3DS usage and experiences, authorization approval rates, fraud losses, and thoughts on emerging technologies that have the potential to impact 3DS. The combined qualitative and quantitative survey was conducted in Q3 2023. The geographic distribution of the FIs included four FIs in Australia, two FIs in Canada, two FIs in Germany, four FIs in the U.K., and eight FIs in the U.S.

The CNP Market

E-commerce sales and transaction growth continue their steady climb as merchants cater to customers who prefer to shop from the comfort of their home and avoid the car drive and crowds at brick-and-mortar stores. After nearly two decades of a slow and steady increase in e-commerce sales, the pandemic slammed the accelerator pedal to the floor, and e-commerce sales spiked in 2020 as in-store shopping literally disappeared overnight across the globe.

Globally, e-commerce sales have enjoyed double-digit growth rates for many years, with 2023 global sales forecasted at US$6.3 trillion and increasing to US$8.1 trillion by 2026 (Figure 1). As a percentage of global retail sales, e-commerce represents 20.2% of all spend in 2023, increasing to 23.3% by 2026.

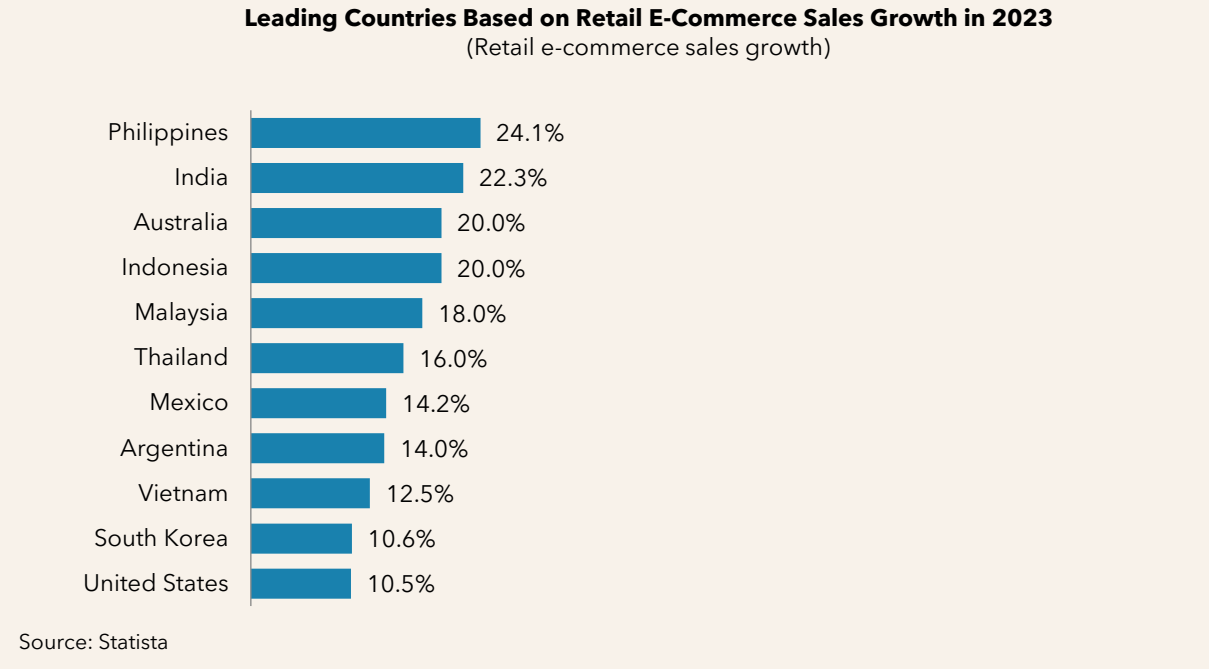
Figure 1: Global Retail E-Commerce Sales, 2014 to e2026



Source: Statista
Estimated years include products or services ordered using the internet via any device, regardless of the method of payment or fulfillment; excludes travel and event tickets.

E-commerce sales vary by region. Significant double-digit e-commerce sales growth is occurring in emerging e-commerce markets, such as in the Asia-Pacific and Latin America. More established e-commerce markets, such as in China, the U.S., and Europe, are experiencing annual growth rates of 10% or less (Figure 2).

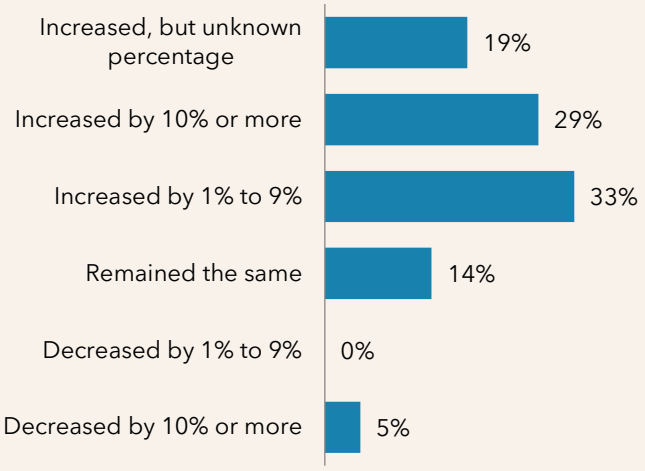
Figure 2: Annual Sales Growth in E-Commerce Retail Sales



Over the past 12 months, 81% of FIs interviewed report that CNP transaction volume has increased, with a weighted average of 9.7%, while 14% of FIs report CNP transaction volume is flat. The surveyed FIs are in more mature e-commerce markets and reflect the general lower-growth nature of CNP transactions in those regions of the world (Figure 3). Of the FIs reporting flat CNP transaction volume, two are in the U.S., and one is in the U.K. The FI reporting decreasing volume is a regional bank based in Australia.

Figure 3: CNP Transaction Volume Trends

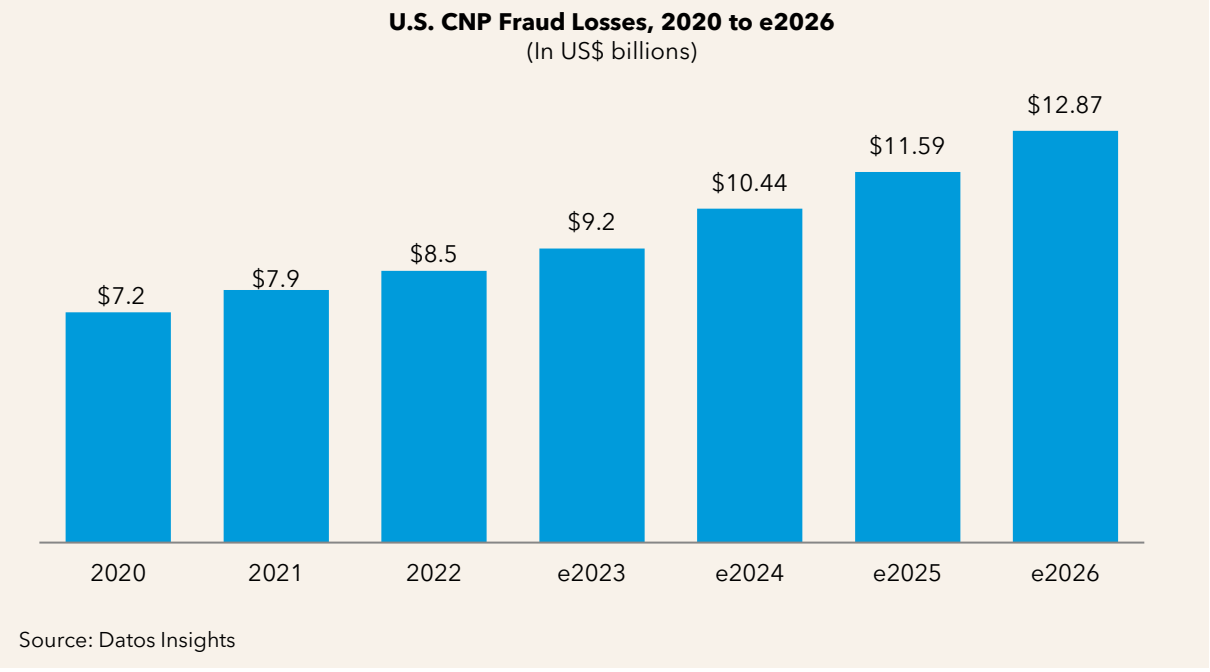
Q. Over the past year has the number of your CNP transactions decreased, remained the same, or increased?
(Base: 20 Financial services executives)



Source: Datos Insights survey of 20 financial services executives in the U.S., Canada, U.K., Germany, and Australia, Q3 2023

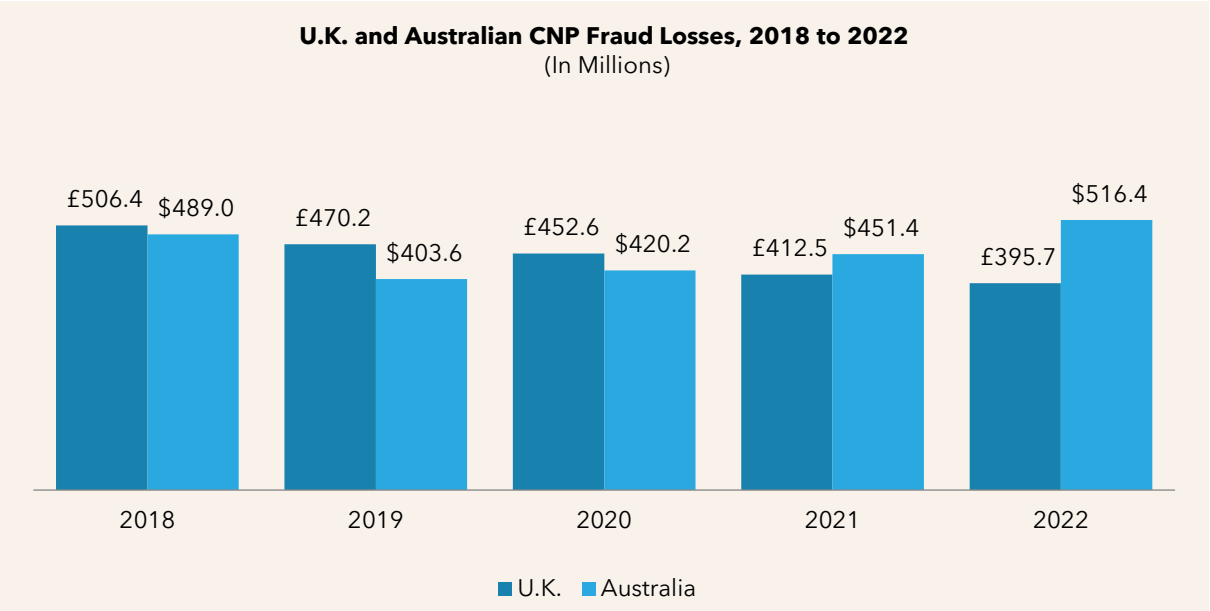
CNP fraud losses continue to grow in many jurisdictions. Datos Insights forecasts U.S. CNP fraud losses will exceed US$9 billion in 2023 and approach nearly US$13 billion by 2026 (Figure 4), at a pace commensurate with the growth of e-commerce transaction volume. In the U.K., the mandate for SCA took effect in March 2022, but many FIs and merchants worked for years prior preparing for the mandate, and as a result, CNP fraud has been steadily declining in that market since 2018 (Figure 5). Australia saw a brief dip in CNP fraud in 2019, concurrent with a mandate that required SCA for a wide swath of merchant category codes. The rising tide of CNP transaction volume drove subsequent increases in CNP fraud, though the 8.6% CAGR from 2018 to 2022 was significantly slower fraud loss growth than the 20% year-over-year growth in CNP transaction volume that Australia experienced during that period.

Figure 4: U.S. CNP Fraud Losses 2020 to e2026



Source: Datos Insights

Figure 5: U.K. and Australian CNP Fraud Losses, 2018 to 2022



Sources: UK Finance, AusPay 2023

Protecting Against CNP Fraud

There is no single solution that mitigates CNP fraud. Therefore, FIs deploy a multi-dimensional set of tools. The FIs interviewed report having some combination of the following in their CNP fraud control frameworks:

- **Transaction fraud monitoring:** These solutions use a combination of ML models and rules engines to assess the risk level of a CNP transaction to determine whether to approve, alert, or decline it.
- **Third-party ML scores:** FIs may subscribe to a third-party service that will send them a fraud score for a specific transaction. Card brands are one type of third-party provider that offer this service and will include their fraud score in the authorization message sent to the FI. Fraud vendors also offer ML scores either in an on-premises or Software-as-a-Service implementation.
- **3DS ACS solutions:** When 3DS is invoked by the merchant, the request is sent to the respective card brand, which in turn sends it to the FI's ACS vendor. These solutions risk assess the transaction and approve, decline, or invoke stepped-up authentication of the cardholder.
- **Device fingerprinting and behavioral biometrics solutions:** Though less common, a few FIs use these tools to risk assess consumers' devices and monitor their behavior in two ways. One, when stepped-up authentication occurs as part of the 3DS flow, the FI can access this data to capture additional risk signals. However, this is only possible when stepped-up authentication is invoked. In another scenario, an FI can access this data when a cardholder uses the mobile banking app to retrieve card data to make payment on the merchant's checkout page.
- **SMS verification:** OTPs sent via email and SMS have long been known to be vulnerable authenticators, with fraudsters compromising via phishing, social engineering, and SIM swaps. The U.K. market has been on the front lines of this attack vector for many years. While all of the U.K. banks interviewed still use SMS OTP as an authenticator, the majority of them bolster the security with a call to the mobile network operator to assess SIM swap risk.

- **Card tokenization:** Cardholders can store a tokenized version of their credit and debit card numbers in mobile wallets (e.g., Apple Pay, Google Pay, Samsung Pay), which ensure the actual card numbers are not provided to the merchant at the time of payment. As long as strong identity-proofing is conducted at the time of provisioning the consumer's card into the wallet, using tokenized cards helps lower CNP fraud.

Global 3DS Usage

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. The goal of 3DS is to mitigate CNP fraud losses by risk assessing the transaction and, if needed, authenticating the person performing the transaction. When 3DS is invoked and a transaction is approved by the issuer, liability for any resulting fraud shifts to the issuer. The merchant determines whether to invoke 3DS, based on its risk appetite as well as local regulatory requirements that mandate multi-factor authentication (MFA), as applicable. Issuers are mandated by the card brands to support it.

When a merchant invokes 3DS, it sends the transaction to its 3DS service provider, which then sends it to the card network. The card network identifies the FI that issued the card being used for payment and sends the transaction to the FI's 3DS service provider (known as the ACS). The FI's ACS risk assesses the transaction and determines what action to take: approve, decline, or authenticate the user. When stepped-up authentication is invoked, the FI is put into direct communication with the person performing the transaction to verify the person is its customer. Afterward, an approve/decline response is returned to the merchant via the same path it was sent. 3DS is for user authentication and is not a replacement for transaction authorization. Assuming the FI responds to the merchant with a 3DS approval, the merchant then sends an authorization message for financial approval of the transaction to the FI. Increasingly, issuers send 3DS authentication outcomes to their authorization system, which enhances that potential for a positive authorization outcome if the authentication result is positive.

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

Table A: 3DS 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 the Asia-Pacific and Latin America.
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 addressing CNP fraud risk by requiring more stringent controls.	Mandates for MFA for CNP transactions are becoming more prolific. All eyes are on the EU, the largest card market to enact such a mandate to date. Countries such as Australia, Japan, Mexico, and Turkey already have active initiatives underway to follow the EU's lead.
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 Datos Insights

Another element of a 3DS transaction is additional data that can be sent from the merchant to the issuer about the transaction and the user performing it. 3DS supports over 150 data elements in its message format—data that is not available in a traditional financial authorization message exchanged between merchants and FIs via the card brands. These additional data elements, when populated, provide insights to the FI to detect potentially fraudulent activity.

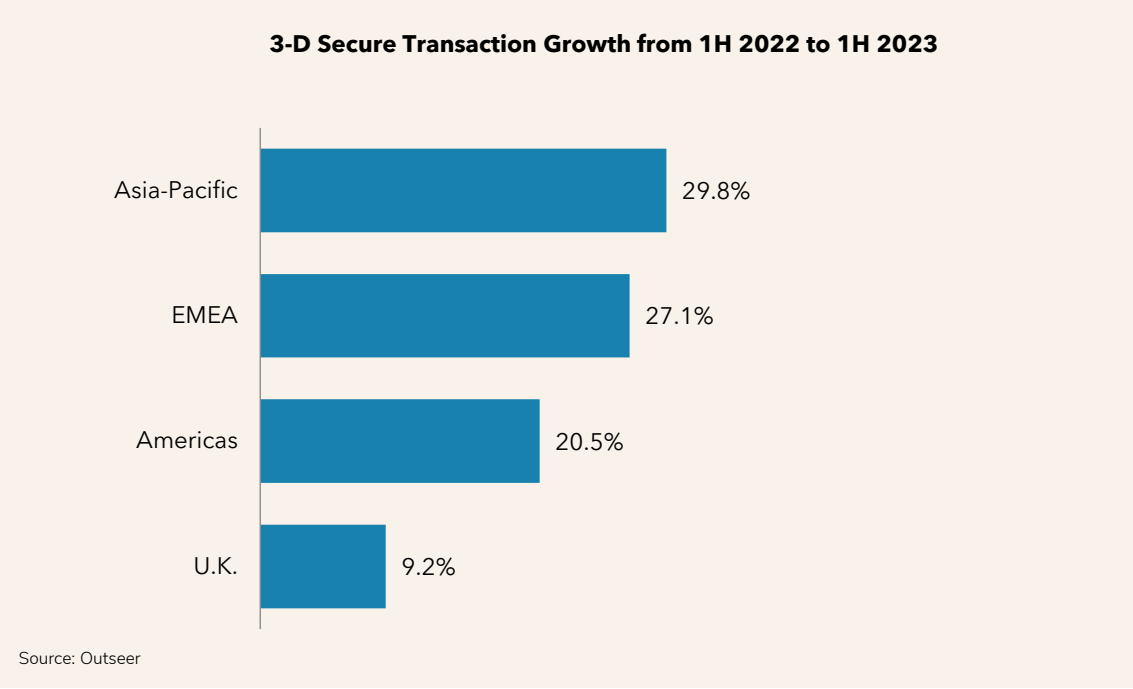
Some regions, such as the EU, Australia, Singapore, India, South Korea, South Africa, and others, mandate SCA. In the EU and U.K., exemptions exist for low-dollar amount transactions, recurring payments, and others. Canada and the U.S. have no mandates for authenticating a user in a CNP transaction, thus 3DS usage is determined by the merchant.

3DS Usage Increasing

3DS usage is increasing globally, driven in part by the rising tide of mandates across various jurisdictions, and in unregulated jurisdictions motivated by the desire of merchants to have the peace of mind of the fraud liability shift to the FI. Figure 6 shows the substantial

year-over-year growth in 3DS transaction volume from the first half of 2022 to the first half of 2023; in aggregate across the various regions, 3DS volume grew 11% from the first half of 2022 to the first half of 2023. While the U.K.'s numbers pale in comparison to other jurisdictions, this is largely because the SCA mandate went into effect there in March 2022, so the substantial uptake of 3DS happened prior to that date.

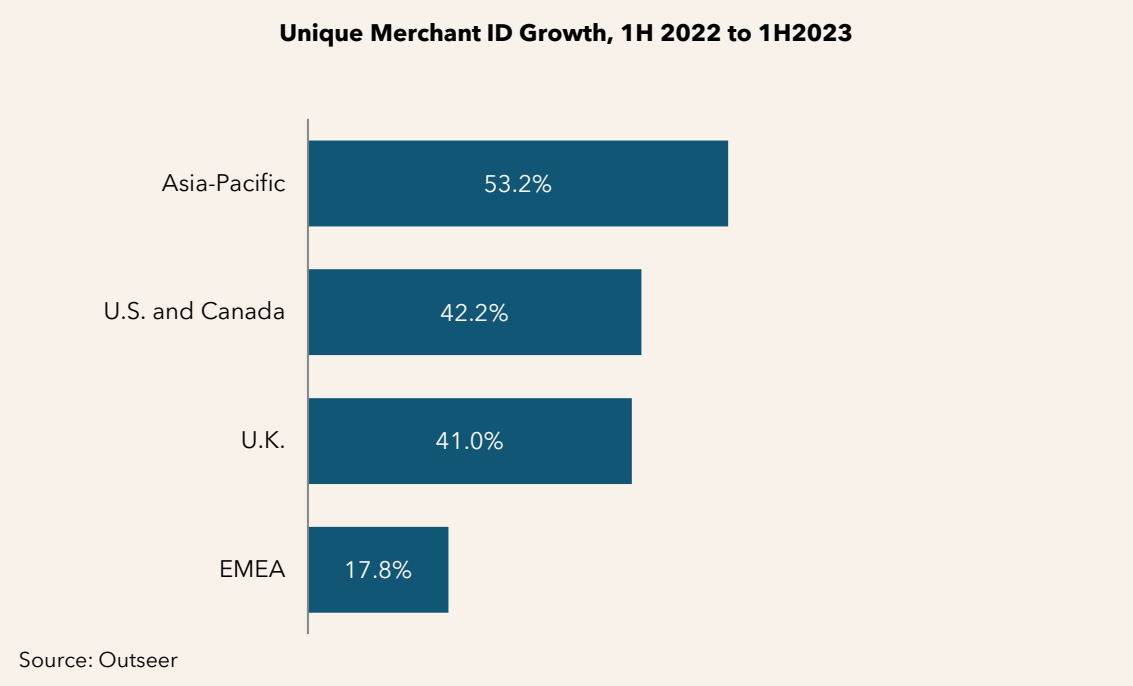
Figure 6: 3DS Transaction Volume Growth, 1H 2022 to 1H 2023



Source: Outseer

As shown in Figure 7, the growth of the volume of unique merchant IDs that are sending transactions across 3DS rails is growing at an even faster year-over-year clip than 3DS transaction volume itself. The total number of merchant IDs invoking 3DS grew globally by 33% from the first half of 2022 to the first half of 2023. The expanding requirement for SCA is likely one growth driver—any merchant that does business with consumers in a region that requires MFA for CNP has to enable a compliant solution.

Figure 7: 3DS Unique Merchant ID Growth, 1H 2022 to 1H 2023

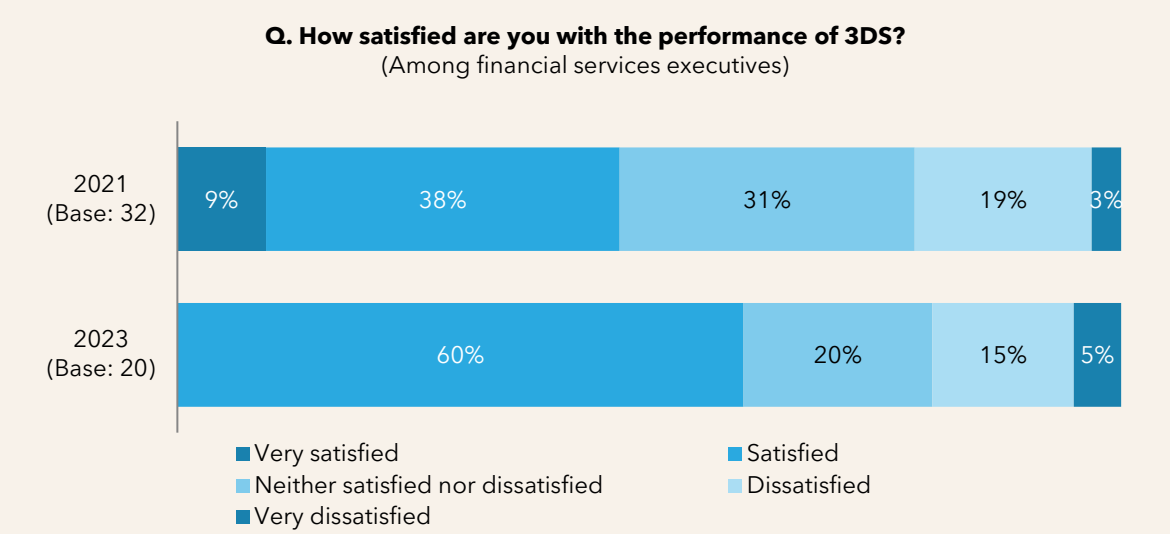


Source: Outseer

3DS usage varies widely around the world, and the differences are noticeable based on the country and whether it has a mandate. In Europe, which has a stronger mandate, nearly 50% of CNP transactions are protected by 3DS. In Australia, which has a softer mandate, nearly 25% of CNP transactions are protected by 3DS. North America has no mandates, and roughly 2.7% of CNP transactions are protected by 3DS. In the U.S., the range is between 2% and 4%, while in Canada, it is between 3% and 5%.

FIs are increasingly satisfied with the performance of 3DS for mitigating CNP fraud. In 2021, 47% of FIs were satisfied or very satisfied with its performance, and that has jumped to 60% of FIs in 2023 (Figure 8). Increased usage of 3DS and the enriched data exchange between merchants and FIs provided by 3DS contribute to higher satisfaction levels.

Figure 8: FIs' Satisfaction With 3DS, 2021 vs. 2023



Source: Datos Insights survey of 20 financial services executives in the U.S., Canada, U.K., Germany, and Australia, Q3 2023; Datos Insights interviews with 34 issuers and issuing processors, May to August 2021

Stepped-Up Authentication

In unregulated markets, the merchant dictates whether to invoke 3DS. In all markets, the FI decides whether to authenticate the user. Many merchants have concerns using 3DS since there is a possibility the user may incur friction in the checkout process if the FI decides to perform a stepped-up authentication. Merchants prefer to complete a sale as seamlessly as possible to avoid the user becoming frustrated with the authentication process and potentially abandoning the transaction (and thus losing the sale). This is why 3DS usage is lower in North America, where on average, only 2.7% of CNP transactions are protected by 3DS.

FIs may consider several factors when determining whether to perform stepped-up authentication, such as the risk level of the transaction, local regulatory requirements, whether the user is a high-value client, the merchant that is invoking 3DS, and others. The North American FIs interviewed for this report invoke stepped-up authentication for nearly 40% of 3DS transactions, compared to 20% for European FIs. There are several reasons for these variations. North American FIs observe that many merchants use 3DS only for the highest-risk CNP transactions in hopes of avoiding financial liability. As a result, North American FIs are more suspicious of CNP transactions coming through 3DS and thus more likely to perform stepped-up authentication to ensure it is their cardholder. This contrasts with a regulated market such as Europe where 3DS usage is required for the vast majority

of CNP, so the risk profile of inbound 3DS transactions is vastly different. Another probable reason for the different rates of stepped-up authentication among regulated and unregulated countries is that fraudsters have a higher bar in perpetrating CNP fraud in regulated markets and thus focus on unregulated markets that represent a softer target.

Australia has an elevated stepped-up authentication rate of 44% for a regulated country though its regulation is not as strict as in Europe. Australian FIs report that more merchants are using 3DS, while more consumers are using payment cards to make higher-value purchases, which tend to have higher risk, especially as scam fraud has increased recently, thus the relatively high stepped-up authentication rate.

Seventy-five percent of the FIs interviewed perform stepped-up authentication by sending the user an OTP via a text message to the user's mobile device or through email. This is the most popular method by a wide margin. Prior to sending an OTP via text messaging, a few FIs (primarily in the U.K.) conduct a SIM swap check on the mobile phone number to ascertain whether it has recently been ported to new device—an indicator of fraudulent activity. Other authentication methods include the following:

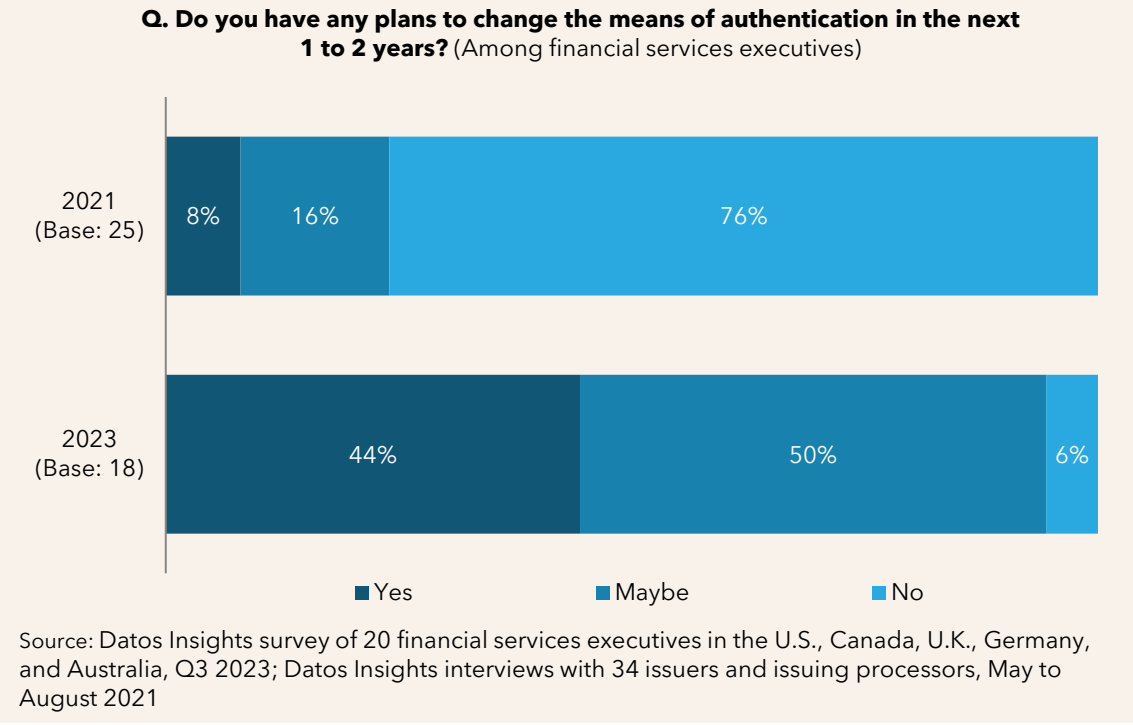
- OTP sent to the mobile banking app. One FI requires consumers to receive the OTP via the mobile app for CNP transactions; it will not send the OTP code any other way.
- OTP via a phone call
- Authenticator apps such as Microsoft Authenticator

OTP delivery via SMS and email is known to be weak as it is easy for fraudsters to intercept the OTP via bank impersonation, SIM swap, or email redirection. The pain associated with these attack vectors was noted by several FI interviewees. Many FIs report using a waterfall approach to determine how best to send an OTP to the user in which the most secure delivery mechanism is attempted first, and subsequently less secure options are used as a fallback. For example, the first choice may be to send the code to the bank's mobile app, assuming the user has installed it. If not, the second choice would be delivery via text message. And if the user does not have a mobile phone to receive a text message, the third choice would be delivery via email.

Given the vulnerability of OTP sent via SMS or email, it is not surprising that all FIs interviewed except one have firm plans in place or are considering changing the way they authenticate a user, which represents a substantial change since the 2021 study. In 2021, only 24% of FIs said they may or would change their authentication method and that

increased to 94% of FIs in 2023 (Figure 9). It's encouraging to see better authentication methods coming soon.

Figure 9: FI Plans to Change Authentication Methods



Source: Datos Insights survey of 20 financial services executives in the U.S., Canada, U.K., Germany, and Australia, Q3 2023; Datos Insights interviews with 34 issuers and issuing processors, May to August 2021

FIs are considering the following new authentication methods as possible replacements for OTP via text message and email:

- Biometrics such as face, fingerprint, and behavioral attributes while possibly including a liveness detection check as part of this process
- Mobile banking app (for those FIs that do not support it today)
- Device ID and maintaining a list of trusted devices for each consumer. Since an OTP represents "something you have," device ID could serve as a proxy for this, which would reduce the need to send OTPs while also improving the user experience.

EMVCo, the company that owns and manages the 3-D Secure protocol globally, is discussing adding Fast ID Online (FIDO) technology in a future version of 3DS, possibly the next version, which will be v2.4. FIDO would enable finger and facial biometrics as new authenticators native to the 3DS protocol. FIs were roughly split as to whether they know about this potential future enhancement. Those that are aware of FIDO's inclusion in a

future version of 3DS were bullish on its impact, believing it would add a strong method of user authentication and improve the user experience. FIs in the U.K. are particularly excited about this since there is a requirement that U.K. passport holders and residents who are not U.K. citizens register their face and thumbprint biometrics, which are then stored in a government database. A cardholder's fingerprint or facial biometric used to authenticate a 3DS transaction could be verified against the government database.

Transaction Abandonment

When users are prompted to authenticate in a 3DS transaction, there is a possibility that they will abandon the transaction. Abandonment can occur because the user is unwilling to perform the authentication process for any number of reasons (e.g., too difficult to do, not comfortable with the process, security concerns, and others) or because the user is actually a fraudster and is unable to authenticate. Since authentication is intended to stop fraudsters from completing the transaction, the abandonment rate will likely never be 0%, but new authentication methods should help minimize the issue. FIs and merchants closely monitor abandonment since high rates negatively impact transaction conversions and thus sales.

The average abandonment rate for North American FIs is 18.3%, and for European and Australian FIs, it is 11.3%. Europe and Australia have had SCA mandates for a few years and consumers are more accustomed to being authenticated, which explains why abandonment is lower there. However, in North America, where there is no mandate and little to no consumer awareness of 3DS authentication, it is not surprising to see higher abandonment rates. Merchants in North America tend to send only their highest risk transactions via 3DS leading FIs to invoke stepped-up authentication more frequently. Therefore, a North America consumer may be surprised to see or be confused by the authentication request and decide not to complete it.

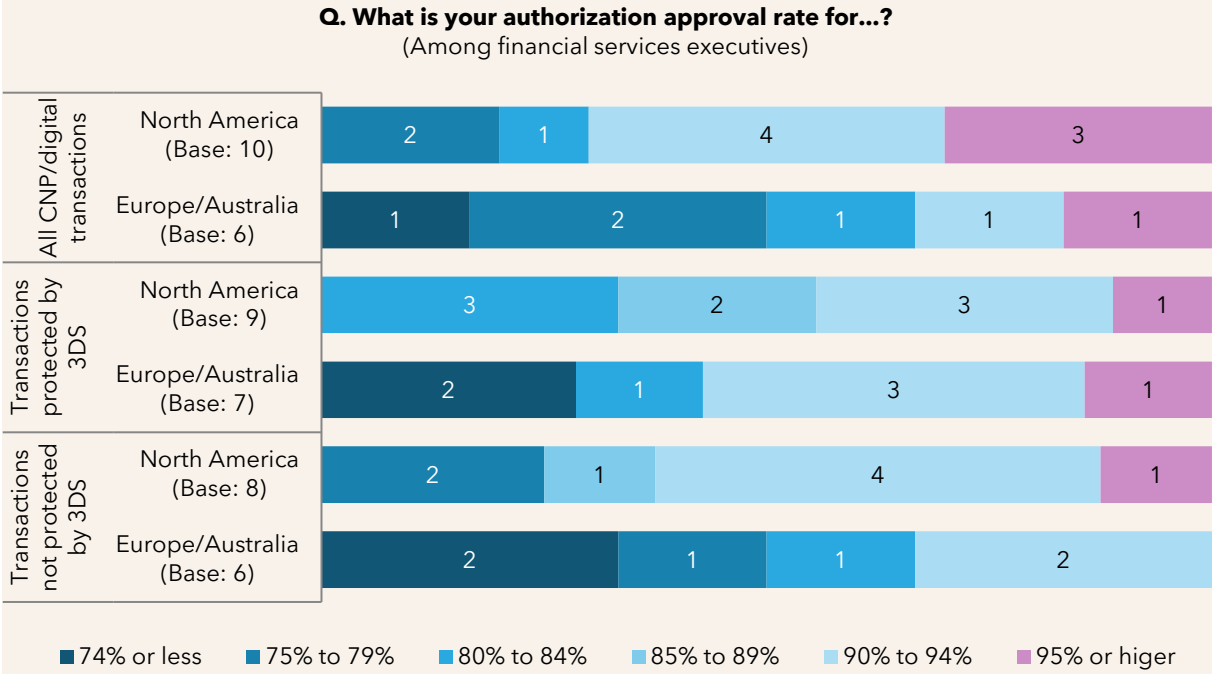
Authorization Approval Rates and Fraud Losses

FIs and merchants have a shared goal: safe and secure CNP transactions with the highest authorization approval rates possible. Unfortunately, authorization approval rates for CNP transactions have generally hovered in the mid-80% range while card-present transactions average over the mid-90% range. Closing this gap has been an industry focus for many years but has been a vexing problem to solve.

When CNP transactions are protected by 3DS, approval rates tend to be higher in regulated versus unregulated markets. Four of seven FIs in regulated markets have CNP

authorization approval rates of 90% or higher compared to only four of nine FIs in unregulated markets (Figure 10). This dichotomy is due to several factors. One, 3DS usage in North America is quite low with a very small percentage of CNP transactions protected by 3DS, and those transactions tend to be high risk and declined more often. However, Europe and Australia have much higher percentages of CNP transactions protected by 3DS and consumers are more accustomed to being authenticated. Therefore, 3DS is effective at increasing CNP authorization approval rates.

Figure 10: CNP Authorization Approval Rates by Region



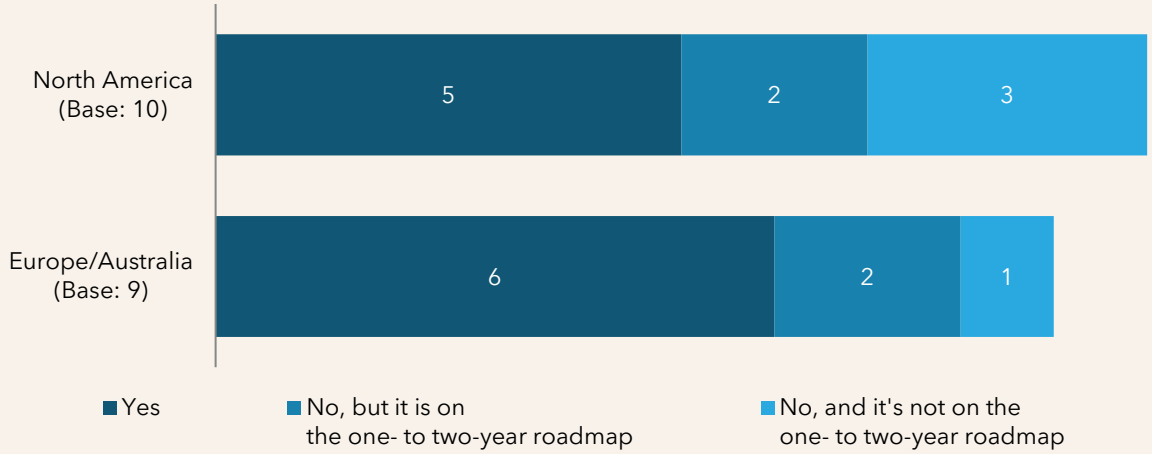
Source: Datos Insights survey of 20 financial services executives in the U.S., Canada, U.K., Germany, and Australia, Q3 2023

FIs appreciate having the ability to risk assess a transaction and authenticate a user as needed prior to the transaction authorization flow. The risk assessment step in the process provides FIs with another fraud score that can be used in decisioning. In a world seeking more data to be better informed, 3DS provides a mechanism for merchants to share considerably more data with FIs than what is available in an authorization message.

FIs have realized the benefits of the enriched data available in 3DS and are leveraging it in their transaction fraud system for authorization decisioning. A majority of FIs in North America, Europe, and Australia send 3DS authentication data to their fraud authorization platform today or have plans to in the next one to two years (Figure 11).

Figure 11: Propensity to Send 3DS Data to Authorization Systems

Q. Does your FI have the ability to send the 3DS authentication data to the fraud system for authorization decisioning and if not, is this on the one- to two-year roadmap? (Among financial services executives)



Source: Datos Insights survey of 20 financial services executives in the U.S., Canada, U.K., Germany, and Australia, Q3 2023

On the other side of the authorization approval rate coin is CNP fraud losses. Since 3DS is a specification for lowering CNP fraud, it is reasonable to expect to see lower fraud losses on 3DS-protected CNP transactions than for all forms of CNP transactions (3DS-protected and non-3DS-protected transactions). This varies by market.

In an unregulated market such as North America, fraud rates on 3DS-protected transactions are nearly six times higher than for all CNP transactions. However, in regulated markets such as Europe and Australia, fraud rates on 3DS-protected transactions range from three times to six times lower than for all CNP transactions. The U.K. is a great example where fraud losses on 3DS-protected transactions average 1 basis point vs. all CNP transactions that average 4.8 basis points.

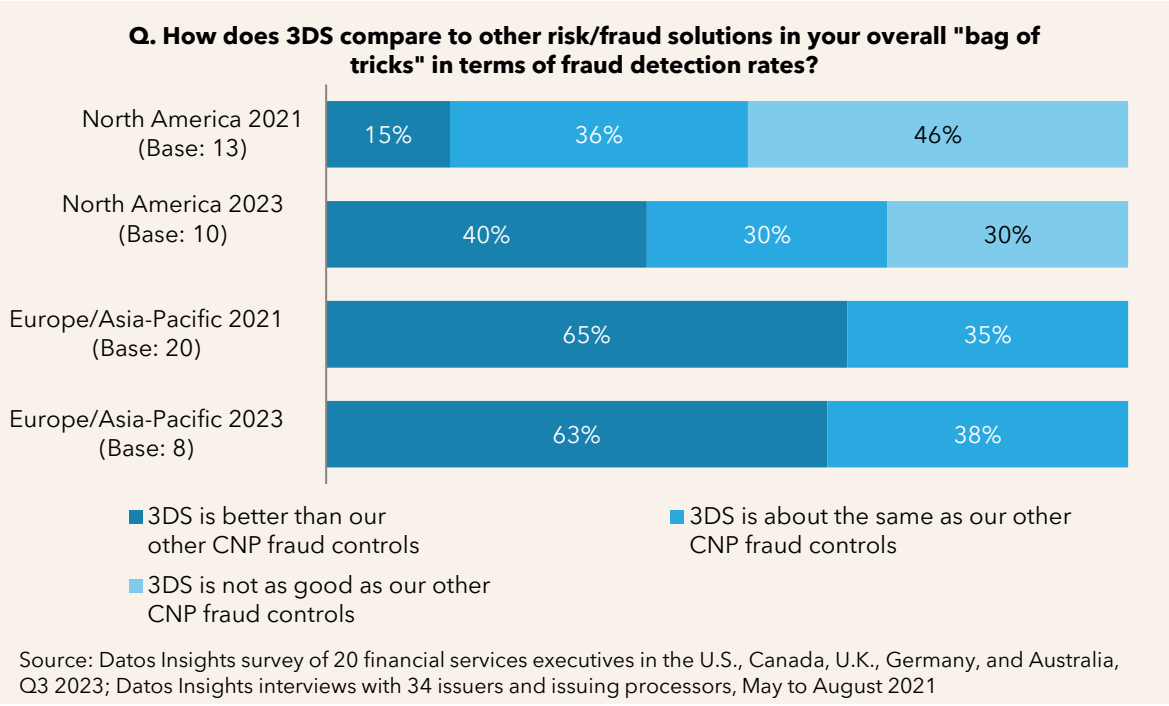
How could a specification to lower CNP fraud losses have such dramatic differences in performance? The answer lies in SCA mandates on CNP transactions. In those areas of the world wherein mandates exist, CNP fraud losses are lower, and authorization approval rates are higher. More data is being shared among merchants and FIs, and FIs have more information to use in their ML fraud detection models. Unfortunately, in unregulated markets in which 3DS usage tends to be quite low, FIs have grown leery of 3DS transactions due to merchants' tendency to use 3DS as an attempt to shift fraud liability to issuers on very high-risk transactions. In fact, many of the interviewed FIs in unregulated markets would prefer to see a mandate so there is more equitable participation, and they

can receive more of the enriched transaction data from 3DS that is not available in an authorization message to improve outcomes.

FI Perceptions of 3DS

FIs deploy multiple tools to mitigate CNP fraud, and 3DS is one of many controls used in production. There are two aspects of 3DS: mitigating fraud losses and the consumer experience. Regarding mitigating fraud losses, FIs are generally positive to neutral on its benefits relative to other tools they are using in production. European and Australian FIs are more bullish on 3DS, with five FIs mentioning it is better than other controls they have in place. Three FIs report it is as effective as other tools (Figure 12). In North America, FIs were evenly split: four FIs say it is better, three say it is the same, and three say it is worse than other controls they have in place.

Figure 12: FI 3DS Perceptions on Mitigating Fraud Losses



Source: Datos Insights survey of 20 financial services executives in the U.S., Canada, U.K., Germany, and Australia, Q3 2023; Datos Insights interviews with 34 issuers and issuing processors, May to August 2021

North American FIs' perceptions have improved considerably since 2021 when nearly half of the U.S. FIs considered 3DS to be less effective than other CNP fraud controls. One North American FI mentioned that with a low volume of CNP transactions that flow through 3DS, its system lacks visibility into the breadth of CNP transactions cardholders perform compared to its transaction fraud detection system that sees all CNP (and card-present) transactions. Another FI mentioned that its ACS provider offers only a rules engine to

manage fraud strategies, whereas its transaction fraud system has ML models that it considers to be more effective than a rules-only approach.

The Future of 3DS

Unfortunately, CNP fraud shows no signs of being eliminated anytime in the near future. When looking into their crystal balls, FIs shared their perspectives on industry trends that may impact 3DS usage as well as what they hope will happen:

- **3DS mandate in North America:** While FIs tend to shy away from more regulations, several U.S. and Canadian FIs would welcome a mandate by the government or card brands that would increase the number of 3DS-protected CNP transactions. One U.S. FI said, "It would be great if merchants and FIs played more nicely together. That could drive 3DS adoption." A Canadian bank said, "The card brands need to work with merchants to get them to adopt and use 3DS more. While mandates have worked in other markets, I don't think it's going to happen in North America."
- **Compelling Evidence 3.0 and merchant/FI data sharing:** Compelling Evidence 3.0 is a Visa program launched in April 2023 to address first-party fraud in which e-commerce merchants can send additional data to the FI about the user, the device, location data, and others. If successful at mitigating first-party fraud, it could spur additional merchant/FI data-sharing collaborations to address other forms of CNP fraud. Mastercard will launch a first-party fraud program in 2024.
- **Card brands performing 3DS checks:** One FI believes the card brands could better serve issuers by performing 3DS checks on their behalf. Since the number of card brands is significantly smaller than the number of FIs in the world, centralizing 3DS checks at the card brands could be more effective at lowering CNP fraud losses.
- **Open banking and real-time payments:** As open banking and real-time payments adoption grow over time, more purchases could be paid via direct bank transfers than by credit and debit cards. If that were to occur, 3DS volume could decrease.

Conclusion

A common disclaimer used in automotive fuel economy estimates is "your mileage may vary." The same is true with 3DS except that it is not based on how you drive but where you live. Regulated vs. unregulated countries and regions of the world affects what performance you see. 3DS continues to be a viable tool to have in one's arsenal to combat CNP fraud losses. FIs should consider the following:

- **Mandates for MFA for CNP are effective.** Where mandates exist, CNP fraud losses are lower and authorization approval rates are higher. More data is being shared among merchants and FIs, and FIs have more information to use in their ML fraud detection models. Many FIs in unregulated markets would prefer to see a mandate so they can see more equitable participation from merchants and have the ability to receive enriched transaction data from 3DS that is not available in an authorization message.

- **Gamesmanship is alive and well in unregulated markets leading to unintended results.** Merchants in unregulated markets that only invoke 3DS for high-risk transactions to shift fraud liability to FIs leads to detrimental outcomes. FIs in these markets are more skeptical of these transactions, leading to higher stepped-up authentication rates and lower authorization approval rates. Conversely, in regulated markets with equitable participation, fraud rates are lower and authorization rates higher.

- **3DS provides an attractive complement to transaction fraud detection systems.** While transaction fraud systems support only a binary approve/decline decision, 3DS provides a mechanism to authenticate cardholders.

- **Ensure you have an effective method of user authentication.** Too many FIs continue to rely upon an OTP sent via text message or email, which are too susceptible to interception by fraudsters. Consider more secure methods such as OTP via mobile banking app, biometrics, and other creative approaches.

- **In North America and other unregulated markets, it's time for merchants and FIs to come together for a shared goal: stopping fraudsters.** Leverage industry groups to have substantive discussions about data sharing. Since the cardholder is a customer of both the merchant and FI, walls can be lowered for mutual benefit.

- **Transaction fraud systems benefit from additional data insights to make better authorization decisions that can increase approval rates and minimize false declines.** FIs should leverage data from the 3DS process and send it to their transaction fraud systems for improved results.

About Datos Insights

Datos Insights 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, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109
www.datos-insights.com

Author information

David Mattei

dmattei@datos-insights.com

Julie Conroy

jconroy@datos-insights.com

Contributing author:

Ana Ropotoaia

aropotoaia@datos-insights.com