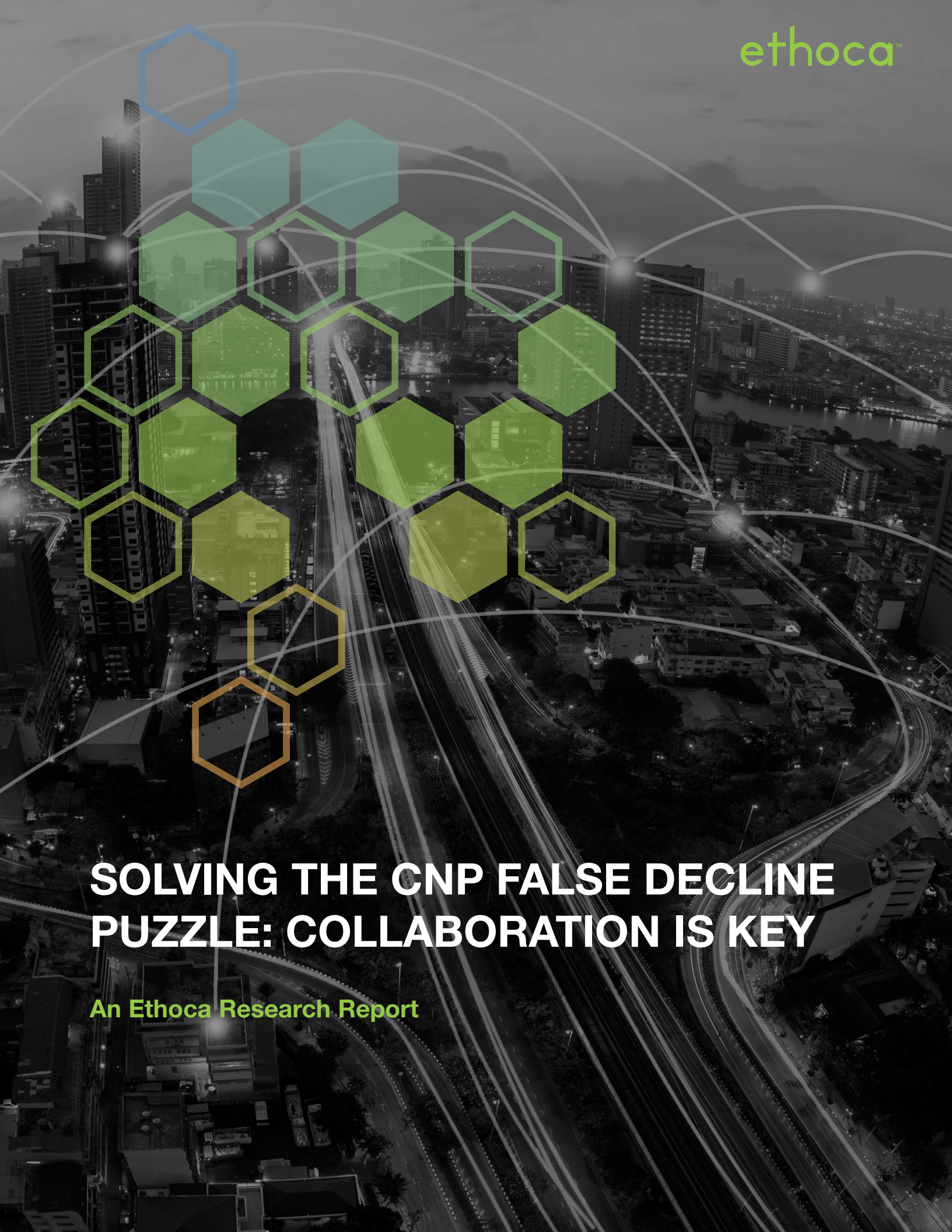


ethoca™

SOLVING THE CNP FALSE DECLINE PUZZLE: COLLABORATION IS KEY

An Ethoca Research Report

ethoca™

making ecommerce simply about **commerce™**

EXECUTIVE SUMMARY

In recent years, the payments industry has started to view the growing CNP fraud problem through an entirely different lens. Today, the overwhelming consensus is that the fraud problem, while increasingly costly, ultimately drives a much larger card acceptance problem. To combat the rise in fraud, both card issuers and merchants alike are deploying multi-layered fraud tools more aggressively to stem the tide of losses and damage to the customer relationship, while effectively controlling operational expenses. The unfortunate and unintended consequence is false declines: good transactions wrongly rejected due to the suspicion of fraud, leading to lost customers. Ethoca's research demonstrates the true nature of this problem goes far beyond declines due to suspicion of fraud, and as an industry we must work together to solve this problem more holistically.

The bottom line is that good customers who transact online are suffering a bad purchasing experience – and this is doubly harmful to both card issuers and merchants. Cardholders may elect to abandon a purchase altogether, seek a different online store to minimize purchase friction, or pull out a different card – sending their go-to card to the back of wallet.

This paper explores the size of the problem, explains the destructive impact on customers who are wrongly turned away, delves into why transactions are declined and reveals how the industry currently manages declines from both a card issuer and merchant perspective. Finally, it presents some possible approaches to the problem, including several pilot programs that Ethoca currently has underway with card issuers and merchants.

KEY FINDINGS

Potentially 475 Million Unique Cardholders Move Preferred Card to Back of Wallet After a Decline

On a global basis, potentially 475 Million cardholders are at risk of moving a preferred card to the back of the wallet after a decline, abandoning their ecommerce purchase entirely or switching to another competitive online store to complete their purchase.

CNP Declines More Complex Than They Seem

While false declines represent a growing problem, card issuers and merchants must take a closer look at the total declines picture.

'DO NOT HONOUR' Declines Contribute to Confusing CNP Purchase Experiences

Merchants lack insight into the true reasons for transaction declines, hampering their efforts to communicate useful and timely order status information.

Digital Goods Customers Respond to Declines in Unique Ways

Decline behaviours vary considerably for customers in the digital channel. Many customers will continue to retry transactions (potentially with another card) until they are approved because digital goods are often exclusive in nature and unavailable from competing vendors.

SIZE OF THE PROBLEM

Ethoca's estimate is that 1.9 Billion CNP purchases – representing USD $145.9 Billion in sales – are declined each year globally.[1] It's critical to clarify that this number represents all declines (i.e., fraud risk, insufficient funds, lost/stolen, etc.), not just declines due to the suspicion of fraud. Analyst firm Aite recently published estimates on a subset of these overall declines – 'false declines' – that are due to overcompensation by card issuers' fraud systems. Aite estimates that in 2016 in the U.S., false declines are at USD $264 Billion and trending to USD $331 Billion in 2018 (*Chargebacks and False Declines, August 2016,* Card Present and Card Not Present combined).

Javelin research estimates that in 2014 U.S. card issuers falsely rejected USD $118 Billion in transactions (also Card Present and Card Not Present combined) due to suspicion of fraud, compared to USD $9 billion in actual fraud – that's a ratio of 13 to one. In direct response, 39% of cardholders will abandon a card post decline, and 25% will move a declined card to the back of the wallet (*Future Proofing Card Authorization, August 2015*). This is a card issuer's worst nightmare: not only is their card no longer first in the cardholder's wallet – it's potentially at the very back.

This is a material impact in a highly competitive space of card issuers vying for 'first in wallet' position with cardholders. Based on Ethoca's overall CNP decline estimate (1.9 Billion transactions) and Javelin's back-of-wallet estimate (25%), we can extrapolate that globally 475 Million unique cardholders change payment methods and potentially move their card to the back of the wallet. Cardholder lifetime value is estimated to be between USD $3,600 - $48,000[2] (inclusive of revenue streams like interchange fees), suggesting the overall financial impact of the decline problem goes well beyond lost merchant sales.

In our research, it is clear the majority of declines are actually caused by cardholders having insufficient funds. The NY Fed Bank Quarterly Report states one in 20 cardholders is at least 30 days late on their credit card and 8.38% of all delinquent cardholders are 90+ days late (*Source: NY Fed Bank Quarterly Report on Household Debt and Credit in 2015*). Given these levels of late payment and delinquency, it should be no surprise that a significant percentage of declines are related to insufficient funds.

[1] *Total volume of global eCommerce estimated at $3.5 trillion by eMarketer, multiplied by 4% of transactions declined annually.*

[2] *https://www.quora.com/What-is-the-customer-lifetime-value-for-MasterCard*

1.9 BILLION PURCHASES, REPRESENTING USD $145.9 BILLION IN SALES, ARE DECLINED A YEAR.

DIGITAL GOODS VS PHYSICAL GOODS – WHAT'S BEHIND THE DIFFERENCE IN DECLINE RATES

Transaction decline rates vary considerably between the physical and digital channels. While physical goods merchants are often in the range of 3-4%, many of Ethoca's digital goods customers report decline rates in the double digits (greater than 15%). As we studied this problem, comparing digital goods to physical goods, we saw that in digital goods it was not unusual for a declined cardholder to keep trying to complete the transaction.

Ethoca's theory is that digital goods customers keep retrying their purchase due to the relative exclusivity of the media, game or service. In many cases, the digital goods vendor is the only available source, compared to physical goods where cardholders have many choices for the same merchandise. For example, a customer may want to watch a new, exclusive movie release using their preferred online media provider. When they are first declined, they will continue to try to get the transaction approved, since the movie is not available elsewhere. Another possible factor here is 'stickiness': many digital goods vendors offer unique games and digital experiences (often cemented through social networking interaction) that drive extremely high user loyalty and addictiveness. The result is many declined customers will return again and again until their purchase is successful.

So what's driving this apparent gap in authorization approvals between digital goods and physical goods transactions? To get to the root of this problem, Ethoca looked closely at both digital goods and physical goods decline rates from a different perspective – by unique cardholder. We measured 'Do Not Honour' declines in these segments and found that overall decline rates were similar. Based on pure transaction authorization attempts, the digital channel sees much higher rates in the range reported by our customers (> 15%), but it's critical to remember that each of these declines does not necessarily result in a lost sale for the merchant.

In the data set we analyzed, we found that the decline rate for one particular digital goods merchant, when measured by unique cardholder, was approximately 4%. That's very consistent with levels in the physical goods channel. Once again, this finding is consistent with our view that customers in the digital channel exhibit unique purchase behaviours. It also suggests that the risk of fraud in the digital channel cannot be accurately assessed by looking solely at gross transaction decline rates.

DECLINE RATES FOR PHYSICAL GOODS MERCHANTS ARE OFTEN IN THE RANGE OF 3-4%, AND CAN BE GREATER THAN 15% FOR DIGITAL GOODS.

MANY DIGITAL GOODS MERCHANTS REPORT FRIENDLY FRAUD RATES BETWEEN 60 AND 90%

NOT SO FRIENDLY FRAUD

In addition to repeat authorization attempts by customers in the digital channel, another important dimension is the growing problem of friendly fraud. Many digital goods merchants are routinely reporting friendly fraud rates between 60 and 90%. What is especially alarming here is the shift in customer behaviour: some merchants are now characterizing this trend not as a 'fraud' problem, but as a 'liar' problem. In part fuelled by the global regulatory environment (Regulations E & Z in the U.S., Financial Ombudsman Service in UK and Payment Services Directive in Europe, to name just four), cardholders have learned it is easier to contact the bank first and avoid responsibility for the transaction – without penalty or consequences.

Along with higher reported decline rates in the digital channel, actual fraud rates can be four to six times higher as well. Ethoca's belief is that a significant portion of these declines are ultimately a by-product of friendly fraud. In some instances, these are innocent cases where customers simply do not recognize the purchase on their accounts (minors or a spouse in the household making purchases on the account), but our merchants are reporting that this problem is becoming increasingly hostile in nature. Customers easily rationalize this behaviour by perceiving their abuses as a 'victimless crime'. Digital goods have a perception of little tangible value when compared to physical goods, so an increasing number of customers show little remorse for 'gaming the system' to their benefit. To the contrary, it appears to further embolden them.

Ultimately, the friendly fraud transactions were legitimate customer purchases now miscoded as fraud – an outcome that has a negative ripple effect on authorization strategies across the value chain. Because friendly fraud transactions are typically coded as fraud, fraud models and rules are tuned incorrectly, resulting in unnecessarily high declines. To cope with the increasing volume of fraud reports and related costs, card issuers are compelled to decline more, but this defensive strategy is based on inaccurate and incomplete data. The inevitable result is higher false positives – more good cardholders getting turned away.

IF AT FIRST YOU DON'T SUCCEED, TRY, AND TRY AGAIN

What's unclear, in cases where customers will continue to retry transactions after receiving a decline, is the cumulative impact of these ongoing declines and when customer experience reaches a breaking point. With potentially half of all declined customers either abandoning a purchase or replacing their preferred card with a competitor's card, the loss in ecommerce revenue and negative customer experience has both card issuers and merchants deeply concerned about a mounting transaction acceptance crisis.

WHY CARDHOLDERS ARE DECLINED – LOOKING UNDER THE COVERS OF 'DO NOT HONOUR'

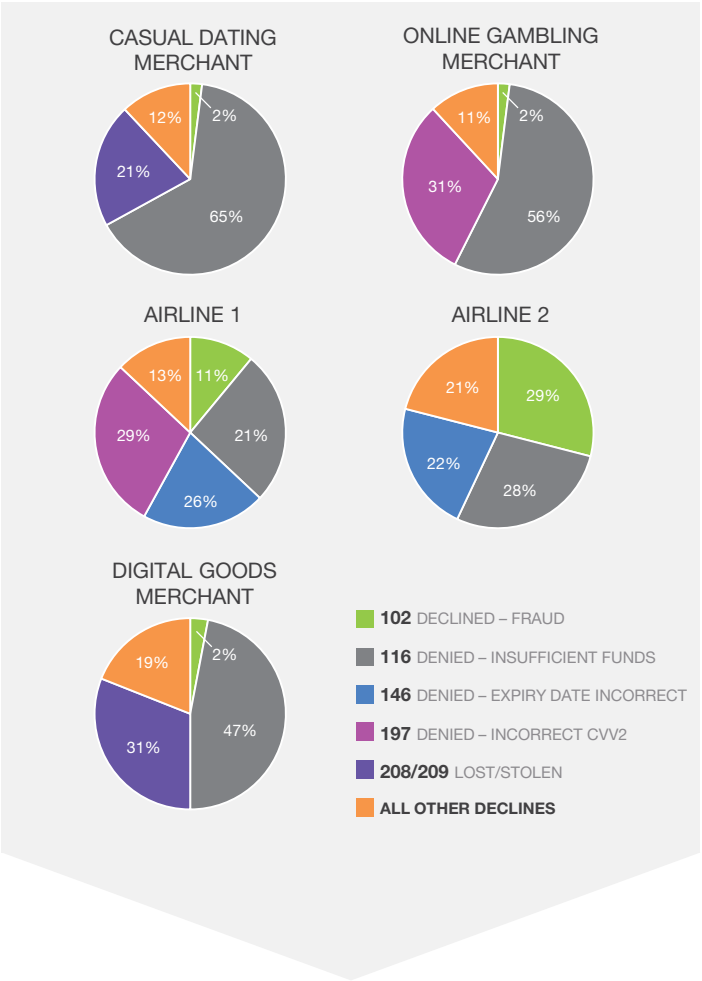
44.4% OF DECLINES ARE DUE TO INSUFFICIENT FUNDS.

A part of the problem around cardholder acceptance is that authorization declines from a merchant's bank (the acquirer) often come back as 'DO NOT HONOUR' to the merchant. This decline reason code message received by the merchant indicates that the card issuing bank has rejected the transaction. It is often interpreted by the merchant that the reason for this rejection is that the issuer has a suspicion of fraud, but the reality is much more nuanced. Merchants are confused by this information and can't understand why a good customer who they have done business with for years – same merchant, same card and sometimes even same dollar amount – are all of a sudden declined due to what they believe to be suspicion of fraud.

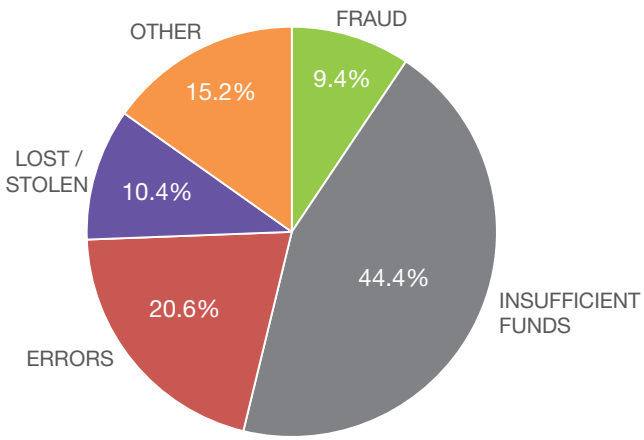
We partnered with one of our card issuing bank customers to do a study with five of Ethoca's merchant customers to reveal what the 'DO NOT HONOUR' reason code truly represents.

As you can see from the results, the number one reason for declined transactions is that the cardholder no longer has sufficient funds in their account or available credit on their card to pay for the goods they are attempting to purchase. What's notable in these results is the sheer diversity in the distribution of decline reasons across different merchant categories. While there is a perception that fraud is the number one reason a customer is declined, for the digital channel customers in our study declines due to suspicion of fraud was only 2-3%.

An interesting outlier here was the airline category, where declines due to suspicion of fraud are markedly higher – 11% and 29% for the two major airline customers that participated. This is unsurprising given the typical size of air travel transactions and relatively high use of 3D Secure. Faced with increased exposure on airline transactions, it's not uncommon for card issuers to decline more to limit potentially large losses for which they are either liable or incur significant expense to recover.



AVERAGE MERCHANT DECLINE RESULTS



52% OF THE ORDERS THE MERCHANT THOUGHT WERE FRAUD, TURNED OUT TO BE GOOD ORDERS THEY COULD HAVE SUCCESSFULLY FULFILLED.

WHY CARDHOLDERS ARE DECLINED

(CONTINUED FROM P.7)

During our research, we asked several card issuers why they did not return authorization decline reason codes that reflected the actual reason for the decline. First, card issuers are protecting their cardholders' privacy. They are reluctant to share with merchants that the cardholder is behind on paying their bill, maxed out on their credit card or have lost their card. The second reason is that if the purchases were made by fraudsters, providing this level of decline information could potentially allow fraudsters to reverse engineer the fraud system and learn how to bypass the fraud checks.

Merchants do something very similar when they are declining a transaction due to suspicion of fraud. In this case, typically the response back to the customer on the website is to recommend calling into the customer service center to complete the order, allowing additional fraud checks to be completed while minimizing the opportunity for a bad customer experience.

MERCHANT DECLINES COMPOUND THE PROBLEM

The false decline problem has two faces, as both card issuers and merchants face high operational costs when it comes to preventing and recovering fraud losses. It's important to recognize that card issuer authorization strategies are just one key dimension of the decline picture. Merchants operate in their own silo and perform an entirely different set of fraud checks. The reality is that there are two distinct opportunities for every transaction to be declined and every customer to be turned away. Merchants also wrongly reject a large number of transactions due to their suspicion of fraud.

At Ethoca we completed a pilot with major merchants and a few major issuers and discovered that 52% of the orders the merchant thought were fraud, turned out to be good orders they could have successfully fulfilled. When the merchant declines an order that is actually good, this costs the merchant lost revenue and potentially a lost customer. In addition to a bad cardholder experience, many times the customer calls their card issuer to ask why the card was declined. The card issuer often does not have insight into why a merchant would have declined an order, resulting in increased frustration for the cardholder. It also increases the issuer's overall call volume, adding operating expense on top of already overburdened call centers.

ON THE FRONT LINES OF MERCHANT DECLINES

To better understand what is happening today, Ethoca embarked on a research project shopping at 22 merchants ecommerce websites to evaluate how declines are currently handled by the merchants.

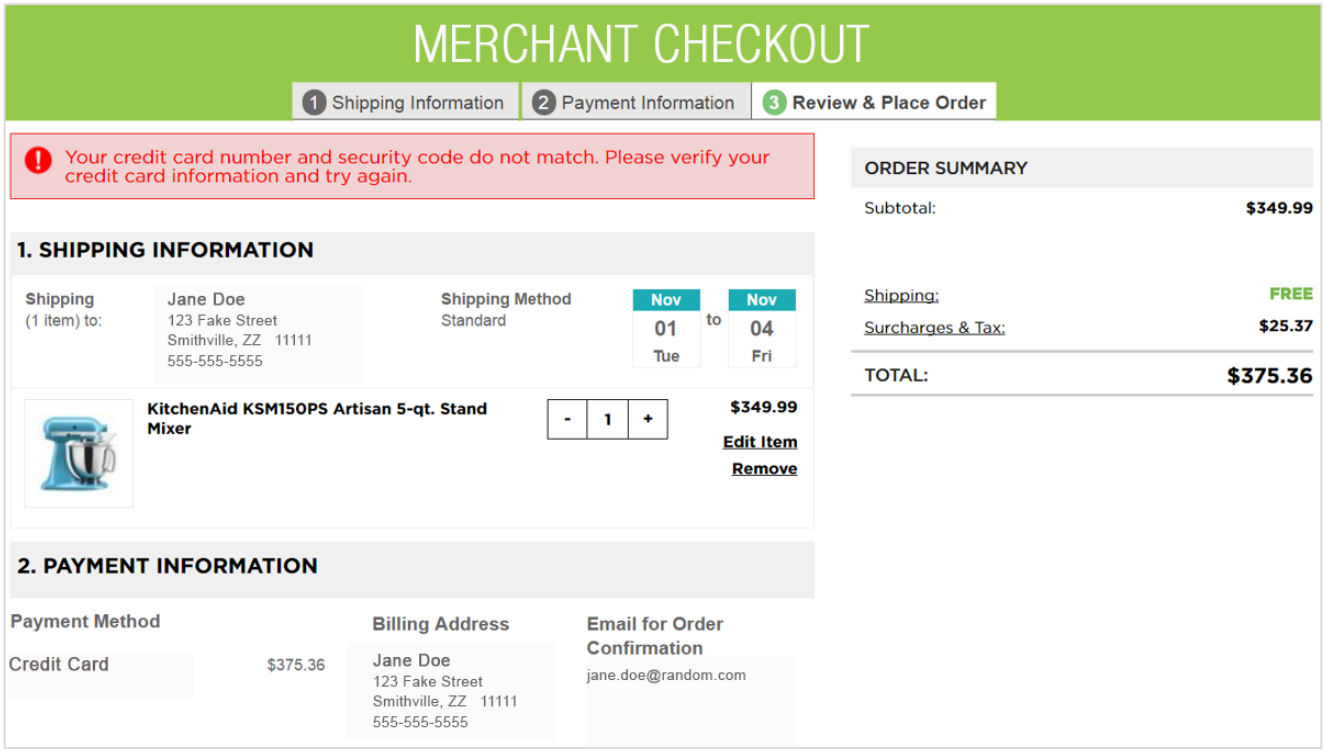
During the research, we attempted to place orders with the following scenarios: A credit card that was reported lost to the bank; a credit card that was cancelled due to fraud; and knowingly typing in the wrong expiration date.

Scenario	Results	Observations
Credit card that was reported lost to the bank	20 websites provided an immediate, vague response at checkout stating to check the information entered. Two websites approved the order and later sent emails stating the order was declined	Very confusing experience as the cardholder has no idea why the card was declined.
Credit card that was cancelled due to fraud	20 merchants provided an immediate, vague response at checkout stating to check the information entered and try again. Three of the 20 suggested in the error message that the cardholder try another method of payment. Two merchants approved the order, but later sent an email stating it was declined, with no specific reason why.	Again, we see a variety of responses from merchants. While several of the merchants suggested the customer try another form of payment, others approved the order initially with subsequent declines by email. Recommendations for retrying transactions were vague and non-specific.
Incorrect Expiration Date*	Six merchants provided vague responses that there was a problem and to please try again. Three of the six suggested in the error message that the cardholder try another method of payment. Two merchants approved the order, but later sent an email stating it was declined with no specific reason why.	The nature of different merchant responses again suggests there is a disconnect in the communication of decline reasons from card issuers: merchants' interpretation of these decline reasons results in unclear and often unhelpful messages back to the customer.

**Incorrect Expiration Date: We suspended the test for incorrect expiration date after we had them tested at 8 websites. In one case the order was declined at checkout. However, after several days, the item ordered arrived regardless.*

It turns out, merchants actually had internal staff working with the issuers to get the order to go through. As a cardholder, we received no indication that the order went through, other than the product arrived.

***We choose not to test incorrect CVV for this research as we were made aware that some merchants will process orders even if the CVV fails.*



In this screen shot (with personal data anonymized, but sourced from a large online retailer), we had typed in an incorrect expiration date and you can see that the error message provided to the customer tells them to check their credit card number and security code – it says nothing about the expiration date. Ethoca believes that this confusing authorization feedback loop is driven by the bundling of declines under the aggregate 'DO NOT HONOUR' reason code.

Once again, we see that a process ultimately designed to protect the cardholder (not disclosing detailed decline reasons due to cardholder privacy considerations), contributes to an unintended negative experience at merchant checkout.

NEW LEARNING ON BUFS (BACK-UP FUNDING SOURCE)

During our most recent Ethoca Card Issuer & Merchant Working Group in September 2016, we discussed how best to approach the specific authorization decline messages and out of those discussions came a new twist on an old business process.

In the card present recurring subscription industry (i.e. gym memberships), merchants have used a process referred to as a Back-Up Funding Source (BUFS). The BUFS encourages and sometimes even requires a cardholder to put in more than one funding source (credit cards, DDA accounts, etc.) when setting up a new account.

A few of the merchants in our working group were already testing the use of BUFS when transactions are declined and we discussed many different ways this could be implemented. In some cases, merchants will utilize a secondary funding source when a primary source fails, document it, notify the customer and provide clear instructions for a back-up funding source. Others may default to a bank account, even when a preferred payment method is a credit card.

Overall, we see a mix of these approaches: some are highly communicative with customers to ensure they consent to use of a BUFS, while others take a more aggressive approach and default to another payment instrument on file automatically. In the latter case, this approach comes with increased dispute and chargeback risk.

CONCLUSION

Ethoca's vision is that ecommerce should simply be about commerce. What our investigation into the growing false declines problem demonstrates is that the way card issuers and merchants communicate today is fraught with challenges and lost opportunities. Both parties are squarely focused on doing the right things to stop growing CNP fraud losses, but without a reliable way to share intelligence and a broader set of data, one of the unfortunate outcomes is good customers unduly penalized by false declines.

One thing is crystal clear: increasing transaction acceptance across the board is going to take an orchestrated transformation of the existing payments value chain. The CNP ecosystem today functions in silos, yet ironically the relationship between card issuers, merchants and customers/cardholders has never been more intertwined. The good news is that the problems and barriers that prevent both parties from realizing full value from the CNP opportunity can be solved through collaboration.

Ethoca has several pilots underway with our card issuer and merchant customers, and card acceptance is at the top of our list. Please contact us at innovation@ethoca.com for more information on participation and to secure your place.

ABOUT ETHOCA

Ethoca is the leading, global provider of collaboration-based technology that enables card issuers, ecommerce merchants and online businesses to increase card acceptance, stop more fraud, recover lost revenue and eliminate chargebacks from both fraud and customer service disputes.

Through the Ethoca Network – the first and only of its kind in the industry – we are closing the information gap between card issuers and merchants. This unique capability makes fraud and customer dispute insight available and actionable in real time.

Our suite of services delivers significant revenue growth and cost saving opportunities for thousands of merchants and hundreds of issuers across the globe. This includes the world's biggest ecommerce brands and largest banks.

To find out more, please visit us online at **www.ethoca.com** or contact us at **sales@ethoca.com**