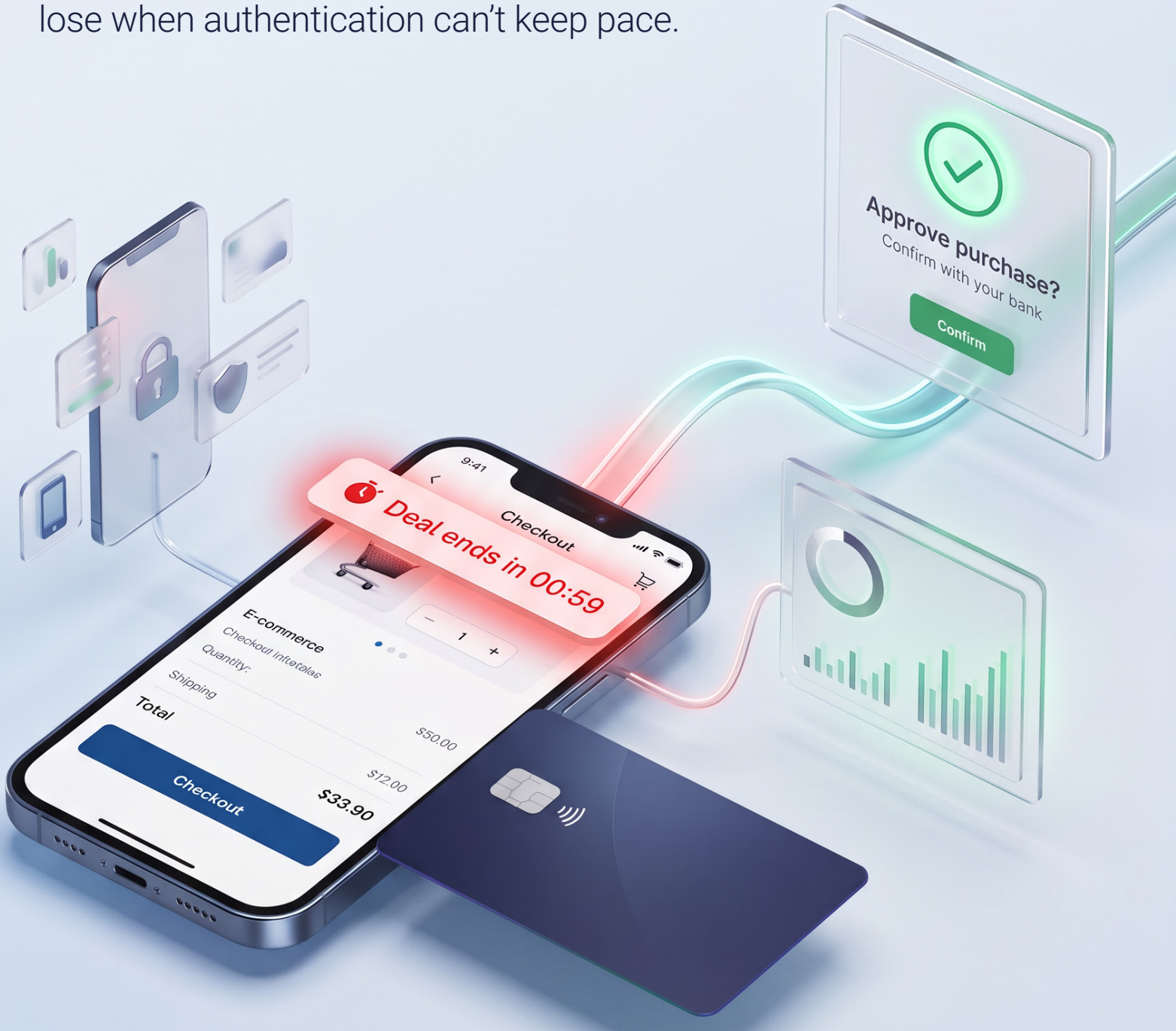
entersekt

Safe, sound, and abandoned: **The holiday friction paradox**

What U.S. holiday online shoppers expect from their bank at checkout, and what card issuers lose when authentication can't keep pace.





Executive summary

Holiday online shoppers *want* their bank protecting the checkout—they just won't *wait* for it

In a survey of 1,026 U.S. holiday online shoppers, 77.8% said they would rather their bank pause and confirm a legitimate purchase during a major online sale than let payments through unchecked. Yet 39.2% abandoned an online purchase in the past year because their bank's approval process took too long or was too complicated. Another 24% came close.

What shoppers want



77.8% prefer the bank to confirm

What they get



39.2% abandoned over a slow approval

That gap is the holiday friction paradox.

Card issuers already hold the trust they need: 48.4% of shoppers feel reassured when their bank pauses a $500+ purchase, while only 11.8% feel annoyed. And 33.5% feel uneasy when a high-value purchase on an unfamiliar site goes through with no check at all. Shoppers are asking for better security: fast, reliable, and aimed at the right transactions.

What shoppers think about friction



48.4% feel reassured by a pause



33.5% feel uneasy with no check

The failures are specific and measurable. More than half of shoppers (54.4%) won't wait longer than a minute for a confirmation step before abandoning or switching cards. Four in 10 (40%) approved a purchase in their banking app, only to return to a checkout that had stalled, failed, or reset. Another 39.5% had their bank decline a purchase they were genuinely trying to make. Meanwhile, the channel shoppers trust most is the one fraudsters exploit best: 41.5% prefer an SMS code, and 17.3% have already responded to a holiday message impersonating their bank.

Taken together, 56.5% of shoppers experienced at least one of these failures in the past 12 months: abandoning over a slow approval, a broken app handoff, or a false decline. For issuers, every one is a lost transaction, a card moved to the back of the wallet, and a dent in trust that took years to build.

Cyber Monday success for issuers depends on knowing, when to step aside, and how to confirm a purchase in seconds without sending the shopper anywhere.

Why they drop off



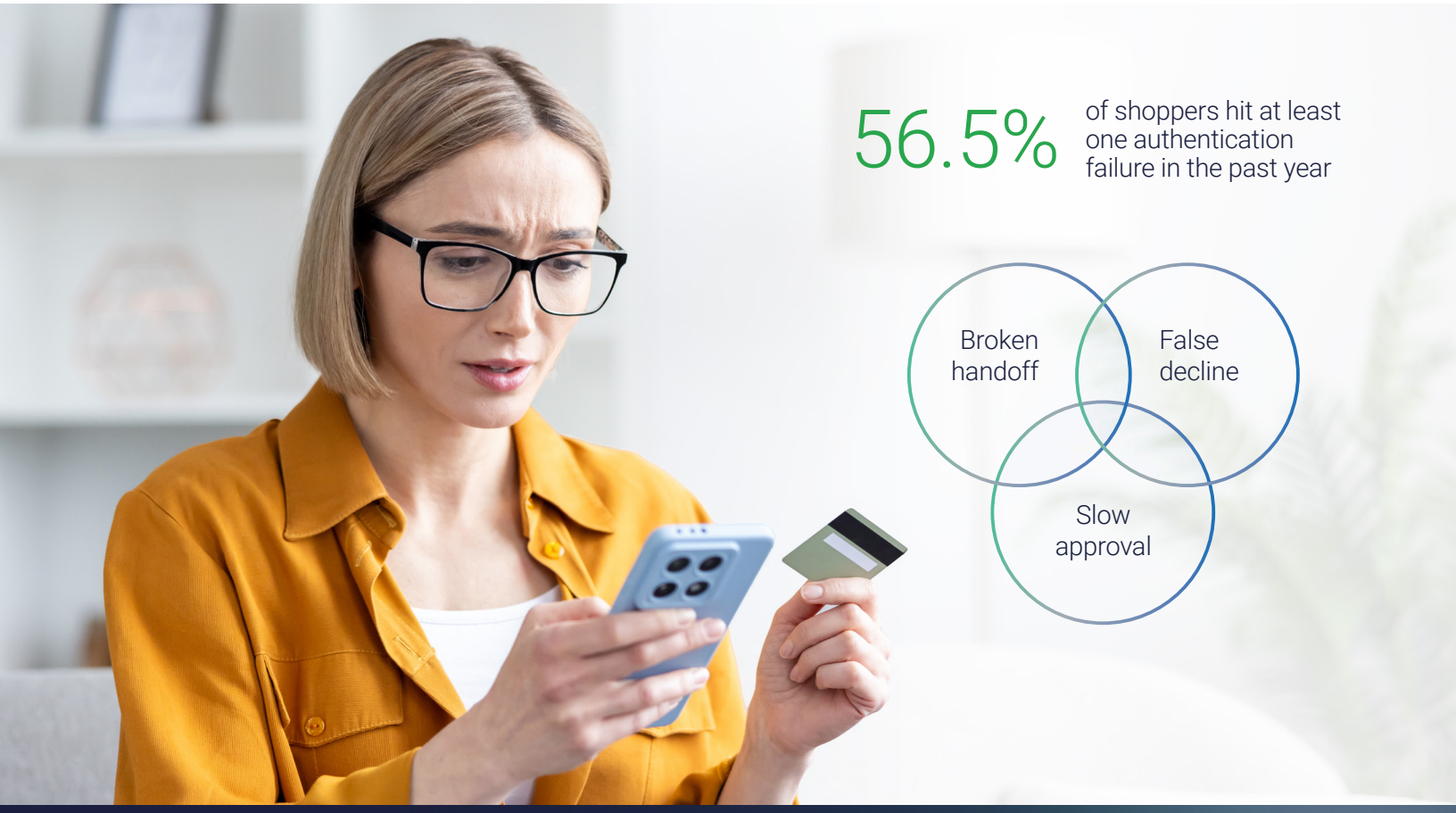
54.4% won't wait past a minute



40% broken app handoff



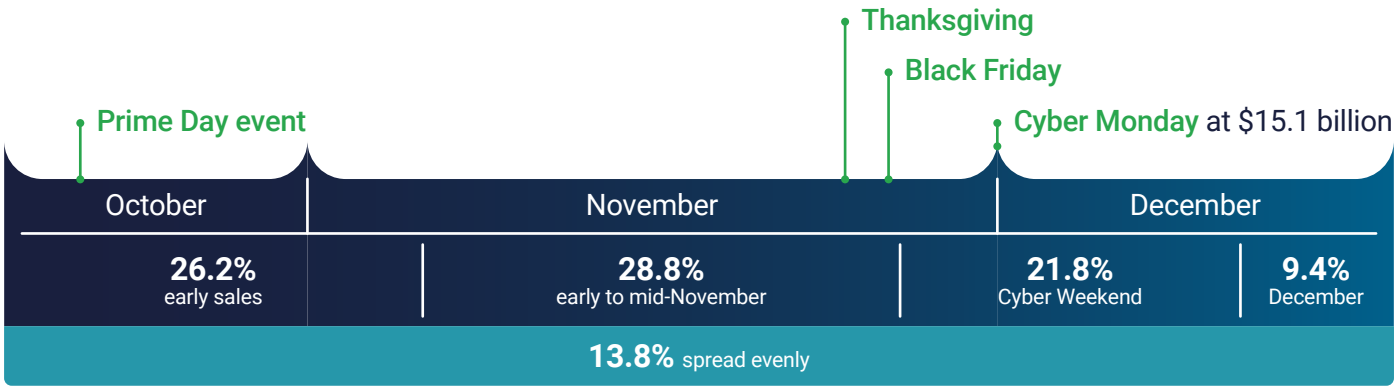
39.5% false decline



56.5% of shoppers hit at least one authentication failure in the past year

Cyber Monday is the biggest online shopping day of the year, and every second at checkout counts

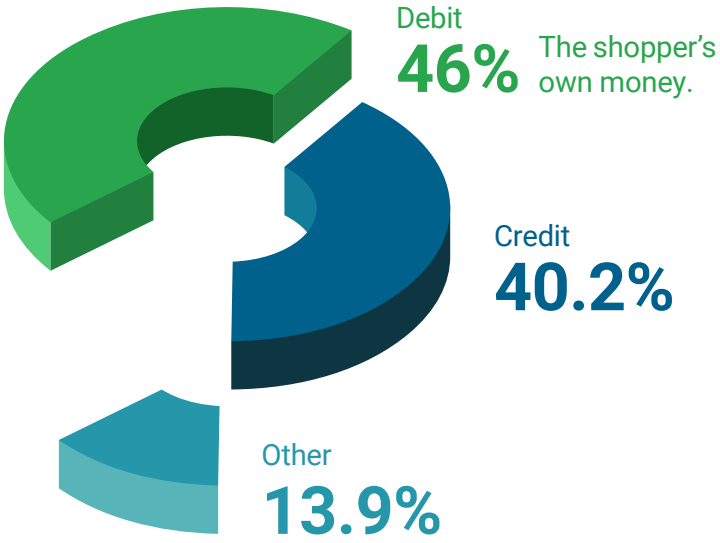
Adobe expects U.S. shoppers to spend $275.1 billion online this holiday season, with Cyber Week driving $47.5 billion and Cyber Monday alone topping $15 billion for the first time. Last year, during Cyber Monday's peak evening hours, shoppers spent $16 million every minute. Most of it now flows through a phone: Adobe forecasts mobile will account for 57.4% of holiday online spend.



That is the environment card issuers authenticate in. Deals expire on a countdown. Shoppers are buying from merchants they found on social media an hour ago. Carts are bigger, purchases are out of pattern, and fraudsters know it.

The shoppers in our survey are already deep into the season. More than half (55%) plan to finish most of their gift buying before Thanksgiving week, and another 21.8% will do most of it across Cyber Weekend itself. Their card of choice matters too. Debit (46%) has overtaken credit (40.2%) as the most-used online payment method, which means many holiday purchases draw directly on a checking account. When something goes wrong, it is the shopper's own money on the line. Buy now, pay later barely registers as a primary method, at 1.3%.

More people are using their own money



To understand how these shoppers weigh speed against security at checkout, Entersekt surveyed 1,026 U.S. adults who plan to make holiday purchases online. We asked how long they will wait for their bank, what makes them abandon, how they react when a purchase is paused, and what has already gone wrong.

The answers point to a single tension. Shoppers want their bank watching. They also want the deal. Card issuers that can deliver both, quickly and invisibly where possible, will own the moment that matters most.

Continue reading to understand the four key findings uncovered in our research, and what they mean for your financial institution.



The issuer dilemma: shoppers want security, but legacy authentication kills sales

The industry has long treated security and conversion as a trade-off. Shoppers don't see it that way.

Asked to choose, 77.8% of holiday shoppers would rather their bank pause and confirm a legitimate purchase during a major sale, even at the cost of a few seconds, than let payments through and risk a fraudulent charge. Only 3% say they want no confirmation step under any circumstances.

The emotional response is just as clear. When a bank pauses a $500+ holiday purchase to confirm it, 48.4% of shoppers feel reassured that their bank is actively keeping them safe. Just 11.8% feel annoyed.

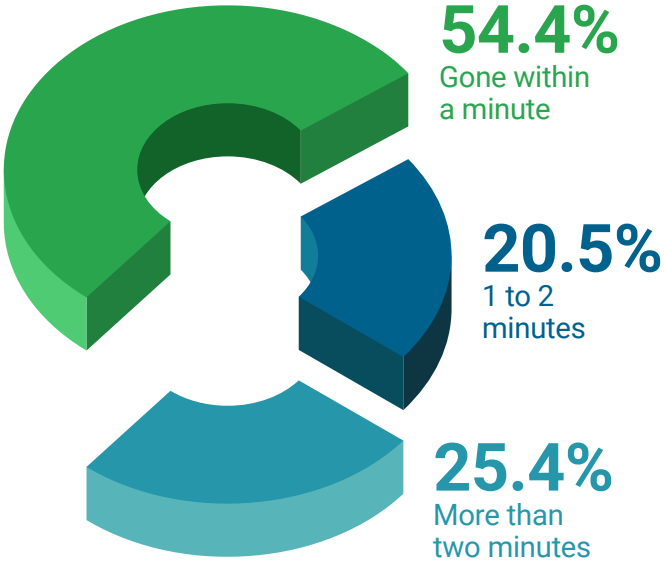
Flip the scenario and the unease shows up: a third (33.5%) would feel uneasy if a high-value purchase on an unfamiliar site went through instantly, wondering whether their bank was watching at all.

Protection on a stopwatch

That goodwill comes with a time limit. More than half of shoppers (54.4%) will not wait longer than a minute for a bank confirmation step during a limited-time sale before abandoning the purchase or reaching for another card. Nearly three in 10 (29.4%) give it 30 seconds or less.

The consequences are already visible. In the past 12 months, 39.2% of shoppers abandoned or exited an online purchase because their bank's approval process took too long or was too complicated, and 16.5% did so more than once. Another 24% came close. Only 36.8% say they always complete the approval process.

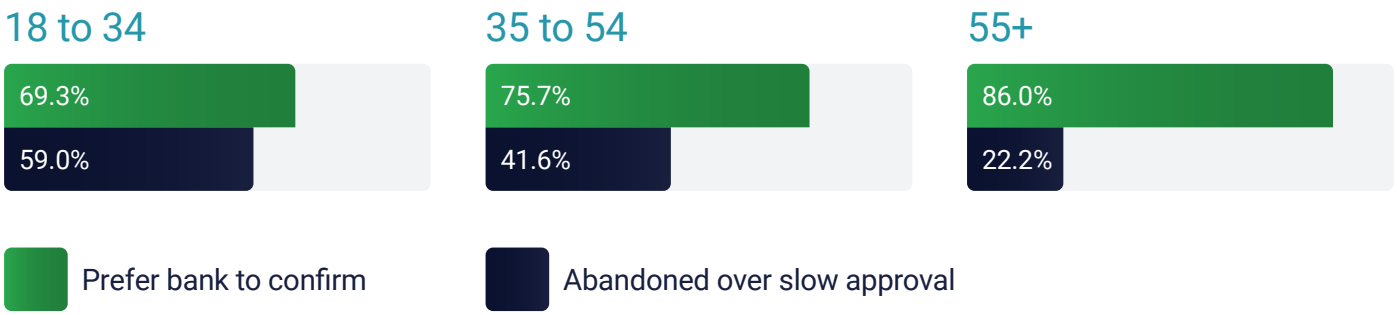
The most telling number sits inside that group. Even among shoppers who have abandoned a purchase over a slow approval, 67.7% still prefer that their bank confirm purchases during a sale. What they walked away from was a process that couldn't keep up.



A generational fault line

Younger shoppers feel the friction most. Among 18- to 34-year-olds, 59% abandoned a purchase over a slow or complicated approval in the past year, compared with 41.6% of 35- to 54-year-olds and 22.2% of those 55 and older. Yet 69.3% of the youngest group still want their bank to confirm purchases during a sale.

The appetite for protection holds across every age group. The tolerance for delay does not.



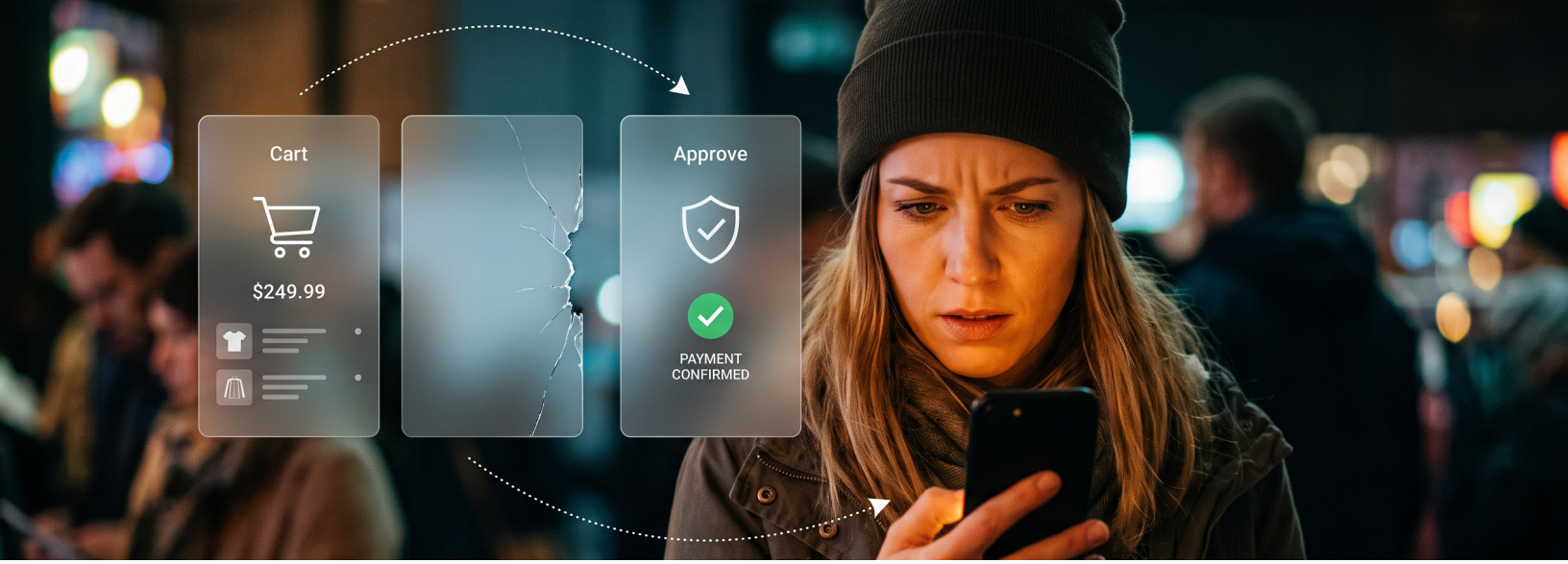
Issuer takeaway: add time to authenticate to your conversion metrics

Shoppers have handed issuers a mandate to intervene. What they haven't granted is unlimited time. For card issuers, three things follow.

First, time to authenticate should sit alongside approval rates, checkout completion, and fraud losses as a core conversion metric. Our data sets the bar: 29.4% of shoppers give a confirmation step 30 seconds or less, and 54.4% are gone within a minute. Every confirmation step should have a time budget measured in seconds, tracked through Cyber Week, with abandonment after a challenge counted as a lost authorization, not a neutral outcome.

Second, the fastest step-up is the one that never happens. Risk-based authentication (RBA) through EMV 3-D Secure lets issuers approve the large majority of low-risk purchases frictionlessly, using device, behavioral, and transaction signals, and reserve a visible challenge for the transactions that genuinely warrant it.

Third, when a challenge is warranted, shoppers want to see it. A fast, recognizable confirmation on a high-value or unfamiliar purchase builds the reassurance 48.4% of shoppers already feel. Issuers that keep that moment short will turn security into a reason to keep their card at the top of the wallet.



Finding 2 | 40.0% experienced a broken handoff

The “app-switching abyss” is e-commerce’s silent killer

The shopper did everything right. The purchase still failed.

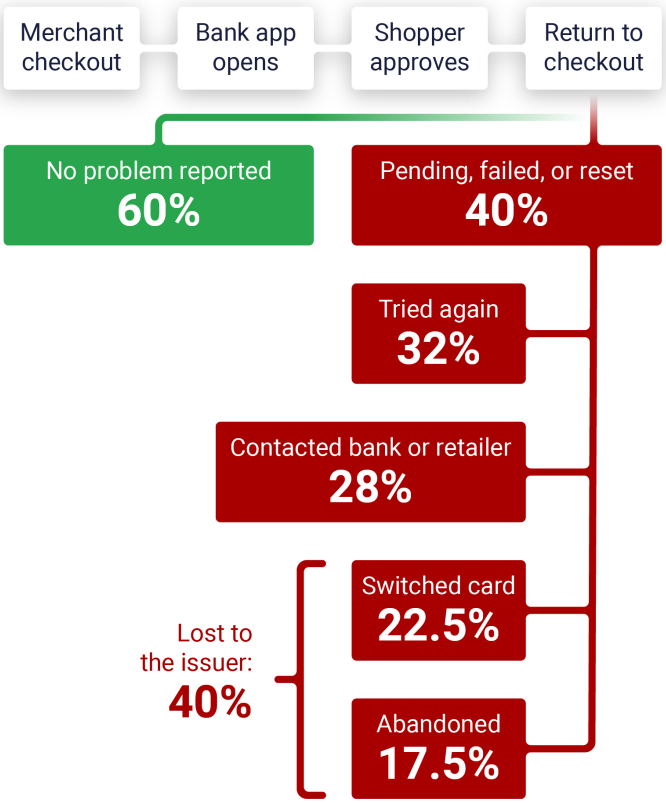
Many issuers have moved checkout confirmation away from SMS codes and into their mobile banking app. It is a stronger approach: the approval is bound to a known device and app, and it is harder to intercept. But it introduces a new point of failure. The shopper leaves the merchant’s checkout, opens the banking app, approves the purchase, and then has to swipe back to the shopping cart. On a phone, in the middle of a flash sale, that round trip—the handoff from banking app to checkout—can break.

Four in 10 journeys have crashed

In the past 12 months, 40% of shoppers approved an online purchase in their bank’s app, returned to the retailer’s checkout, and found the order still pending, failed, or requiring them to start again. For 15%, it happened multiple times.

What happened next is where the cost lands. Of those affected, 32.1% tried the purchase again and 28% contacted their bank or the retailer. The rest were lost to the issuer outright: 22.4% switched to a different payment method and 17.5% abandoned the purchase entirely. In total, roughly four in 10 shoppers who hit a broken handoff took their business off that card.

Shoppers know exactly what this feels like. When asked which checkout issue would most likely make them abandon a Cyber Monday purchase, 22.9% picked an app approval that doesn’t register at checkout. Only a false decline ranked higher.



Shoppers burned by a broken handoff abandon four times as often

A broken handoff is what happens when that round trip fails: the shopper approves the purchase in their banking app, but the merchant's checkout never registers it. Shoppers who have been through one are also far more likely to give up on their bank's approval process altogether.

Hit a broken handoff

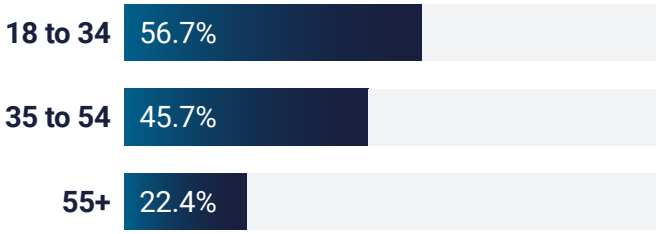


Never hit one



Among shoppers who hit a broken handoff, 72% also abandoned a purchase over a slow or complicated bank approval in the past year, compared with 17.4% of those who didn't. The more often it happened, the higher that figure climbs: 66.4% for shoppers who hit one once or twice, and 81.2% for those who hit them repeatedly. A failed handoff rarely costs just one sale.

The problem is concentrated among the most mobile shoppers. More than half (56.7%) of 18- to 34-year-olds have experienced a broken handoff, compared with 22.4% of shoppers 55 and older. By institution type, it was reported most often by customers of community banks (49.5%) and regional banks (45.3%).



All of this plays out on a single screen. Adobe reports that 57.5% of Cyber Monday 2025 online sales came through a mobile device, up from 41.4% five years earlier. The more checkout moves to the phone, the more often shoppers are asked to juggle a browser, a merchant app, and a banking app at the moment of purchase.

Issuer takeaway: own the return trip, not just the approval

Moving away from SMS was the right call. But the job isn't finished until the approval reliably completes the purchase.

For card issuers, success should be measured at the merchant, not in the app. An approval that never reaches checkout is a failed checkout experience, a likely lost transaction, and, for 28% of affected shoppers, a support contact. Issuers should track end-to-end completion through their 3-D Secure access control server (ACS), not only in-app approval rates, and treat handoff failures during peak events as a priority incident.

The longer-term fix is to stop sending shoppers away. Device-bound passkeys and in-browser biometric authentication let the shopper confirm a purchase with Face ID or a fingerprint without leaving the merchant's page, while keeping the phishing resistance that made app-based approval attractive in the first place. Visa and Mastercard have both launched payment passkey services built on these standards.

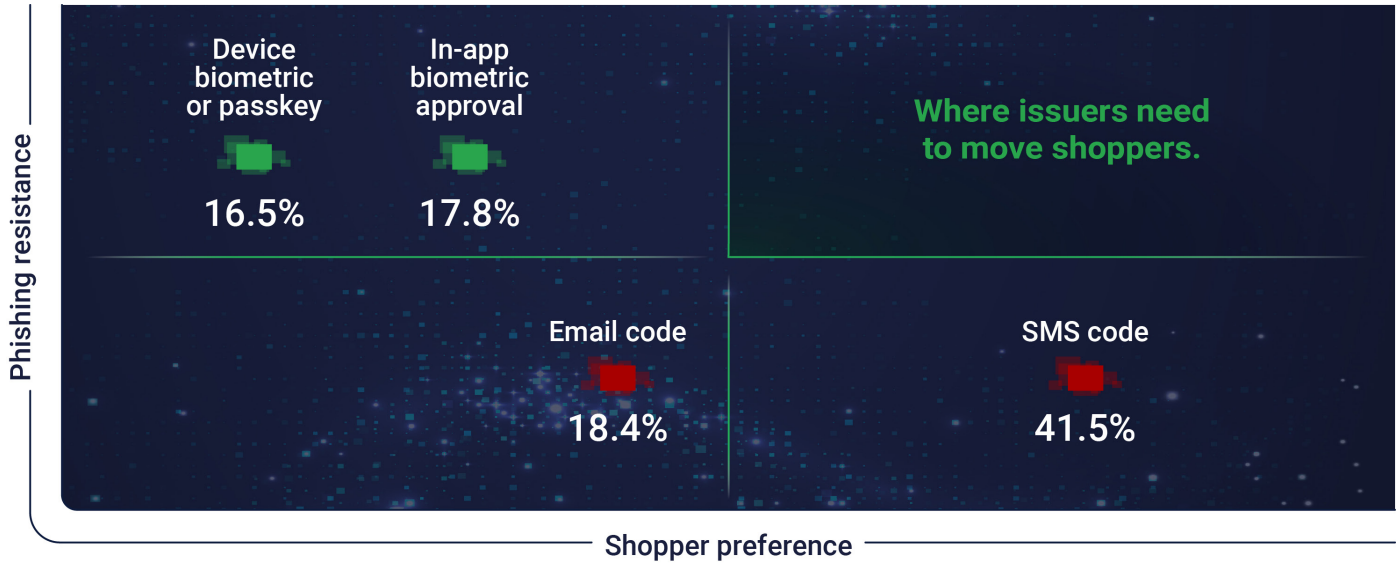
Where an app approval remains the right step, it should be designed for the return trip: resilient to timeouts, clear about status, and fast enough that the merchant's session is still waiting when the shopper comes back.

The SMS phishing trap: high trust, extreme risk

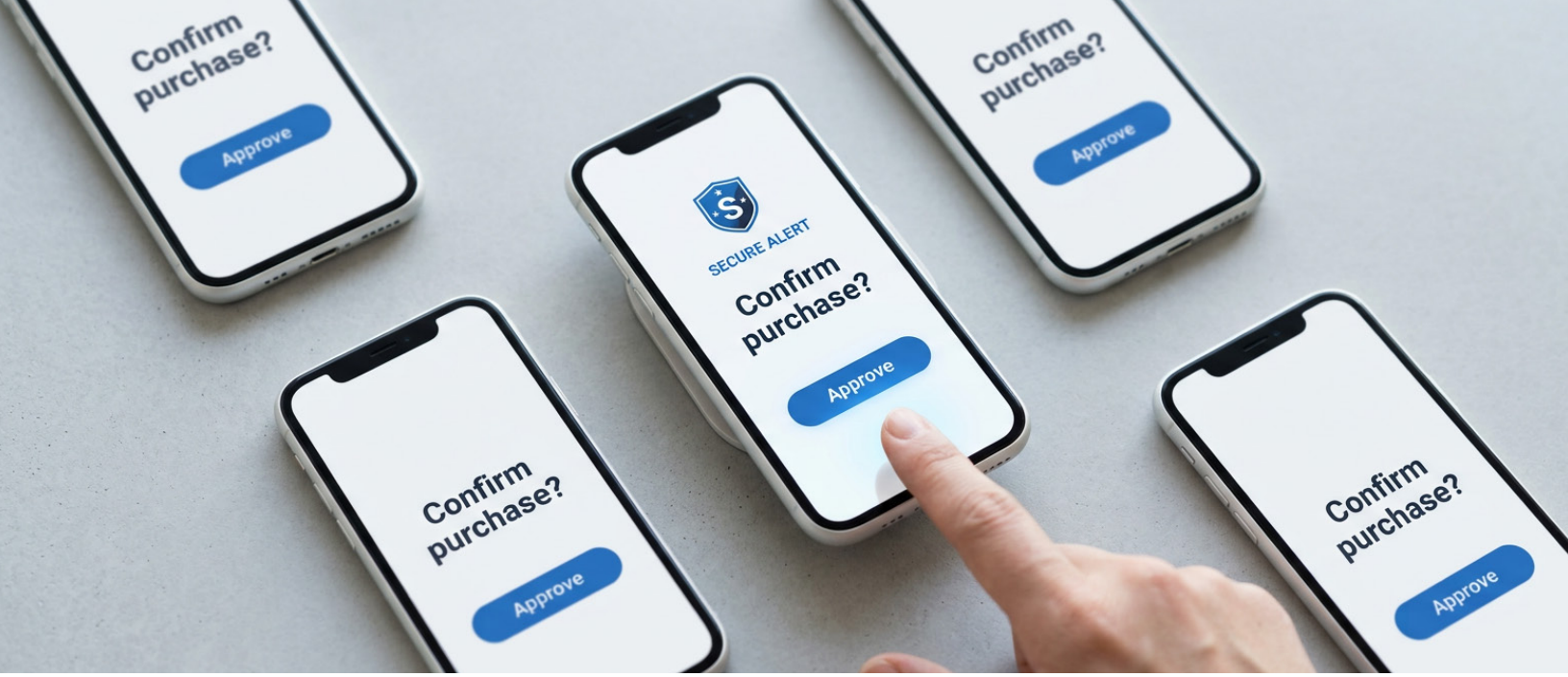
Shoppers trust the text message because their banks taught them to. Fraudsters noticed.

For more than a decade, the one-time code sent by text has been the default way U.S. banks confirm a card-not-present (CNP) purchase. It worked well enough to become a habit. Today, when asked which confirmation method they trust and prefer most at online checkout, 41.5% of shoppers choose an SMS code. Add email codes (18.4%) and 59.9% of shoppers still favor a one-time code of some kind. Only 34.3% prefer in-app or device-based confirmation: one-touch or biometric approval in the banking app (17.8%) or a biometric or passkey prompt on their device (16.5%).

That preference is about familiarity more than conviction. In Entersekt's The state of digital banking security survey earlier this year, only 18.2% of consumers rated a text-message code as the most secure verification method. Shoppers choose what they know.







The habit fraudsters exploit

The same habit that makes a code feel safe makes a fake request feel normal. During past holiday seasons, 38% of shoppers received a text, call, or email pretending to be their bank and asking them to confirm a purchase. Nearly one in five shoppers overall (17.3%) responded to it. Another 10.8% aren't sure whether they did.

$3.5 billion
lost to imposter scams in 2025

The national picture is consistent. The Federal Trade Commission reports that Americans lost $3.5 billion to imposter scams in 2025, nearly triple the 2020 figure, with bank impersonators responsible for the largest losses among business imposters. The FTC notes that some of the costliest schemes begin with a fake security alert, often styled as a message from the victim's bank.

And the damage runs both ways. When a real bank pauses a real purchase, 12.8% of shoppers say their first reaction is suspicion that the approval prompt itself might be a scam. Impersonation doesn't only steal money. It erodes the credibility of every legitimate confirmation that follows.



38% were targeted by a fake bank confirmation request. Nearly half of them took the bait.

- **17.3%** Responded
- **20.7%** Recognized the scam
- **10.8%** Not sure
- **51.2%** Not targeted

No one is immune

Younger shoppers are the most exposed: 25.3% of 18- to 34-year-olds have responded to a bank impersonation attempt, compared with 8.2% of shoppers 55 and older. Older shoppers, meanwhile, lean hardest on text codes, with 46.2% preferring SMS. Credit union members show the strongest attachment of all, at 51.5%.

Preference for a stronger method is no shield on its own. Shoppers who favor in-app or biometric confirmation were actually more likely to have responded to an impersonation attempt (25.9%) than those who favor SMS (12%), a gap that largely reflects their younger profile and higher exposure. The lesson for issuers is that protection has to be built into the method, not left to the shopper's judgment.

Issuer takeaway: retire the code without breaking the reassurance

Issuers can't switch SMS off before Cyber Monday, and they shouldn't try. Shoppers want a confirmation they recognize, and for 41.5% that is still a text. The goal is to keep the reassuring moment while removing the interceptable secret behind it.

That starts with enrollment. Every successful app approval, card activation, or login is a chance to register a device-bound passkey, so that SMS becomes the fallback rather than the default. Visa's own analysis found that biometric authentication carried roughly half the fraud rate of SMS one-time codes, and Mastercard has set a goal of eliminating one-time passwords and manual card entry by 2030. The networks are moving. Issuers that enroll customers now will be ready when they arrive.

Until then, every confirmation should be unmistakably genuine. Show the merchant and amount in the prompt, deliver it inside channels the shopper already trusts, and tell customers plainly what the bank will never ask them to do. The 12.8% who already suspect real prompts are a warning: in a season full of fake alerts, authenticity is part of the user experience.



False positives are a major Cyber Monday revenue leak

The most damaging checkout failure is a flat no to a good customer.

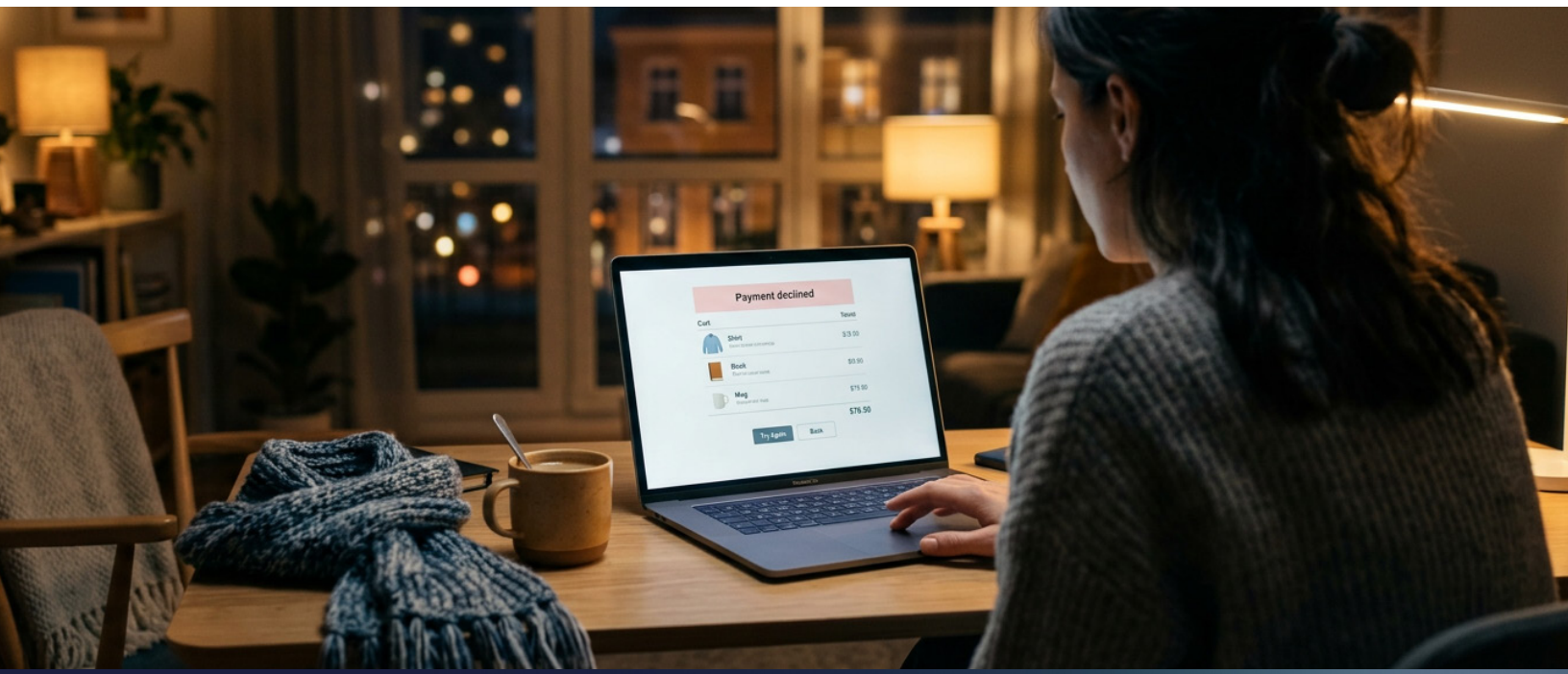
Holiday shopping is built to look unusual. Purchases are larger, merchants are unfamiliar, and buying happens in bursts at odd hours. Adobe found that during the 2025 season, the share of units sold in the most expensive product tiers rose 19% as discounts pulled shoppers toward bigger-ticket items. To a static fraud rule, much of that looks like risk.

The number one reason to walk away

In the past 12 months, 39.5% of shoppers had their bank decline an online purchase they were genuinely trying to make, and 16.5% experienced it more than once.

Shoppers rank it as the worst thing that can happen at checkout. Asked which issue would most likely make them abandon a Cyber Monday purchase, 26.9% chose a legitimate purchase being blocked or declined by their bank. That outranks a broken app handoff (22.9%), a slow checkout page (21.6%), and manual card entry (13.7%). Having to complete an extra security step ranks near the bottom, at 14.8%, and is considered only a “minor irritant”.

Read together, these numbers reframe the friction debate. Shoppers are far more forgiving of a bank that checks than of a bank that says no.





A decline is rarely a one-off

False declines leave a lasting mark on behavior. Among shoppers who had a legitimate purchase declined, 71.1% also abandoned a purchase over a slow or complicated bank approval, compared with 18.4% of shoppers who were never wrongly declined. Once a card has failed a shopper at the wrong moment, every later confirmation carries less benefit of the doubt.

Age shapes both exposure and sensitivity. Younger shoppers are declined far more often (57% of 18- to 34-year-olds versus 23.7% of those 55 and older), but older shoppers are the most likely to name a false decline as their top reason to abandon (30.9%, versus 22.2% of the youngest group). Customers of digital-only banks reported the highest decline rate of any institution type, at 47%.

Analysts see the same pattern from the issuer side. Datos Insights research on unnecessary card declines finds that cardholders rarely call to complain after a decline. Many simply switch to another card, which then becomes their top-of-wallet choice.

Shoppers forgive a question. They don't forgive a no.

Declined

39.2%

had a legitimate purchase declined by their bank.

71.1%

of them also abandoned a purchase over a slow or complicated approval.

Asked to confirm

48.4%

feel reassured that their bank is actively keeping them safe.



Silence isn't the answer either

The fix is not to wave everything through. A third of shoppers (33.5%) say they would feel uneasy if a high-value purchase on an unfamiliar website completed instantly with no verification, and that unease rises with age, from 27.6% of 18- to 34-year-olds to 40.1% of those 55 and older. Only 25.3% would feel relieved.

33.5%	41.1%	25.3%
Uneasy	Neutral	Relieved

Shoppers are asking for something more precise: approve what is clearly theirs, check what is genuinely uncertain, and never refuse a purchase that a quick confirmation could have saved.

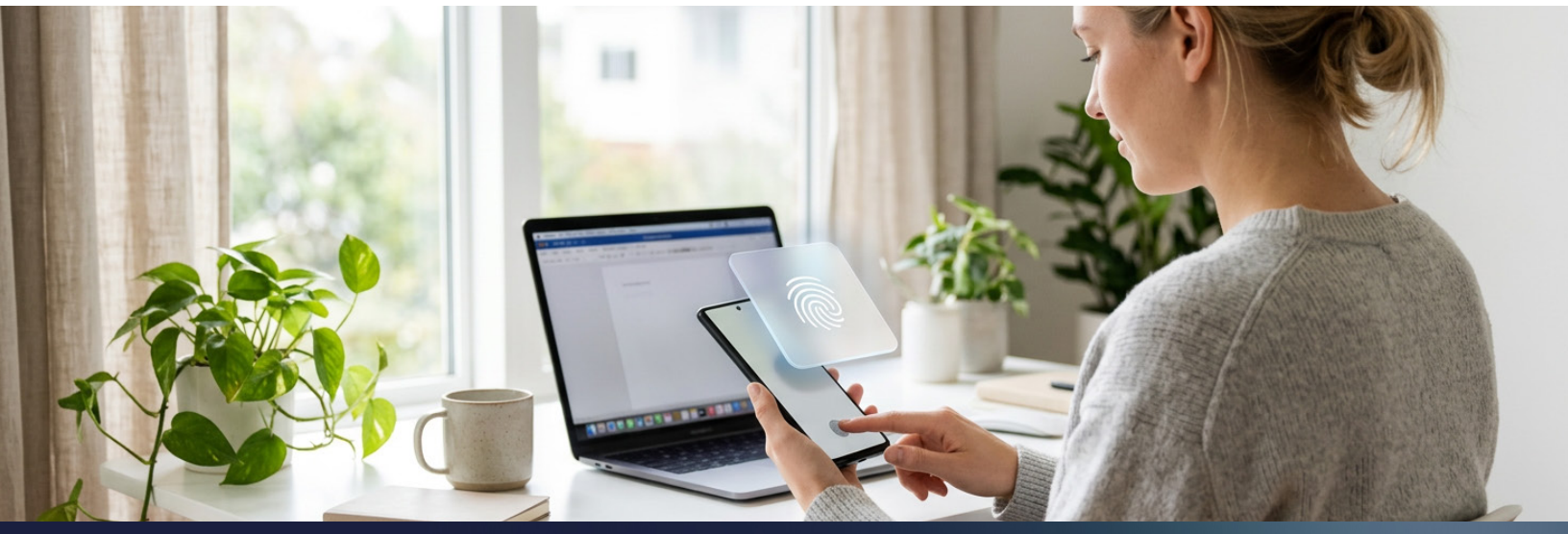
Issuer takeaway: replace the hard decline with a smart question

For most issuers, false declines are invisible on the balance sheet. The shopper doesn't complain; they just stop using the card. That makes Cyber Week the best possible time to measure them.

Issuers should start by separating fraud declines into those that stopped fraud and those that stopped customers, segmenting by merchant category, ticket size, and customer tenure through the peak weeks. Static, portfolio-wide thresholds tuned for an ordinary Tuesday will misfire when spending patterns shift every November.

The second shift is to make step-up authentication the alternative to a decline, not an addition to it. When a purchase is uncertain rather than clearly fraudulent, a fast, risk-aware challenge through EMV 3-D Secure gives the genuine cardholder a way to prove it is them in seconds. Richer 3-D Secure data on device, merchant, and behavior also lets issuers approve more confidently in the first place.

Finally, keep the reassurance visible where it counts. Shoppers want to see their bank at work on large purchases from unfamiliar merchants. A well-timed confirmation on those transactions, and silence everywhere else, is how issuers earn both the approval and the trust.



Know when to challenge, and when to step aside

Holiday shoppers have given card issuers something rare: explicit permission to intervene. More than three-quarters want their bank to confirm purchases during a sale, and nearly half feel reassured when it does. Trust is already in place.

What breaks that trust is execution. A confirmation that takes longer than a minute. An approval that never makes it back to checkout. A code that a fraudster can ask for just as easily as the bank. A decline for a purchase the shopper was always going to make. More than half of shoppers (56.5%) hit at least one of these failures in the past year, and each one sent some of them to another card, another merchant, or no purchase at all.

The issuers that win this holiday season will share four habits. They will measure authentication by completed purchases, not prompts sent. They will let most transactions through silently and challenge only where risk is real. They will confirm purchases without sending shoppers on a round trip to another app. And they will move customers from interceptable codes to device-bound credentials before fraudsters force the issue.

That is the work Entersekt does for banks, credit unions, and card issuers. Our 3-D Secure ACS and Context Aware™ Authentication use real-time device, behavioral, and transaction signals to approve trusted customers frictionlessly and step up only when risk warrants it. Our risk intelligence capabilities turn those signals into sharper decisions on every transaction, helping issuers cut false declines without opening the door to fraud. And when a confirmation is needed, push and biometric approval and passkey support let cardholders say yes in seconds.

To see how your authentication experience will hold up on Cyber Monday, and to benchmark it against the expectations in this report, visit entersekt.com or speak to an expert.

Shoppers will forgive a bank that checks. They won't wait for one that's slow, and they won't come back to one that says no.

Four habits winning issuers will share this season

1.
Measure completions

39.2%

of shoppers have abandoned over a slow approval or a broken handoff

2.
Challenge only real risk

26.9%

named a blocked or declined legitimate purchase as the top reason to walk away

3.
Keep them on the page

40.0%

approved in the app but hit a pending, failed, or reset checkout

4.
Move past the code

17.3%

responded to a fake message impersonating their bank

Appendix

Methodology and demographics

Methodology: This report analyzes data from an October 2026 survey of 1,026 U.S. adults ages 18 and older who plan to make holiday purchases online this year. The survey explored how shoppers weigh speed against security when their bank authenticates a purchase at online checkout, and what getting that balance wrong costs the banks and credit unions behind their cards. Respondents were recruited through the Centiment online audience panel. All respondents passed an attention check. Subgroup comparisons by age and institution type are unweighted. Percentages may not total 100% due to rounding.

Participant demographics: All participants were based in the United States. The largest age group (20.5%) was 65 or older, and 38.2% were 55 or older. Most held their primary checking account or credit card with a large national bank (42.2%), followed by credit unions (15.9%), regional banks (14.6%), digital-only banks or fintech apps (11.4%), and community banks (10%). Debit cards were the most-used online payment method (46%), ahead of credit cards (40.2%) and digital wallets (11.5%).

Age	Share	Primary institution	Share
18–24	11.2%	Large national bank	42.2%
25–34	17.3%	Credit union	15.9%
35–44	18%	Regional bank	14.6%
45–54	15.2%	Digital-only bank or fintech app	11.4%
55–64	17.7%	Community bank	10%
65 or older	20.5%	Not sure	5.8%