ACI Worldwide Scamscope Report Finds APP Scam Losses Expected To Hit $6.8 Billion by 2027

December 5, 2023

- Losses to APP scams are expected to record an average CAGR of 11% from 2022-2027 across analyzed markets.
- APP scam losses are expected to grow at almost 50% of the CAGR of real-time transaction value.
- Report outlines scam defense strategies, which include creating an intelligence-sharing network, embracing responsible AI and boosting consumer education.

MIAMI--(BUSINESS WIRE)--Dec. 5, 2023-- Authorized Push Payment (APP) scam losses are on the rise and expected to climb to $6.8 billion — a combined compound annual growth rate (CAGR) of 11% — by 2027 across six leading real-time payment markets (U.S., U.K., India, Brazil, Australia and Saudi Arabia) according to Scamscope, a new report by global payments software company ACI Worldwide and GlobalData, a leading global analytics firm. During the same period, the overall value of real-time transactions is also forecasted to grow at a faster pace, reaching 25% CAGR.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20231204840417/en/

(Graphic: Business Wire)

APP fraud scams involve fraudsters tricking their victims into willingly making large bank transfers to them – in many cases, this happens via social engineering across social media networks or via telephone. “As real-time payments surge forward, the slower yet disconcerting rise of APP scams puts regulators under pressure to define accountability and assign liability,” commented Cleber Martins, head of payments intelligence and risk solutions at ACI Worldwide. “A cross-industry payments intelligence model for sharing anonymized fraud intelligence signals can strengthen the insights for automated AI systems and facilitate collaboration in real time to profile transaction risk without compromising IP, data privacy or compliance obligations.”

Fraud prevention key to unlocking sustainable growth in real-time payments

Among the markets covered in the report, Saudi Arabia and Brazil are the top two markets with the highest CAGR in scam loss value and among the top three with the highest CAGR in real-time payments value. This implies a concerning correlation between the increase in scams and the expanding volume of real-time payments and underscores the importance of addressing scams within the rapidly growing landscape.

In Brazil, scammers are exploiting PIX’s success, benefiting from a lag in the development of processes and tools to detect fraudulent transactions. This hinders the identification of mule accounts used to transfer stolen funds. In Saudi Arabia, a nascent real-time payments market, scams seen in more established real-time payment markets are now emerging here as well. With centralized regulatory control, there is an opportunity to encourage banks to improve both data quality and collaboration to combat mule networks.

Real-time payments leap ahead of APP scams, yet caution prevails

APP scam losses in the U.S. are projected to increase by 9% from 2022 to 2027. However, real-time payments adoption fueled by the FedNow Service is projected to surpass this growth, with a remarkable 41% CAGR. With the expanding scope of real-time payments, banks should seize the opportunity to adopt a proactive stance toward preventing fraud.

India mirrors the U.S. trend, with APP scam loss value significantly lower than the real-time transaction value. Indian banks are turning the tables on scams with proactive fraud management. For example, the Indian Banks Association suggested fixing a threshold limit of transactions for newly opened accounts. These efforts would be bolstered by a network intelligence framework to share vital data signals and by leveraging AI and machine learning to spot transaction abnormalities.

Regulatory mandates put banks on the hook for scam victim reimbursement

According to the Scamscope report, APP scam losses in the U.K. hit more than $587 million in 2022. Mounting consumer losses are driving market trends toward regulatory mandates, compelling financial institutions to compensate scam victims. In June 2023, the U.K.’s Financial Services and Markets Bill came into effect, requiring banks to reimburse the victims of APP scams.

With APP scam losses expected to reach $1.5 billion by 2027, Australians have implored their government to follow the U.K.’s lead. Banks have pushed back, contending that telecom and social media firms should also bear responsibilities. The Australian Competition and Consumer Commission calls for a united front across public and private sectors to combat scams. Recently, the Australian banks came together to form a new Scam-Safe Accord - a confirmation of payee system that will help reduce scams by ensuring people can confirm they are transferring money to the person they intend to.

The report outlines four key recommendations for financial institutions to tackle the issue

- According to the Scamscope report, approximately 3 out of 10 fraud victims close their accounts, posing financial consequences for banks. There is also increasing pressure on regulators to hold banks accountable for fraud. Banks must get ahead of regulatory mandates to fortify control and build trust.
- APP scams are a cross-industry problem that requires solutions, techniques and intelligence shared among financial institutions, the government, telcos and social media tech companies. Seamless collaboration is needed to combat social engineering, liability disputes and mule account scams.
- By closely monitoring both incoming and outgoing transactions and analyzing account behavior, banks can break the mule account chain and detect mule accounts associated with synthetic or stolen identities and instances of account takeover.

- In the AI-driven era, a proactive approach is paramount to combat scammers. Leveraging diverse data signals and advanced technologies like voice biometrics enables institutions to understand customer intent, prevent emerging AI threats and safeguard customer relations.

Scamscope key findings at a glance:

- APP fraud losses by country 2022-2027
  - Australia: $793-$1,522.9 million
  - Brazil: $246.7-$635.6 million
  - India: $393.7-$611.9 million
  - Saudi Arabia: $25.3-$81.5 million
  - U.K.: $587.2-$934.7 million
  - U.S.: $1,939.9-$3,030.8 million

- CAGR of APP scams value vs. CAGR of real-time transactions value (2022-2027)
  - Australia: 14% vs. 24%
  - Brazil: 21% vs. 26%
  - India: 9% vs. 22%
  - Saudi Arabia: 26% vs. 34%
  - U.K.: 10% vs. 22%
  - U.S.: 9% vs. 41%
- Top 3 APP fraud scams by country
  - Australia: Outstanding Balance (33%), Product (22%) and Investment (22%)
  - Brazil: Advance Payment (27%), Product (20%) and Investment (17%)
  - India: Product (42%), Investment (21%) and Advance Payment (16%)
  - Saudi Arabia: Product (33%), Investment (16%) and Advance Payment (14%)
  - U.S.: Product (23%), Investment (23%) and Advance Payment (17%)
  - U.K.: Advance Payment (25%), Product (24%) and Investment (19.5%)

Note to editors:
*Authorized push payment (APP) scams: The term describes a method of fraud in which criminals coerce legitimate users to initiate a payment to a destination account under their control. Funds leaving legitimate customers' accounts will travel through one or several mule accounts before being collected by the fraudsters or converted by them into hard-to-trace digital assets, such as crypto or NFTs. Other terms for APP scams include "PIX fraud" in Brazil, "scams" in Australia and "APP fraud" in the U.K. This report uses the terms "APP scam" and "scams" interchangeably to refer to the same problem.

About ACI Worldwide

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.

© 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.

View source version on businesswire.com: https://www.businesswire.com/news/home/20231204840417/en/

Media

Nick Karoglou | Head of Communications and Corporate Affairs | nick.karoglou@aciworldwide.com

Lyn Kwek | Communications and Corporate Affairs Director, APAC/South Asia | lyn.kwek@aciworldwide.com

Source: ACI Worldwide