



# Real-Time Payment Fraud Trends and How To Fight Them in Three Simple Steps

**ACI Worldwide®**  
Real-Time Payments



## Introduction



“

Combating a new wave of fraud and scams will require integrated approaches involving broad contextual analysis, federated machine learning and two-way communication with the customer.”

**Cleber Martins**  
Head of Fraud Management for Banking  
ACI Worldwide

Real-time payments are ready for exponential growth. According to the [2023 Prime Time for Real-Time](#) report, 195.0B real-time payment transactions were recorded globally in 2022, a year-over-year growth of 63.2 percent. With the adoption of online banking, real-time payments are increasingly being used for day-to-day purchases in place of cash. With an ever-changing payments landscape, there is an increased need to alter fraud prevention strategies to match.

Despite the multifarious benefits, real-time payments are also an attractive target to fraudsters, so they require real-time fraud detection. As payment limits increase and the technology evolves, fraudsters find new ways of committing financial crime. As banks have bolstered fraud prevention strategies, fraudsters have targeted the weakest link — the consumer. The availability of real-time transactions leaves banks, processors and financial intermediaries vulnerable to attack, with a tiny window to prevent fraudulent transactions and scams.

## Understanding the changing payments fraud landscape

Developed real-time payment markets are suffering an epidemic of social engineering scams and even kidnappings designed to convince — or coerce — individuals to transfer funds to accounts controlled by criminals. These authorized push payment (APP) scams pre-date real-time payments, but instant clearing, a strong supply of mule accounts and successes tackling other types of fraud have all made the “business case” stronger. Other terms for APP scams include “PIX fraud” in Brazil, “scams” in Australia and “APP fraud” in the U.K. This report uses the term “APP scam” to refer to the same problem.

## Shaping fraud defenses

As we think about the future of fraud management, methods will continue to evolve as the global adoption of real-time payments gains momentum. Banks must provide consumers with the products they need to meet their demands, but new payment offerings should be adequately protected. Combating a new wave of fraud and scams will involve integrated approaches, including broad contextual analysis, federated machine learning and two-way communication with the customer. With the right partner, banks and financial institutions can clamp down on payments fraud and scams.



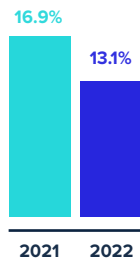
## Global Fraud Trends: From Physical to Digital

According to our [2023 Prime Time for Real-Time](#) report, there is a continued fraud trend from the physical to the digital. When assessing large real-time payment markets, we have seen that methods, such as APP scams, are reaching large numbers compared with card fraud. The data below shows that as other markets look to move towards real-time payments, they can learn from these trends.

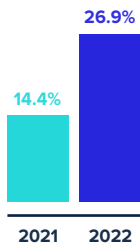


### ACI Prime Time for Real-Time Report

Card Details Stolen Online



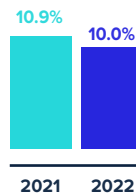
Confidence Tricks/  
APP Scams



Card Details Stolen/  
Skipped In Person



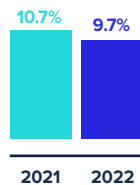
Bank Account Hacked



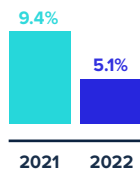
Identity Theft



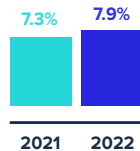
Card Lost or Stolen



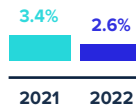
Other



Digital Wallet Account  
Hacked



Don't Remember



If banks and financial institutions work with the right provider, they can target these increasingly popular methods by using digital footprints to their advantage.



## Consumers at Greater Risk of Becoming Victim to Real-Time Fraud in Leading Real-Time Markets

### U.K.: Ready To Regulate

Real-time payments in the U.K. represent a 10.1 percent share of total payments volume in 2022 above the European regional average. Faster Payments has been live in the U.K. since 2008, and with continued real-time payments adoption and the planned launch of the New Payments Architecture (NPA) in 2025, real-time payments are expected to increase. By 2027, real-time payments will have overtaken paper-based payment transactions, reaching a 12.5 percent share of total payments volume. With the move from ISO 8583 to ISO 20022, NPA will provide rich data in payment messages, and therefore enable real-time fraud prevention.

In the meantime, authorized push payment scams continue to rip through the U.K. According to our [SCAMSCOPE](#) report, losses to APP scams will double from \$789M in 2021 to \$1,564M in 2026. Banks and regulators are continuing to grapple with the problem as the payment system regulator (PSR) is proposing that the liability be split between initiating and receiving banks. The data below shows a stark increase in APP scams compared with slow decreases of other payment fraud types in the last year:

### Keep Watch of Digital Wallet Accounts for Mule Activity

There is a trending increase in fraud being committed through the digital wallet account across all our focus markets. Of course, as consumers adopt digital payment methods, there will be more opportunity to exploit this. But we cannot ignore that digital wallet accounts can be used as mule accounts by fraudsters. Successful fraud management should consider this before these fraud tactics become more prominent than traditional card fraud.



2021-12.8% 2022-24.3%



2021-5.6% 2022-7.1%



2021-16.7% 2022-14.4%



2021-12.8% 2022-11.4%



## India: Real-Time Leader

India is the leading real-time market in the world. The Unified Payments Interface (UPI) disrupted the payments space by enabling payments through QR codes, mobile numbers and virtual IDs. Most real-time fraud takes place due to the massive influx of UPI, a major catalyst in the government's push for the adoption of digital payments as a key part of its larger Digital India mission. [According to the complaints reported on the National Cybercrime Reporting Portal \(NCRP\), UPI fraud rose by 23 percent in 2022.](#)

This shows that there is a large need for banks to focus strategies to use rich data from UPI transactions to tackle real-time fraud. One trend includes QR code fraud, in which

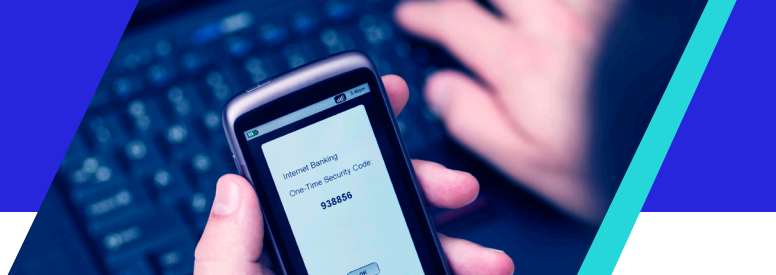
someone pretends to make a purchase with a QR code, but instead receives money as soon as the victim scans the QR code.

India has seen a stark increase of APP scams in recent years, doubling from 13.7 percent of all fraud in 2021 to 25 percent in 2022. According to our recent [SCAMSCOPE](#) report, losses to APP scams are expected to almost double from \$330M in 2021 to \$612M in 2026. The data below shows a stark increase in APP scams compared with slow decreases of other payment fraud types in the last year.

### APP Scams Are the Ones To Watch

In all of these large real-time markets, [confidence tricks, also known as APP scams, have considerably increased, at least doubling from 2021 to 2022.](#) In conjunction with this, the share of fraud attacks from card details stolen in person has decreased across the board. As fraud detection systems have become more sophisticated, fraudsters have turned their eyes to a more vulnerable and unprotected part of the financial services chain — bank customers themselves. Fraudsters trick bank customers to unknowingly unauthorize the fraudulent transaction or take their identity and make it seem like they have authorized it. Successful fraud management should consider this before these fraud tactics become more prominent than traditional card fraud.





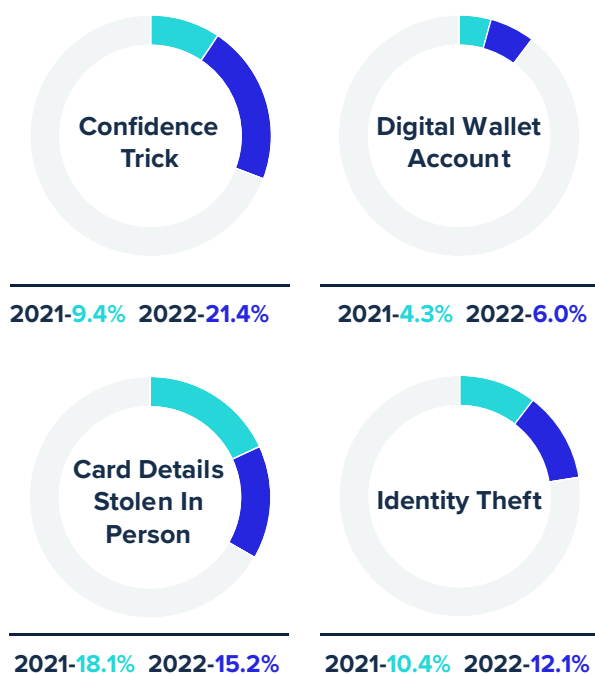
## Brazil: Protecting Financial Inclusion Growth

Our [Prime Time for Real-Time](#) report data shows that in 2022, Brazil was the second biggest and most developed real-time payments market in the world, behind only India. Its real-time payment systems represented a 16.1 percent share of total payments volume in 2022. This is thanks to the rapid adoption of PIX, a mobilebased real-time payments scheme introduced in 2020. With all of its benefits, PIX is undoubtedly the future of payments in Brazil. But, when it was launched in October 2020, [Sao Paulo saw a 40 percent rise in kidnappings](#). The Brazilian central bank subsequently implemented a \$200 transfer limit on P2P payments made overnight.

However, we continue to see a surge in APP scams, also known as PIX fraud, having almost tripled from 12 percent of all fraud in 2021 to just under a third (28.5 percent) of all fraud in Brazil in 2022. Maintaining confidence in digital payments with the right fraud strategies is vital to realizing PIX's huge potential, which will be accompanied by significant societal benefits, including increasing financial inclusion, economic growth and prosperity.

## Australia: Mature Market With Room To Grow

The New Payments Platform (NPP) is the national real-time payments infrastructure in Australia. Having been made available to nearly 90 million customer accounts, real-time payments accounted for just 6.1 percent of the total payments volume of transactions in 2022, expected to increase to 16.3 percent by 2027. Much like our other spotlighted markets, Australia is facing an epidemic of scams: [Australians lost a record \\$3.1B \(Australian Dollars\) to scams in 2022, an 80 percent increase from 2021](#). According to ACI's [Prime Time for Real-Time](#) report, scams have more than doubled from 9.4 percent in 2021 to 21.4 percent of all fraud in 2022. It is becoming critical for financial institutions in the market to have the right strategies in place to protect their reputations, losses, and most importantly, consumers, from scams.

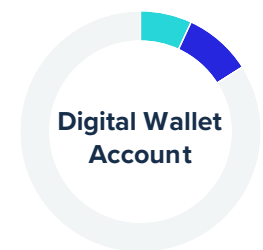




## U.S.: Time To Prepare

Real-time payments are still only a small piece of the overall payments mix in the U.S., accounting for only a 1.2 percent share of the total payments volume in 2022. The growth of real-time payments will benefit from the launch of FedNow in July 2023. As of now, Regulation E states that banks must reimburse victims of ‘unauthorized fraud’, meaning consumers are covered for any payment that was not authorized by themselves. But this regulation does not cover authorized payments, even under false pretences,

illustrative of the regulatory gray areas. There is no reason to assume that without action, the U.S. will not follow the path to crisis levels of APP scams as seen in other markets, [with APP scams almost tripling from 7.4 percent in 2021 to 18.6 percent of all fraud in 2022](#). In the wake of FedNow’s launch, the U.S. is in a prime position to learn from other market’s real-time payment fraud journeys and implement strong fraud strategies.



2021-7.4% 2022-18.6%

2021-6.9% 2022-9.1%



2021-23.0% 2022-16.9%

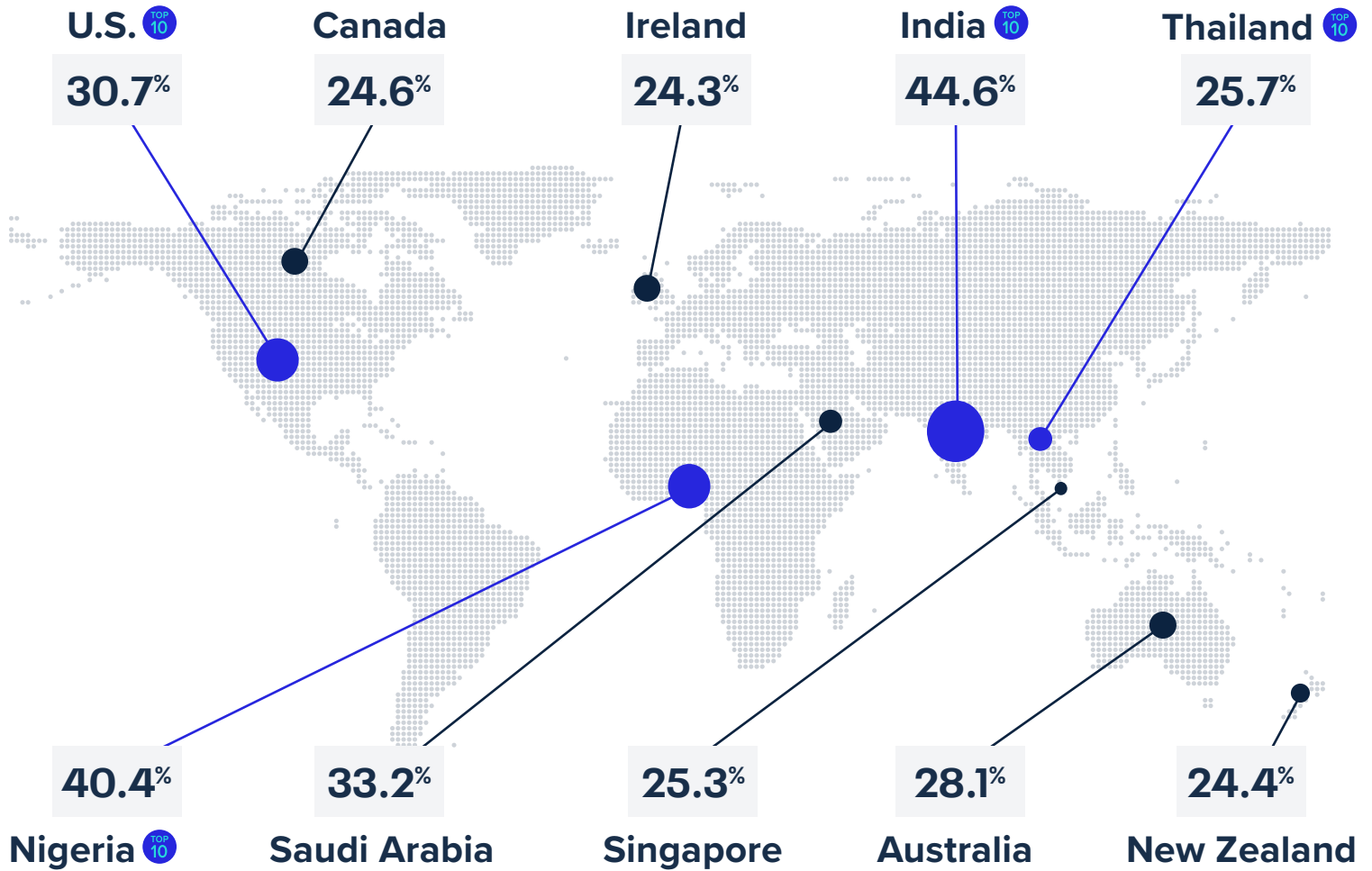
2021-18.7% 2022-15.6%



## Consumers at Greater Risk to Falling Victim of Real-Time Fraud in Leading Real-Time Markets

Top Ten Countries (Fraud Victims, 2022)

**TOP 10** A Top-Ten Market for Real-Time Payment Transactions





## Three Simple Steps To Fight Real-Time Payments Fraud

Technology is enabling fraudsters to scale their crimes. The same technology can be used by banks and financial institutions to build advanced fraud processes and systems to protect banks and their customers and protect the consumer link in the chain.

### 1 | Protect enterprise-wide transactions with contextualized decisioning

Banks and financial institutions need sophisticated enterprise-wide fraud prevention tools that use a broad range of contextual decisioning to reduce their fraud costs. This decisioning needs to be based on key factors, such as biometric data, digital identity, confirmation of payee and telco intel through collaboration. Banks must do this not only on the initiating end, but must also use this technology to monitor incoming transactions on the receiving end. This data can create behavioral profiles, lists and rules to inform risk-based authentication decisions, improve onboarding risk management and shut down mule accounts.

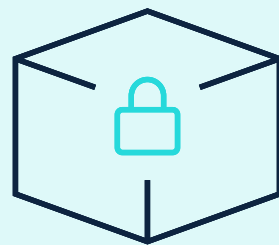
### 2 | Accelerate decision making with machine learning

Increase decision making speed for the real-time world. This will decrease the number of false positives and improve operational efficiency, enabling banks and financial institutions to catch more fraud. This is needed in conjunction with our first step, as machine learning models are only as good as the signals they have been given.

### 3 | Strengthen the weakest link with two-way communication

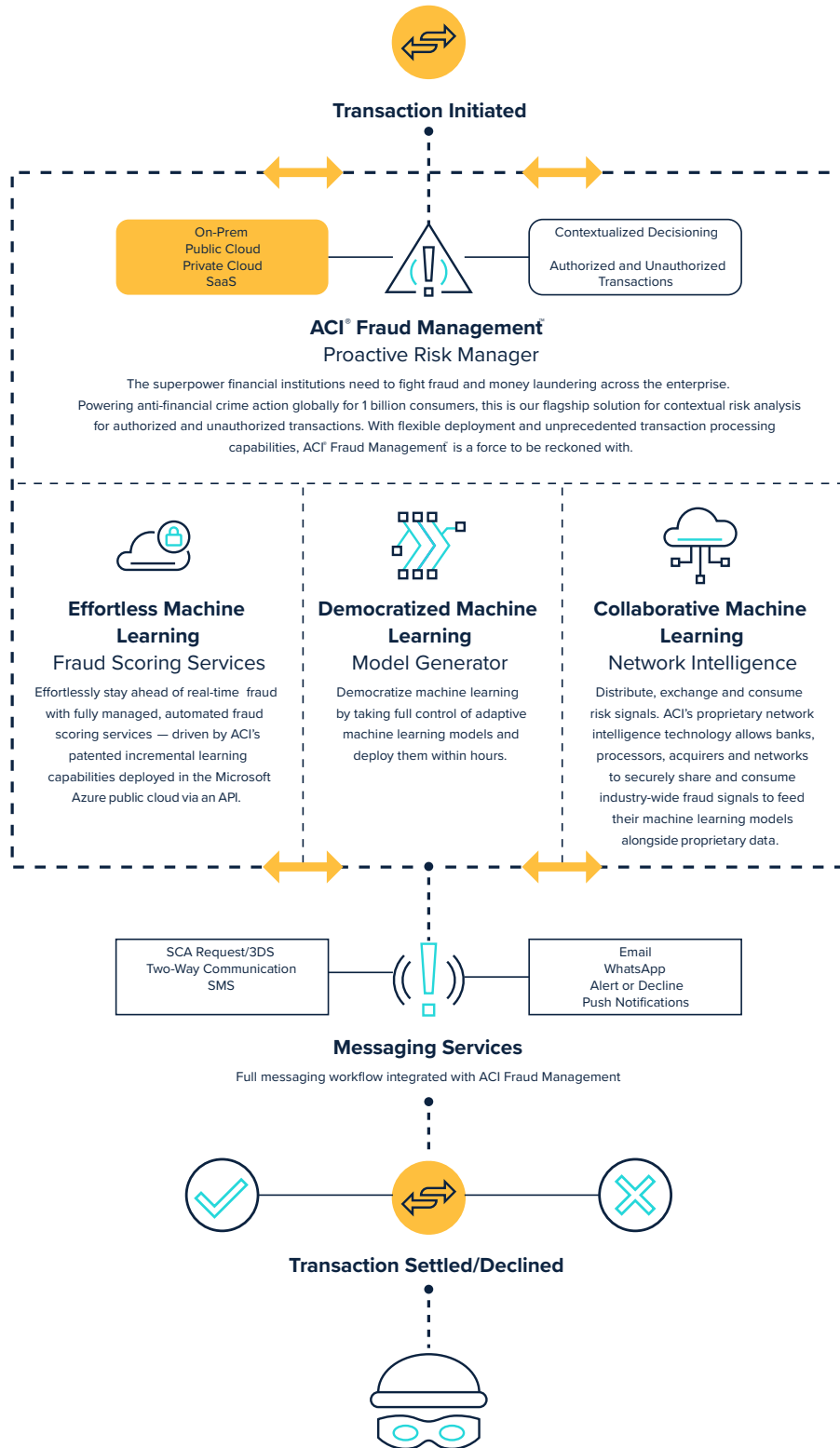
As fraudsters increasingly identify the consumer as the weakest link, make them a part of your fraud team. Send customers a simple SMS, push alert or email instantly when a fraudulent transaction or scam is suspected. This step is important for monitoring outgoing transactions, but steps one and two are important for covering all bases for incoming transactions, too.

With an effective three-pronged approach, a seamless customer payments experience will not be impeded. Collaborating in the right way will not infringe on a financial institution's differentiating fraud controls or on data privacy. Having the right tools to send risk signals, with privacy designed into the process, allows banks to protect customers from all corners.





## Placing AI Capabilities Directly in the Hands of Fraud Teams





By going on ACI's fraud management journey (depicted in the infographic above), financial institutions can arm themselves with the right fraud strategies to capitalize on the opportunity to bring real-time payments to market, without fraud management becoming a cost center. ACI helps banks improve their detection rate, decrease fraud losses and improve false positive ratios to:

- **Reduce losses from fraud.** Turn fraud prevention from a cost center to a revenue generator
- **Generate new revenue streams.** Facilitate real-time payments seamlessly in the way the customer needs, as well as facilitate more transactions
- **Make life easier for customers.** Less burden on the customer in terms of verification, with the knowledge their money is safe

[Our customers have seen the following results for 1 billion consumers across the world:](#)

- Fraud scoring services increase fraud detection rates by up to 35 percent and achieves 3:1 false positive rates
- ACI's model generator functionality has enabled detection rates of 80 percent at the largest public sector bank in Asia
- ACI's model generator has provided a false positive rate of 4:1, with a detection rate of 70 percent.

- Everlink improved CNP fraud detection rates by 11 percent utilizing the ACI® Fraud Management™ solution, with a detection rate of 85 percent and a 6.4:1 false positive rate.
- A large North American bank is seeing fraud detection rates of 95 percent with a false positive rate of 3:1.

Globally, real-time payments technology is still in its infancy, and the time has never been better for retail banks, processors and acquirers to be a wave-maker in financial crime prevention.

Use our calculator to see how much our fraud management services options would cost your business.



ACI Worldwide is a global leader in mission-critical, real-time payments software. Our proven, secure and scalable software solutions enable leading corporations, fintechs and financial disruptors to process and manage digital payments, power omni-commerce payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with a local presence to drive the real-time digital transformation of payments and commerce.

#### LEARN MORE

[www.aciworldwide.com](http://www.aciworldwide.com)  
[@ACI\\_Worldwide](#)  
[contact@aciworldwide.com](mailto:contact@aciworldwide.com)

#### CONTACT ACI

Americas +1 402 390 7600  
Asia Pacific +65 6334 4843  
Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide, Inc. 2023

ACI, ACI Worldwide, ACI Payments, Inc., ACI Pay, Speedpay and all ACI product/solution names are trademarks or registered trademarks of ACI Worldwide, Inc., or one of its subsidiaries, in the United States, other countries or both. Other parties' trademarks referenced are the property of their respective owners.

**ACI Worldwide®**  
Real-Time Payments