Fraud Protection & Compliance
Enterprise Payments Fraud

WHITE PAPER

FICO®

Digital Consumer Banking and Fraud Survey

2021

FICO®

Table of Contents

Executive Summary **3**

Part 1: Consumer banking has gone digital and it's not going back **5**

Part 2: Digital customer experience and fraud **8**

Part 3: Customer perceptions of banks' security measures **10**

Part 4: Top takeaways and next steps **16**

How FICO helps **17**

Banks balance digital fraud and customer experience in shifting global markets

Executive Summary

In September 2021, FICO surveyed 12,028 banking customers from 12 different countries across North America, South and Central America, the UK, Europe, and the Asia-Pacific region. The goal was to assess consumer perspectives on issues at the crossroads of customer experience and fraud management.

Though attitudes toward these issues vary significantly across markets, the connection between fraud management and customer experience is clear.

Survey results show that customers generally consider banks trustworthy, their transaction security adequate, and their treatment of fraud victims fair. However, significant customer cohorts are willing to defect for reasons ranging from a single, erroneously declined card transaction to discovering a bank's involvement in a money laundering scandal. Results indicated that poor fraud management can be costly for banks in the customer experience and cost columns, as more than **80% of customers worldwide will either complain to their bank or leave for a competitor if they are unhappy with how their bank manages fraud** (Figure 1).

FICO's survey also revealed the extent to which consumers are embracing digital transformation:

- **Most customers (80%) prefer using digital channels such as text, email, and bank apps to verify payments.**
- **Most customers (65%) plan to continue banking digitally, even if local economies reopen.**
- **More customers (61%) plan to maintain or increase their use of real-time payments than not.**

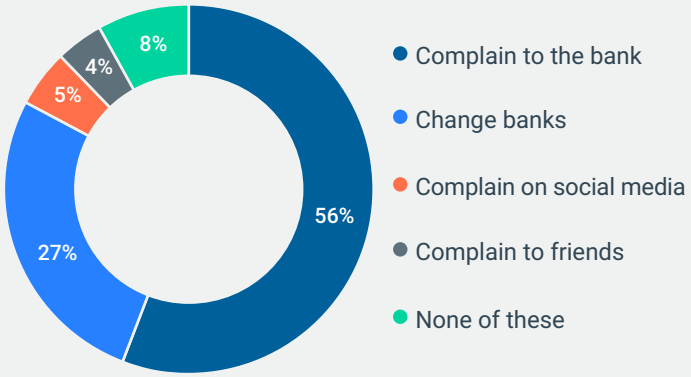
As a result, banks face substantial challenges delivering frictionless customer experiences and fraud management capabilities across the expanding number of digital channels. They must communicate with customers through whichever channel they prefer, often despite documented security risks.

This shift to digital not only expands the fraud attack surface, but it makes for a more complex set of customer experience concerns. These pit the need for superior fraud management

Figure 1:

83% of customers will complain or leave if they are unsatisfied with a bank's fraud management.

If you are a fraud victim and are unsatisfied with your bank's response, how will you react?



against the desire to cater to customer communication, authentication, and verification preferences while eliminating friction from shopping and payment processes.

The survey also shed light on the prevalence of reported fraud, and what specific kinds of fraud are most concerning to consumers. Globally, 41% of respondents said they had reported actual or suspected fraud to their bank, although the rate of reporting varied significantly in different countries, from a low of 17% in Germany to a high of 66% in India.

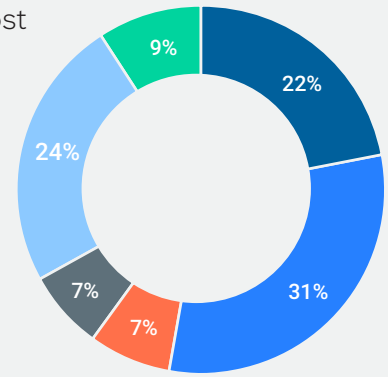
When asked what kinds of fraud are most concerning, consumers cited account takeover as their top concern (31%). The most surprising result was that globally, consumers had the least amount of concern around being tricked into sending payments to a fraudster (less than 7%), even lower than their stated concerns about being pickpocketed (7.1%). This laissez-faire attitude is despite the dramatic and devastating uptick in scams, particularly authorized push payment (APP) scams — which in the UK alone accounted for £479 million in gross losses in 2020.

As banks move forward into this increasingly digital market, they face a delicate balancing act. They will need to build and maintain customer trust through a combination of effective fraud management, efficient customer experiences, and proper stewardship against financial crimes, while enforcing their own fraud risk policies.

They will also have to avoid anything that can cripple their reputation, such as money laundering, while working to identify and help consumers battle complex scams that both attack and take advantage of new technologies such as real-time payments. Banks that get the balance right will emerge as leaders in the new digital landscape.

Figure 2:

Which of these is of most concern to you:



- A fraudster stealing my identity and using it to open a financial account
- A fraudster using information about me to take over one of my financial accounts
- A fraudster tricking me into sending a payment to them
- A pickpocket stealing my wallet or purse
- A criminal using my credit or debit card details to buy things
- Not worried about any of these

Part 1: Consumer banking has gone digital and it's not going back

If consumer banking was not already largely digital, its digitalization happened through 2020–2021. The COVID-19 pandemic forced consumers to adopt digital tools to complete everyday tasks online, including shopping and banking. Our data shows most consumers do not plan to go back to in-person banking.

Majority of customers will continue banking online

89% of banking customers worldwide plan to continue using online banking (see Figure 3) regardless of whether COVID-19 restrictions are lifted. Only 7% plan to return to as much in-person banking as possible.

65% of banking customers worldwide will continue to do *all* their banking online, including banking via mobile device. These customers are also 1.4x more likely to use real-time digital payments in the coming year.

Real-time digital payment adoption explodes

PaymentsJournal defines real-time payments as those that are "initiated and settled nearly instantaneously" and that will process transfers any day or time, including holidays and weekends. In the UK, the Faster Payment System platform was processing nearly 300 million real-time payments per month at the time of writing. The US has also established a real-time payments platform dubbed The Clearing House to provide federally insured depositories a basis for offering real-time payment services.

Real-time payments should continue to grow rapidly, as 50% of our respondents worldwide reported that they are more likely to use real-time payments in the coming year (see Figure 4), while only 11% said they are less likely to use them. Real-time payments grew 41% globally in 2020, according to GlobalData and ACI Worldwide, exceeding 70 billion total transactions and more than USD$92 trillion in value. Real-time payments are expected to continue to grow explosively, from roughly 10% of global electronic transactions in 2020 to more than 17% in 2025.

Figure 3:

A majority of customers will continue to do all of their banking online.

As the economy reopens, will you continue to rely on digital banking or go back to in-person banking?

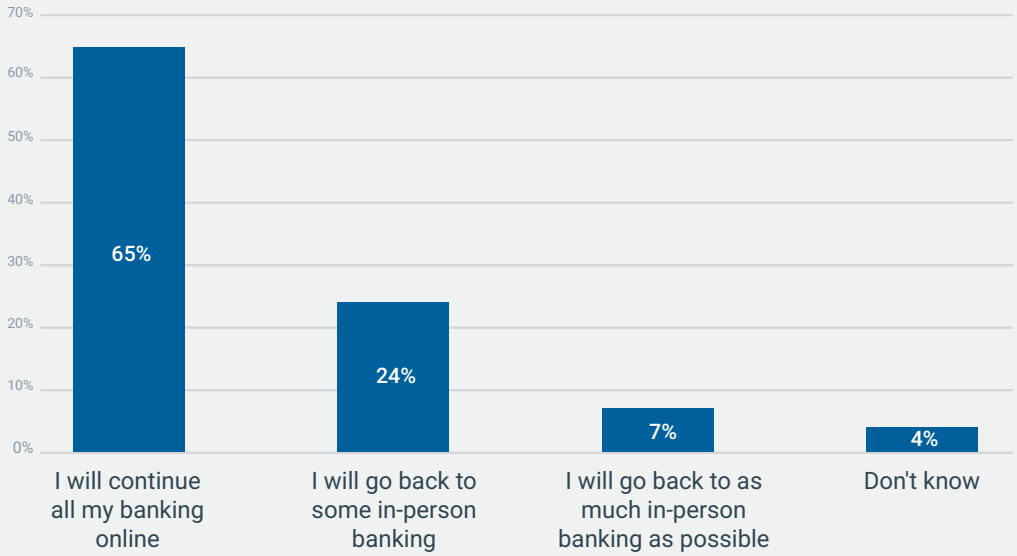
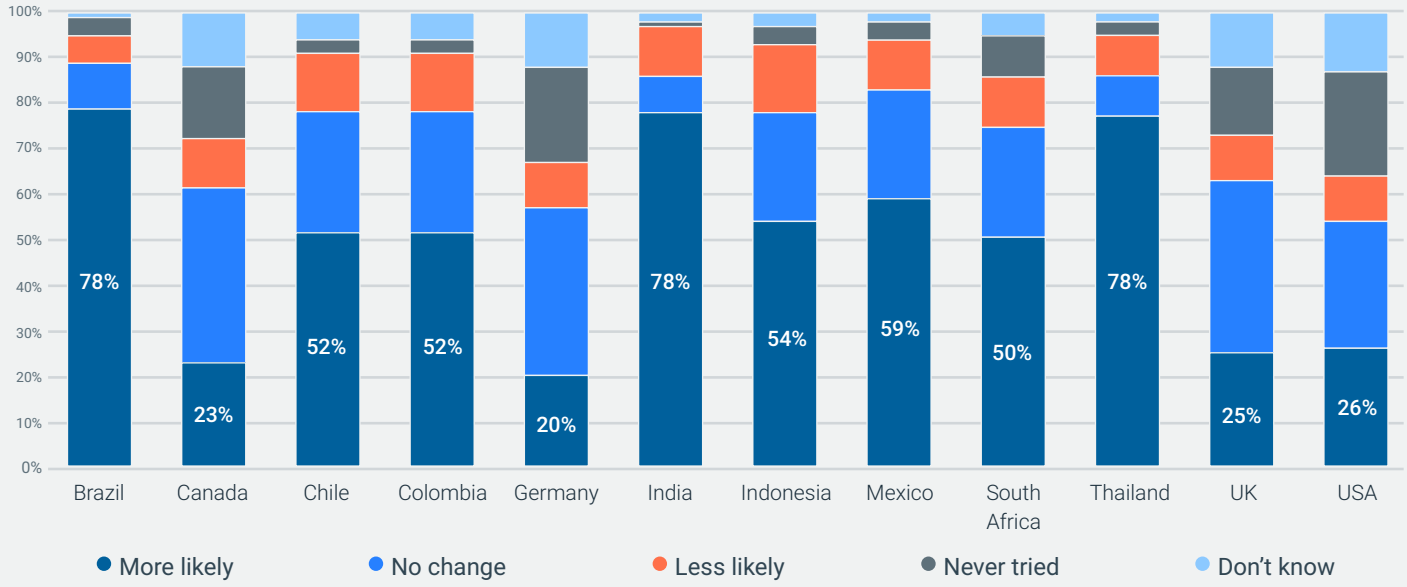


Figure 4:

In most countries, real-time digital payment usage is set to continue its explosive growth.

Are you more or less likely to use real-time payments in the next year?



Our survey showed that while digital payment usage is growing nearly everywhere, it is most likely to increase in India (78%), Thailand (78%), and Brazil (78%). Customers who plan to increase their use of digital payments are 1.7x more likely to continue doing all their banking online. Digital payment adoption also tracks to age, as younger cohorts tend to adopt at a greater than average rate. For example, while 59% of the 25–34 age group plans to increase use of digital payments, only 24% of the 65+ group feels the same.

Only 11% of respondents said they are less likely to use digital payments in the coming year. In contrast to digital payment adopters, these customers are twice as likely to return to some in-person banking, but are also 1.7x more likely to say the type of fraud they are most concerned about is being tricked into sending real-time payments. This could help explain their desire to use the technology less often.

For the coming year, 24% of global banking customers anticipate no change in their use of digital payments. They are 1.5x more likely to be over 55 and 1.5x less likely to have personal loans, car loans, or pay later loans.

In the survey, 9% of respondents indicated that they have never used real-time payments. They are more than 3x more likely to be 65+ and to want to return to in-person banking. They are also twice as likely not to have a personal loan, car loan, or pay later loan, and 1.5x less likely to have a savings account.

Customers prefer digital channels for verification, but not necessarily their bank's

Nearly 80% of banking customers worldwide prefer to use digital channels, including text messaging, emails, bank apps, and third-party messaging services, to verify payments, but bank apps are not the most frequently preferred digital channel for payment verification.

If implemented appropriately, banks' branded apps could offer retail banking customers the most secure option for identity authentication and payment verification. Bank apps are now the second most preferred channel (20%) among customers worldwide for verifying payments. However, the use of banking apps to verify payments is substantially lower than banking app adoption rates in general.

For example, bank app adoption exceeds 40% in the US and hits nearly 70% among Millennials, but only 6.5% of all US customers and 10% of those aged 25–34 prefer to use bank apps to verify payments. This should present an opportunity for banks to encourage more engagement, such as with payment verification, through the secure branded apps their customers already have and use.

The challenge, however, is most customers prefer to use channels other than bank apps, regardless of security considerations. Despite security flaws described as early as 2016, 60% of consumers indicated that they prefer to verify payments via text message or email (see Figure 5). Hence, banks once again face decisions that balance security and fraud risks against customer experiences.

Payment verification preferences also vary significantly by country. In the USA, 64% of customers prefer a text message while only 2% want to use a third-party messaging app. Brazil, by comparison, is far more diverse: 28% prefer a text message, 30% prefer a bank app, and 12% would like to use a third-party messaging app to verify payments.

Impact on customer experience and fraud management

As digital channels expand and customer preferences evolve, banks are being exposed to new vulnerabilities and risks related to fraud, brand trust, and customer defection. While our survey shows that most customers are satisfied with bank security, it also shows that customers are not primarily concerned with the common fraud tactics most likely to victimize them. And because customers most often prefer to communicate with banks via less secure channels, they face a combination of vulnerability and lack of awareness that criminals aim to exploit.

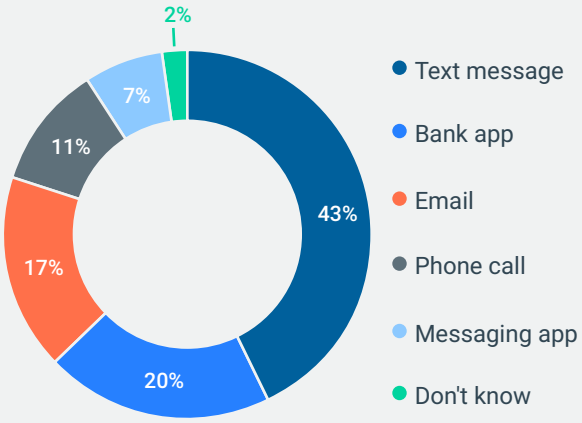
Our survey shows that when fraud strikes or money laundering scandals break, banks face customer experience risks, such as increased complaints and care costs, and serious reputational risks, such as mass customer defections.

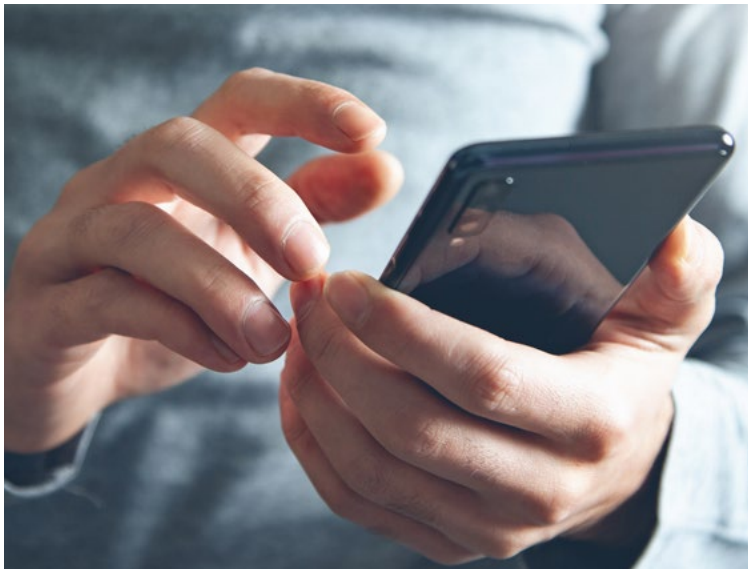
Banks have an opportunity now to increase their leadership role in educating customers about detecting and preventing fraud while providing them effective methods and tools to do so. Our survey shows banks will need to be cognizant of significant regional differences, which can impact tens or hundreds of millions of customers, as they implement robust technology tools to detect and prevent fraud and proactively communicate with customers through their preferred channels.

Figure 5:

Nearly 80% of banking customers worldwide prefer to use digital channels to verify payments.

If your bank needs to send a code to verify a payment, which channel would you prefer to use?





Part 2: Digital customer experience and fraud

Globally, 41% of our survey respondents say they have reported actual or suspected fraud to their banks. This is indicative of the intricate intertwining of digital customer experience and fraud, because while every customer has an experience, not every customer has or knows whether they have experienced fraud.

While this fraud experience rate is consistent across men and women, it varies substantially from country to country (see Figure 6). Germany shows the lowest fraud experience rate at 17%, while India is at the high end with a 66% rate.

Nearly half of customers from South Africa, USA, and Indonesia have reported fraud experiences as have about 40% of customers from Chile, Colombia, and Thailand. Less than 40% of customers from the UK, Canada, and Brazil have reported fraud experiences.

When asked specifically if they had been victims of account takeover (ATO) frauds, 18% of those surveyed replied "yes." ATO fraud rates vary substantially by country, however, and the global rate belies the true scope of the problem. For example, 51% of customers from India said they had been victims of account takeover frauds. Given a population of 1.4 billion, with an estimated banked rate of 48%, that would equal roughly 672 million people with bank accounts and more than 340 million ATO victims in India alone.

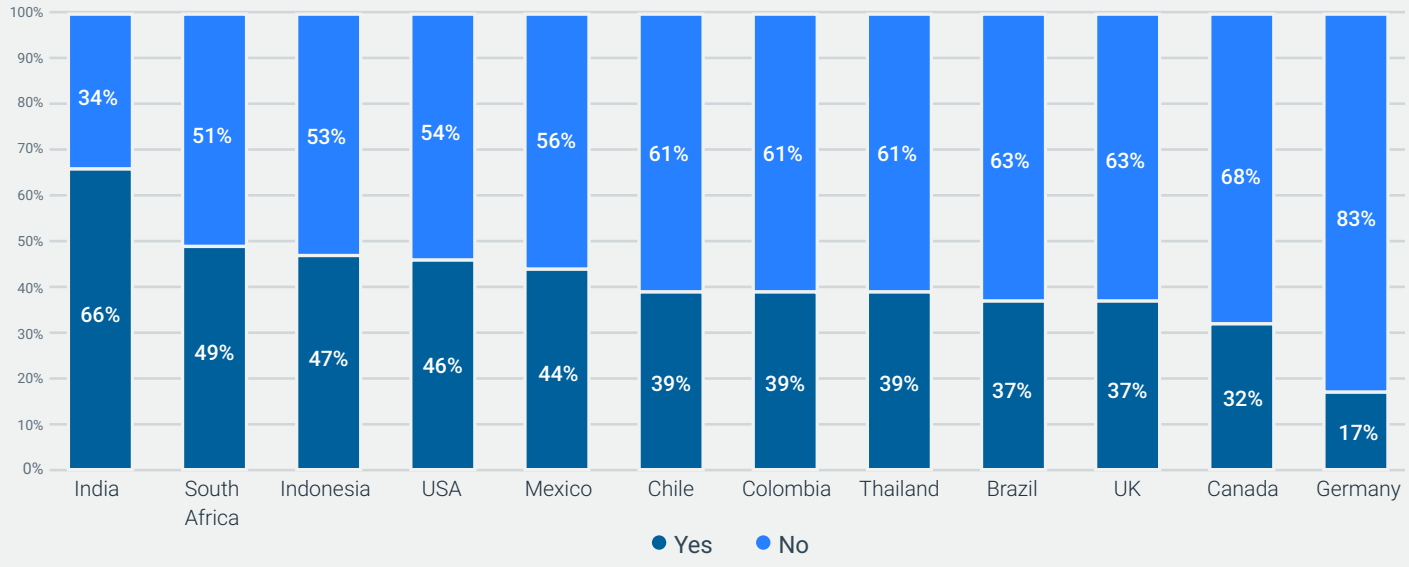
While reported fraud rates remain relatively high in most markets, the concurrent explosive growth of a variety of digital frauds suggests even these numbers may be low. *Security magazine reported in June 2021* that banking fraud attacks grew a stunning 159% from Q4 2020 to Q1 2021, with 93% of all frauds attempted via online banking, which itself made up 96% of all banking transactions worldwide. The magazine lists account takeover (42%), account opening identity theft (23%), and impersonation scams (21%) as the top three most common banking scams today.

Does consumer fraud awareness match the scams?

When asked which of five types of fraud concerned them most, 31% of the banking customers FICO surveyed worldwide replied they were most concerned with account takeover fraud; 24% with having credit or debit card details stolen; and 22% with account opening identity theft. Given the prevalence of ATO fraud

Figure 6:
Worldwide fraud reporting rates

Have you ever reported suspected or actual fraud to your bank?



mentioned previously, it is no surprise that it has achieved such awareness among banking customers.

On the contrary, only 7% of customers worldwide were most concerned with scams where fraudsters trick them into sending payments, which is known in the UK as authorized push payment (APP) fraud and is growing rapidly.

In September 2021, UK Finance reported a 71% increase in APP fraud during the first six months of 2021, which was accompanied by a 9% decline in payment card fraud. UK banks reportedly blocked a majority of card fraud attempts in that time frame — £736 million in attempted unauthorized card fraud. But APP fraud aims to skirt those defenses by persuading victims to send real-time payments directly from their bank accounts to the fraudsters, which they cannot subsequently retract.

Despite the known and growing threat APP fraud poses to UK banks, only 6% of UK banking customers list APP fraud as their top fraud concern. By comparison, 24% list payment card fraud and 26% rate both Account Opening Identity Theft and Account Takeover Fraud as their main concerns.

The survey also shows, however, that past victims of ATO fraud are twice as likely to rank being tricked into sending a payment as their top fraud concern. Customers who have reported fraud to their bank in the past are 1.6x more likely to share this concern. And customers in Asia-Pac countries such as India, Indonesia, and Thailand are more likely to identify scams that trick people into sending money as their top fraud concern.

As new scams and frauds emerge, banks are increasingly challenged with balancing customer experience needs against fraud risks and controls. They must cater to a range of communications preferences and both digital and physical banking habits. They must support new services, such as real-time payments, yet educate customers to protect them from fraud. They must also balance preferences related to everything from the number of card transaction declines customers will tolerate to how they prefer to verify a variety of different online, mobile, and real-time payments. And of course, these preferences and tolerances vary significantly in different countries.

The good news for banks is that customers tend to trust them, to rate their customer service well, and to consider their security measures to be adequate. The risk for banks is that these attitudes can change very rapidly in the face of scandal or simply because of poor fraud management, resulting in customer complaints at best and mass customer defections at worst.

Who is worried about real-time payments fraud?

Less than 7% of bank customers worldwide rate scams that trick people into sending real-time payments from their bank accounts—also known as Authorized Push Payment (APP) fraud—as their top fraud concern.

In the UK, this kind of fraud grew 71% in the first half of 2021 alone and has nearly equaled card fraud losses for banks. This phenomenon is happening across global markets.

The minority of customers who are aware of and concerned about this kind of fraud stand out from the crowd.

These customers tend to hail from the Asia-Pac region; are more likely to have experienced fraud in the past; skew younger; and are more likely to use other banking products like car loans.

Real-time payments fraud worrier profile

Geography
- 2.5x as likely from India
- 1.4x as likely from Indonesia
- 1.4x as likely from Thailand

Fraud history
- 2x as likely to be a past victim of account takeover (ATO) fraud
- 1.6x more likely to have reported fraud in the past

Age
- 1.4x as likely to be 18–24
- 1.2x as likely to be 35–44

Banking
- 1.6x as likely to use pay later loans
- 1.4x as likely to use personal loans
- 1.3x as likely to use car loans

Oddities
- 1.4x as likely not to have a cell phone
- 1.2x as likely not to have a credit card

Part 3: Customer perceptions of banks' security measures

Banks are fortunate to be trusted by most of their customers. Banks as an industry tend to rate well among customers, and when compared against other service industries, in both trust and customer service. For example, a recent survey from the American Bankers Association found that 54% of American consumers are "very satisfied" with their primary bank; 82% consider their banks' customer service "very good" or "excellent"; and more consumers trust banks to keep personal information secure (48%) than they do health care providers (25%), telecom providers (2%), or the government (10%).

Most customers think their money is safe with their banks

According to FICO's survey, 72% of customers worldwide think their bank does enough to keep their money safe, while only 20% believe they could do more. This degree of trust holds across countries, even those with higher fraud reporting rates such as India, where 88% of customers feel banks do enough to keep their money safe.

Similarly, across a range of payment transaction types — including online payments, in-store payments, payments set up through a bank account, and credit transfers from a bank account — on average 65% of customers view their banks' security measures favorably (see Figure 7).

Good fraud management leads to positive customer experience

The data validates that trust erodes among customers who have been victimized by fraud or scams. For example, in Chile the 37% of customers who expect banks to do more to keep their money safe are also 1.4x more likely to have reported fraud in the past, and 39% of customers in Chile have done so.

Banks, however, seem to be doing a good job defending customer trust against common types of fraud. Most customers think banks are fair with fraud victims, which speaks to positive fraud management practices across different aspects of the customer experience. For example, nearly half or more of all customers think their banks are fair with victims of card fraud, APP fraud, and ATO fraud (see Figure 8). Customers who have reported fraud are 1.5x more likely to think banks are fair in how they treat fraud victims. In fact, ATO fraud victims are 3x as likely to say their bank is fair with victims of ATO fraud.

Figure 7:

Are there enough security checks when you make payments and transfers?

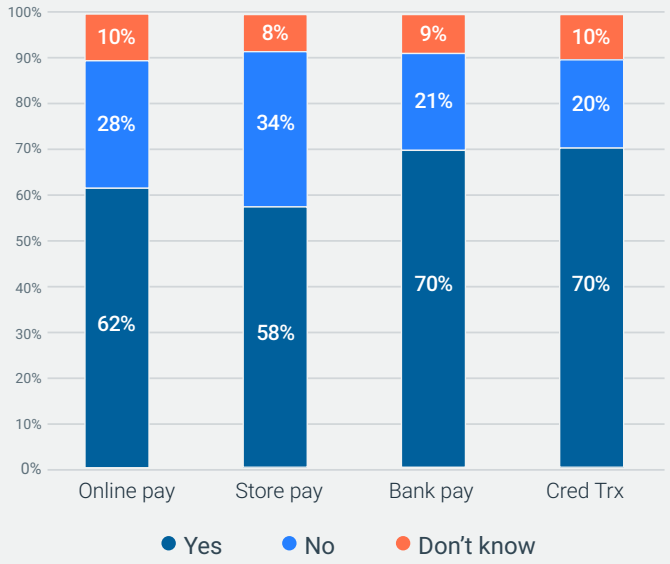
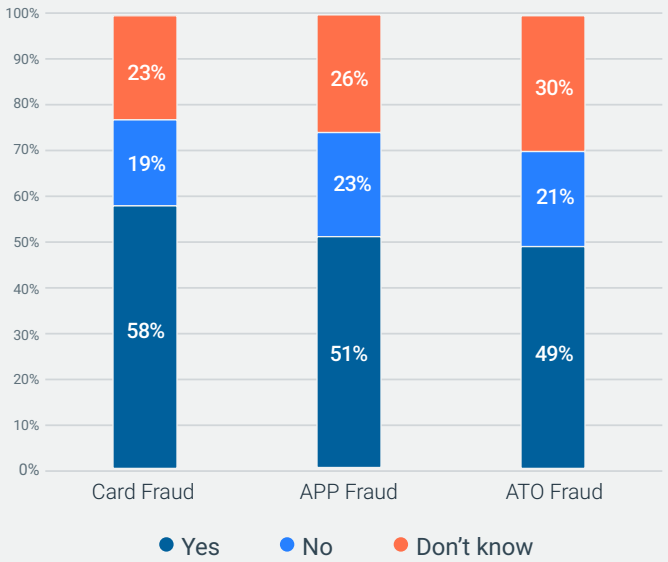


Figure 8:

Are banks fair with victims of different frauds?



A negative fraud management experience is a negative customer experience

The risk for banks is that the reverse is also true; when customers experience poor fraud management, their reactions can prove costly for banks and card issuers. Worldwide, 83% of customers will either complain to their bank (56%) or change banks (27%) if unsatisfied with their bank's response to a fraud event (see Figure 1). Less than 10% said they would either complain to friends or on social media, trends that hold across countries as well.

According to the US-based Bank Administration Institute (BAI), banks spend up to $10 per contact on the call center. Any upward pressure on contact center volume driven by poor fraud management experiences will result in escalating costs for banks, in addition to the potential for declining customer experience scores and brand trust erosion.

What is a negative fraud management experience?

What makes a fraud management experience negative can be subjective and will vary across markets. Of the 69% of bank customers surveyed that selected one of the choices provided, 41% are most irritated when a fraud alert about a transaction decline either fails to reach them or reaches them too slowly (See Figure 9). In other words, among customers' greatest irritants is when well-intended fraud management practices perform poorly. This is an example of how poor fraud management can translate into negative customer experiences, potentially on a large scale.

Focusing on a different segment of the customer lifecycle, 35% of customers are irritated because their financial institution continues to change how it authenticates customers. Proper customer authentication is not only crucial to fraud management, but also a central component of a bank's customer experience in any channel. There is a clear connection between customers' sensitivity regarding authentication and their perception of fraud management and customer experience quality. Banks should respect this connection as they encourage customers to adopt their branded apps and channels for user authentication and payment verification.

Figure 1 (repeated):

83% of customers will complain to the bank or change banks if fraud is managed poorly.

If you are a fraud victim and are unsatisfied with your bank's response, how will you react?

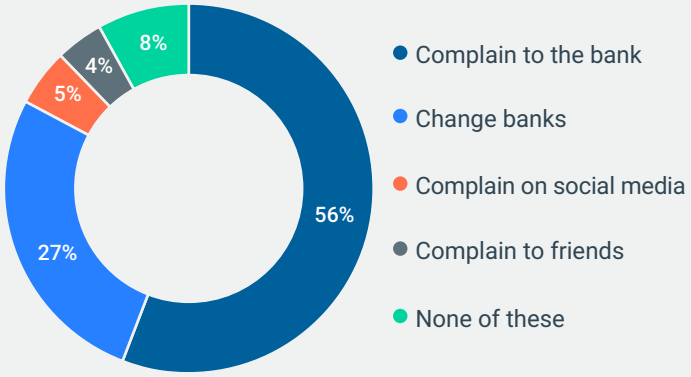
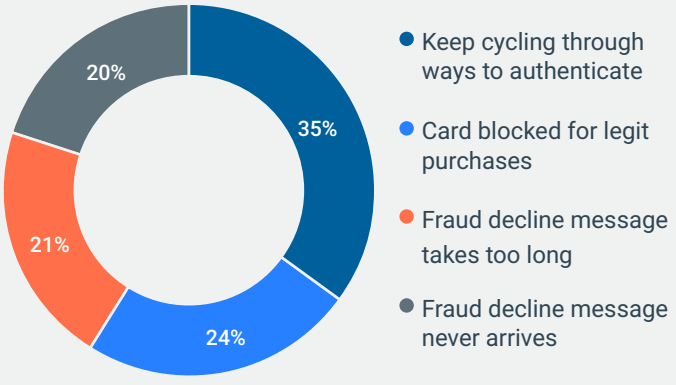


Figure 9:

41% of customers are irritated when fraud decline alerts don't reach them in time or at all.

What irritates you most about bank security measures?



Do declined card transactions impact customer experience negatively?

Only 17% of customers worldwide rate false card declines as their biggest irritation with bank security, but 46% view in-store card declines negatively (similarly, 47% for online). To what degree a card decline results in a negative customer experience is based on how customers react to events such as well-intended but erroneous card declines. The largest portion of customers (42% worldwide) will tolerate two or three false declines before considering changing providers. Another 37% would tolerate more than four false declines or said they would not leave a provider for this reason.

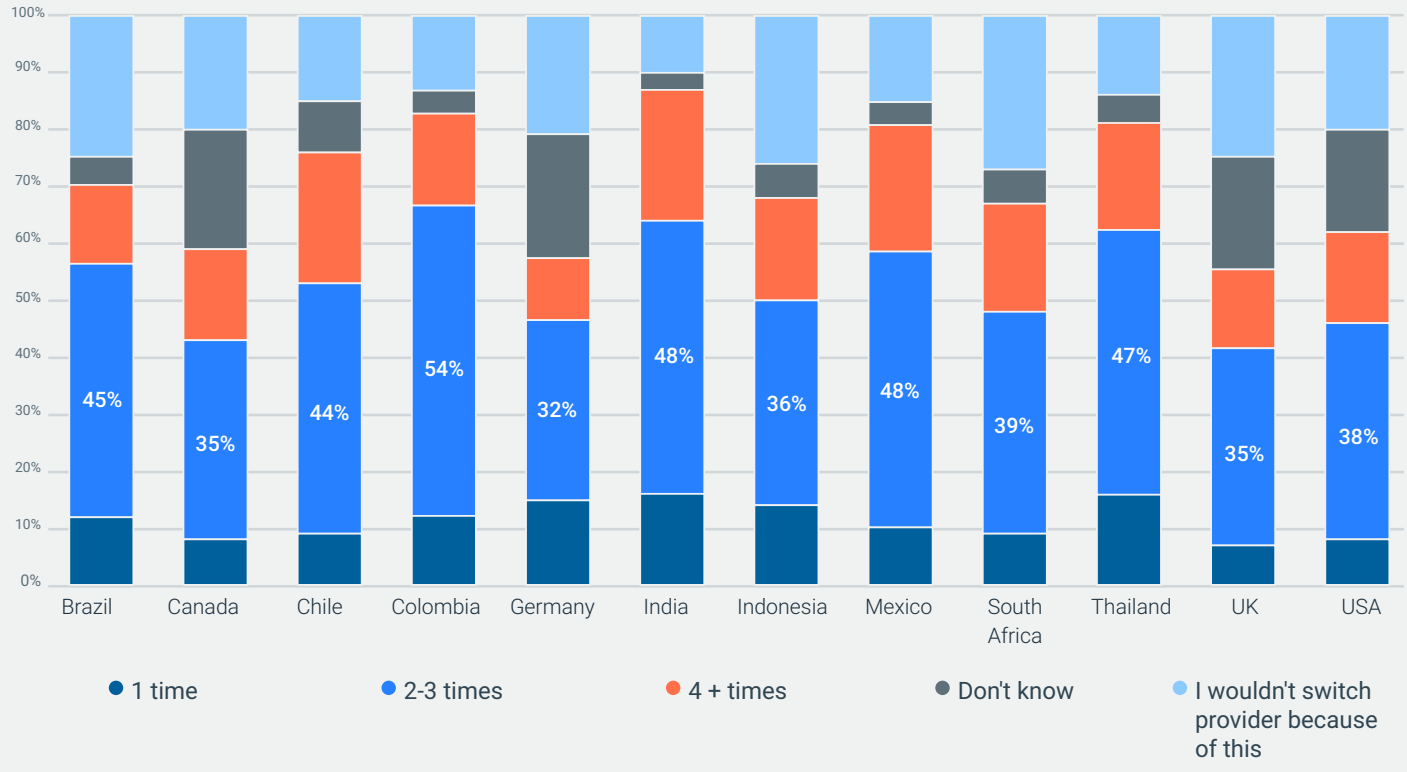
Though a minority of customers (11% worldwide, no more than 16% in any country) would consider changing card providers after just one erroneous decline of a legitimate transaction, the absolute figures paint a more daunting picture.

For example, in Thailand, 16% of customers would leave a provider after just one false card decline. In a country of 54 million adults, adjusting for a credit card penetration rate of just 10%, that's more than 860,000 credit card customers willing to drop a provider for a single false transaction decline. In South Africa, only 9% of customers would quit a provider after a single false card decline. The country has 35 million adult inhabitants, but only about 3 million credit cards, yet this means more than 280,000 accounts are at risk of turnover after a single false decline.

Figure 10:

Most customers worldwide will tolerate 2-3 false card declines before considering changing card provider.

When making a payment online using a credit or debit card, how many false declines before you'd consider changing provider?



Reactions to card declines will differ

Despite the previous examples where customers perceive false card declines negatively, attitudes toward card declines vary significantly by country.

In India, for example, 54% of customers view in-store card declines positively. Those customers are more than twice as likely to have experienced fraud in the past. They are also significantly more likely to use car loans, credit cards, mortgages, and personal loans — in other words, to be engaged with financial institutions across a variety of products.

In Thailand, where more than 800,000 card accounts may be at risk as noted earlier, 39% of customers actually view in-store card declines positively. These customers are 3x more likely to use credit cards, twice as likely to have savings accounts, and twice as likely to have experienced fraud.

And while in the UK only 19% of customers view in-store card declines positively, these customers are also more than twice as likely to have experienced fraud and are significantly more likely to use personal loans, car loans, and mortgages.

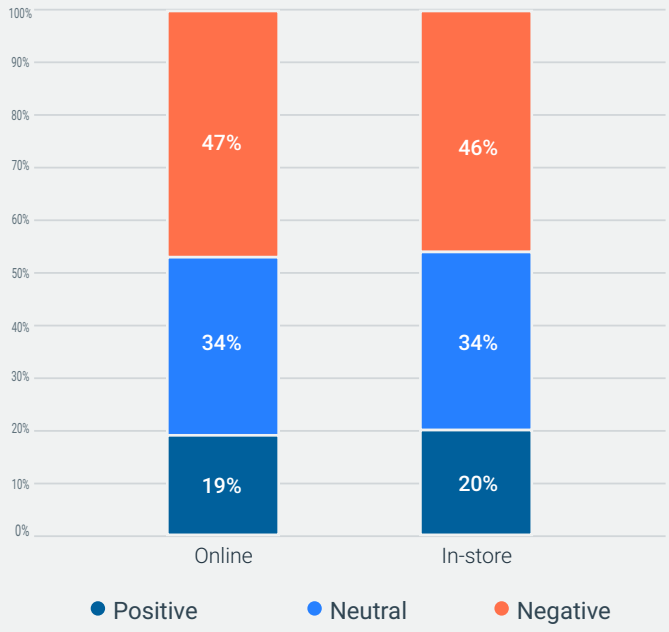
Clearly, customers have broadly differing perspectives on fraud management experiences. Individuals will react very differently to stimuli such as a series of false card declines, and are most irritated when fraud management alerts don't work and when authentication schemes change.

Banks face some fundamental hurdles as they implement strong fraud management practices that aim to take advantage of customers' preferred communication channels to support fraud alerts, payment verifications, and other transactions. The question is: What stands in the way of good, proactive fraud management, and how do we fix it?

Figure 11:

20% of customers worldwide view declined transactions positively.

When a debit or credit transaction is declined online or in-store, how do you feel about it?



Money laundering scandals destroy customer relationships

Perhaps no event has the potential to color customers' perceptions of banks more negatively than a money laundering scandal. Worldwide, 76% of survey respondents say they would switch to another bank if theirs were caught up in such a scandal (see Figure 12).

This rate jumps to 84% among past victims of fraud, and more than 80% of customers in Brazil, South Africa, Mexico, Colombia, Indonesia, and India would switch banks due to a money laundering scandal. Those who said they would not leave a bank for this reason do not exceed 16% of customers in any country.

This finding establishes a connection between customer experience and banks' anti-money laundering (AML) operations. Banks must focus not only on compliance, but also on accurately identifying and reporting suspicious activity. When banks miss on this aspect of AML and face both regulatory action and bad press, the cost in reputation and customer attrition can be even more damaging.

Barriers to proactive fraud management

Though the need to communicate information to customers in real time is increasing, inaccurate customer contact information may prove to be the fly in the ointment for banks when it comes to defending customers and customer trust from negative fraud experiences or market events. Worldwide, 22% of credit card customers report that their card provider does not have an accurate mobile number for them (see Figure 13). Debit card providers face similar rates of inaccuracy in customer contact information, with 18% of customers reporting inaccurate mobile numbers and 28% reporting inaccurate home addresses (Figure 14).

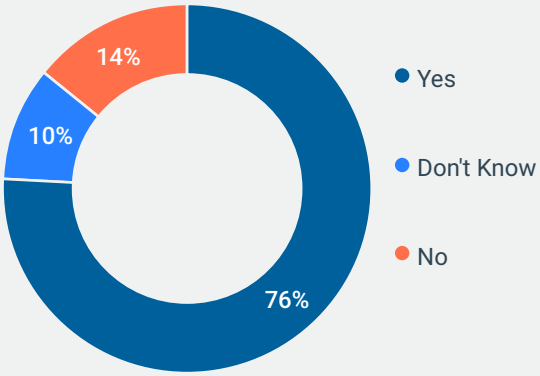
In August 2021, Shift Processing reported there are 2.8 billion credit cards in use globally. The leading issuer provides more than 500 million cards. The possibility that a single issuer could have more than 110 million cards associated with the wrong cell phone numbers is stunning. Even half that rate would result in a massive customer data cleansing challenge.

Basic customer contact issues aside, the increasing dependencies between mobile numbers, user security, and anti-fraud controls make this more than a data accuracy problem. Inaccurate information becomes a barrier to proactive fraud

Figure 12:

76% of customers would leave their bank in the wake of a money laundering scandal.

If your bank were involved in a money laundering scandal, would you switch to another bank?



management and a threat to customer experiences, particularly mobile and digital ones.

Customers continue to use mobile devices for banking at an increasing rate. For example, according to UK Finance, 50% of UK adults now use a mobile banking app. Global Business Outlook estimates 72% of UK adults will use mobile apps for payments by 2023. But 20% of UK bank customers reported their debit card provider does not have their mobile number correct.

Given roughly 50 million adults in the UK with a current bank account, 70% of which also have a credit card, more than 10 million will have a mismatch between their actual mobile number and the mobile number their credit or debit card providers want to use to communicate, authenticate, and verify their identity and transactions.

With PSD2 in effect in the UK and the European Union, multi-factor authentication is required by regulation for many types of common online purchases. As issuers are often or increasingly reliant on one-time passcodes sent via text message (OTP via SMS) to authenticate purchases, inaccurate mobile numbers can lead directly to large volumes of checkout failure as payments will not transact, resulting in more frustrated customers and retailers likely to complain.

Given the evident yet concerning challenges banks face, the important next step is to focus on taking appropriate actions to educate customers, leverage and refine fraud management controls effectively, and create positive outcomes and customer experiences that sustain trust and satisfaction.

Figure 13:

Inaccuracy rates of credit card customer contact info

Does your credit card provider have your contact info correct?

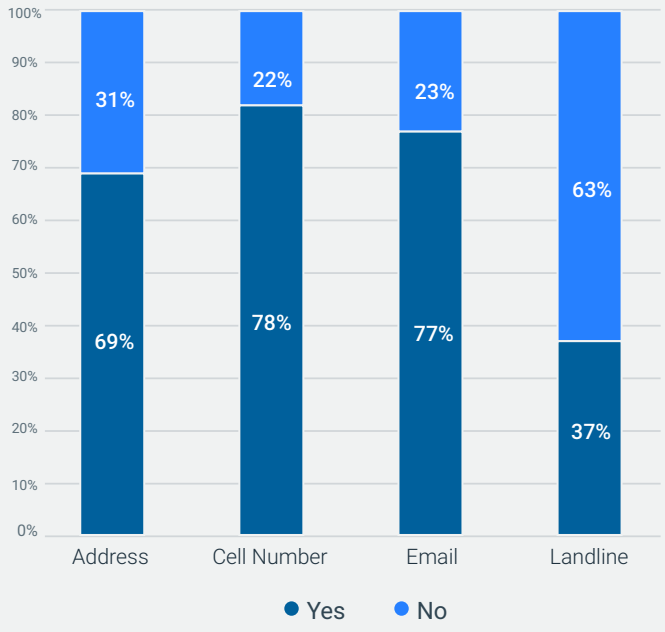
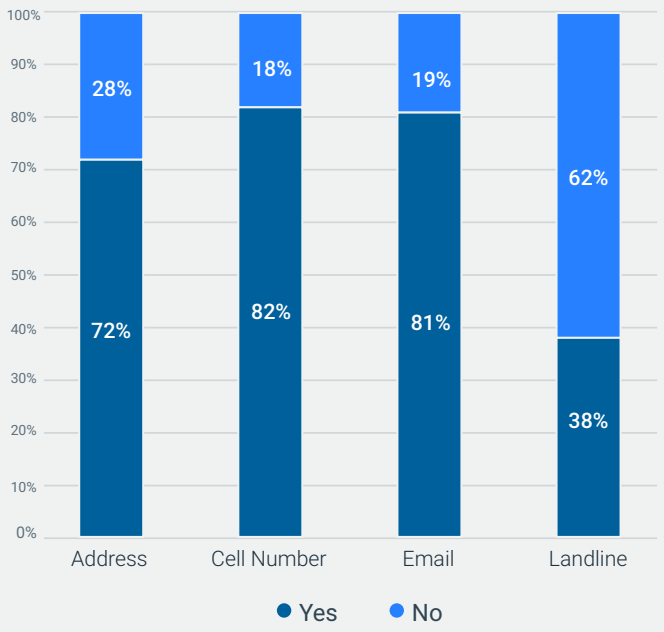


Figure 14:

Inaccuracy rates of debit card customer data

Does your debit card provider have your contact info correct?



Part 4: Top takeaways and next steps

What is clear above all is that customer experience and fraud management are closely linked, and actions to mitigate fraud can have a substantial impact (positive or negative) on customers' trust in their banks and card providers. A negative fraud management experience can turn a positive customer relationship into a confrontational one. Conversely, however, a positive, effective, and fair fraud management process protects trusted relationships and improves how customers view banks and their anti-fraud measures.

Here are seven trends, backed with evidence from our global survey, coupled with advice for banks and card issuers, on how to defend customer experiences and trust through strong customer knowledge and superior fraud management practices, processes, and capabilities.

Trend	Evidence 1	Evidence 2	Evidence 3	Advice for banks and card issuers
Digital dominates.	80% of customers will do some or all banking digitally.	53% want to do as much digital banking as possible.	50% of customers plan to use real-time payments more.	*Fraud must be defended against across all channels.*
Communication channel preferences are changing.	64% of customers prefer text messages to verify payments, despite security risks.	20% prefer the safety of a bank's app.	Past ATO victims are 2x as likely to prefer a phone call or third-party messenger app.	*Real-time dialogue is needed in any preferred channel to mitigate fraud and improve CX.*
Customer contact info is subject to change.	More than 17% of customers say their card providers have their mobile or email wrong.	42% of customers say their card providers have their landline phone wrong.	25% of customers say their card providers have their address wrong.	*Contacts must be verified to automate fraud management and CX.*
Digital banking opens the door to new scams and fraud.	31% are concerned about account takeover; 18% have experienced it.	Only 7% say they're worried about falling for push payment scams, which are a fast-growing fraud vector.	Those most concerned about push payment scams are 2x as likely to be past victims of account takeover.	*Implement proactive measures, such as ML/AI scam models, to prevent fraud while continuing fraud and security education.*
CX views of fraud and security controls vary significantly by geography.	Regional variances mean there is simply not a one-size-fits-all approach.	In India, where fraud rates are highest, 54% view a false card decline positively.	In the US, where fraud rates are lower than the group average, only 21% view a card decline positively; 44% are negative.	*Banks and card issuers need a partner with global expertise to help manage consumer expectations and prevent fraud where and how it happens.*
Customers everywhere expect banks to be ethical.	76% of customers would leave their bank after a money laundering scandal.	85% of past ATO victims and 81% of fraud victims would leave.	89% of customers in India would leave; nearly 600 milion people.	*Financial crime compliance isn't just about avoiding regulatory fines — customers are banks' biggest judges, and they'll vote with their feet.*
Good fraud management has a positive impact on CX.	60% to 70% of customers say banks do enough to keep their money, payments, and transfers safe.	Whereas 50% of all customers think banks are fair with ATO victims, 75% of ATO victims do.	If dissatisfied with fraud management, more than 80% of customers will complain to the bank or leave.	*Banks hold a trusted position and must use fraud mgmt. and AML as part of CX to defend it.*

How FICO helps

As global consumers continue to expand their use of digital banking, institutions will need to continually adapt and evolve to fight existing and emerging fraud threats. Banks and other FIs will also have to invest in the best communication tools to engage with their customers, in the channel of their choice and when it is most appropriate.

FICO offers proven, powerful solutions — built on an open and extensible platform — that address challenges such as real-time card transaction and payments monitoring, KYC and identity authentication, anti-money laundering and financial crimes compliance, and alert and case management.

FICO's enterprise fraud management solutions allow users to design rules, execute machine learning models, orchestrate workflows, manage investigation and more. FICO empowers you to accurately identify behavior indicative of criminal activity, while delivering experiences that are convenient and secure for your legitimate customers. And FICO can help you stop financial crimes faster, reduce false positives, and remove silos and overlapping functionality between fraud and financial crimes functions.

When it comes to communicating with your customers, you need the power to automate outreach and the ability to choose the best channel. With FICO, you can proactively, automatically connect with your customers through their preferred methods, while maintaining accurate, centralized details to inform a 360-degree view of your customer relationships.

The best way to help your customers and your organization beat fraudsters is to break down silos within your walls and work collaboratively. FICO gives you the integrated, enterprise-wide capabilities to address all your fraud protection and compliance needs, while simultaneously supporting your customer communication requirements.

For more information, please contact a FICO representative at info@fico.com

FICO More Precise Decisions

5094WP 01/22 PDF

FOR MORE INFORMATION
www.fico.com
www.fico.com/blogs

NORTH AMERICA
+1 888 342 6336
info@fico.com

LATIN AMERICA & CARIBBEAN
+55 11 5189 8267
LAC_info@fico.com

EUROPE, MIDDLE EAST, & AFRICA
+44 (0) 207 940 8718
emeainfo@fico.com

ASIA PACIFIC
+65 6422 7700
infoasia@fico.com