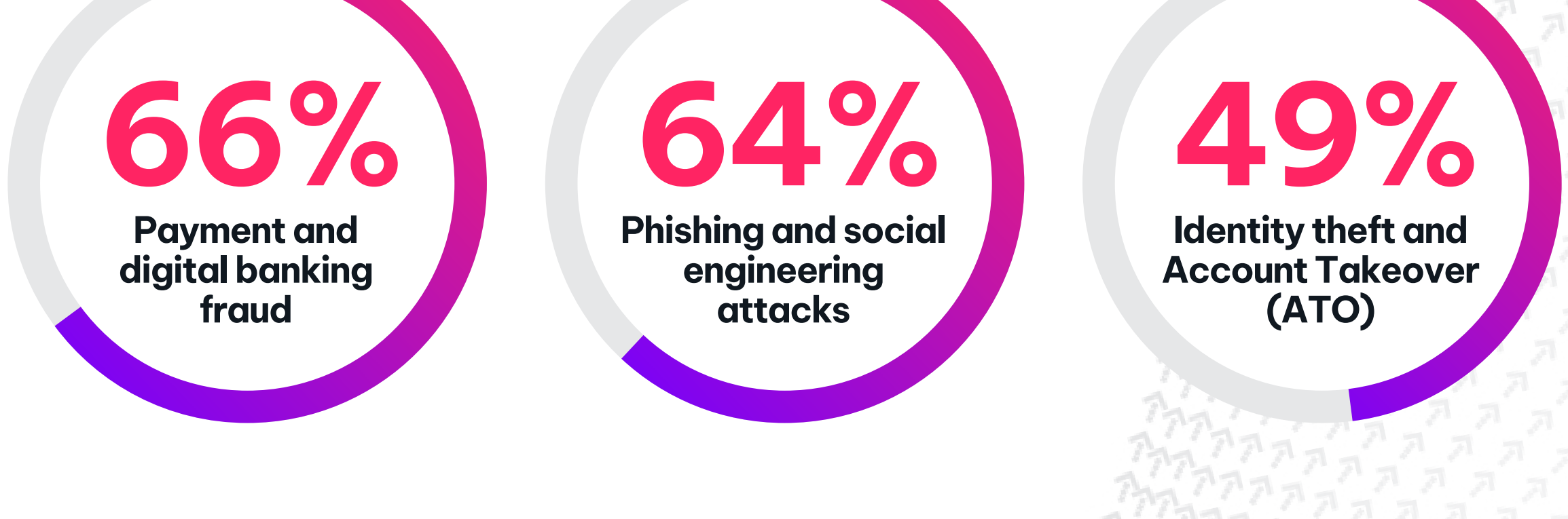NICE **Actimize** | **R2** Regulation Asia

FRAUD BAROMETER 2024

New Faces of Fraud: How Asia's Financial Sector is Responding to the Evolving Threat Landscape

In the latest financial year 2023-2024, over 114 fraud risk practitioners operating predominately across nine countries in APAC ranked the most common fraud threats their financial institutions (FIs) face:

66% Payment and digital banking fraud

64% Phishing and social engineering attacks

49% Identity theft and Account Takeover (ATO)

According to the respondents, FIs are focused on improving fraud detection and prevention by investing in technologies such as:

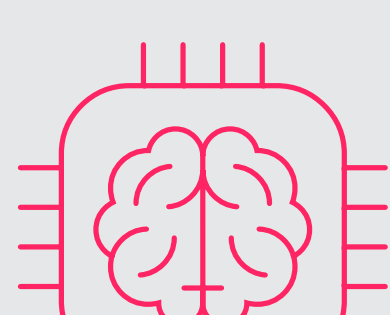**Advanced analytics** **Biometrics** **AI** **Machine learning**

Though use of advanced tools in fraud risk management is still limited, adoption of such tools is expected to increase over time.

Across Asian markets, research showed real-time payment systems are widespread, driven by a mobile-first consumer base. FIs will need to strike a balance between consumer demands for speed and convenience with robust security measures to reduce unauthorised account access. Suggested measures include implementing multi-factor authentication, using behaviour analysis to detect transaction anomalies and leveraging AI to conduct real-time fraud analysis.
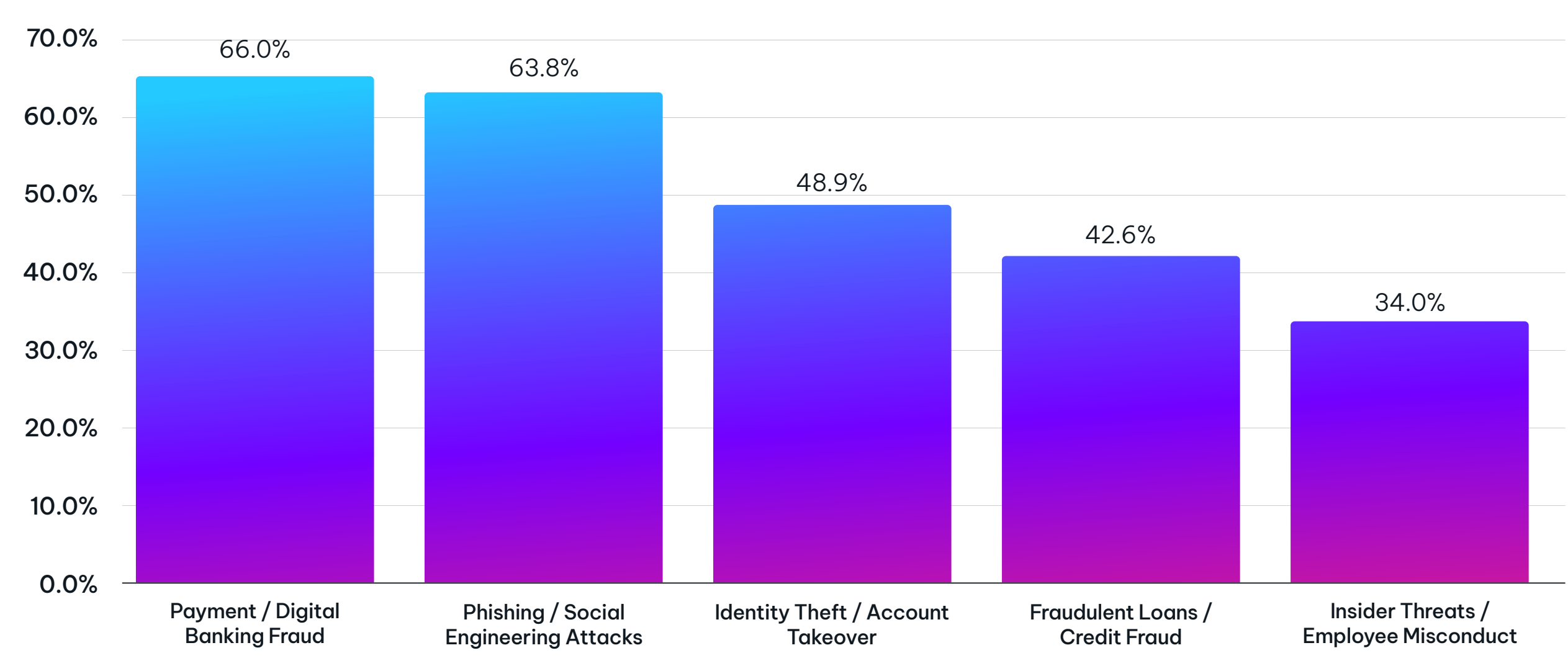
A surge in digital transactions has inevitably led to increased cyber related frauds, including **phishing attacks, online scams, and data breaches.** Meanwhile, traditional and emerging financial fraud typologies, including bank and credit card fraud, continue to plague the region.

Phishing and social engineering attacks have become a significant fraud risk within Asian economies, exploiting human psychology and the region's deep engagement with digital technologies. These attacks often involve tricking individuals into divulging confidential information, such as bank account details, passwords, or personal identification numbers, which are then used for fraudulent purposes.
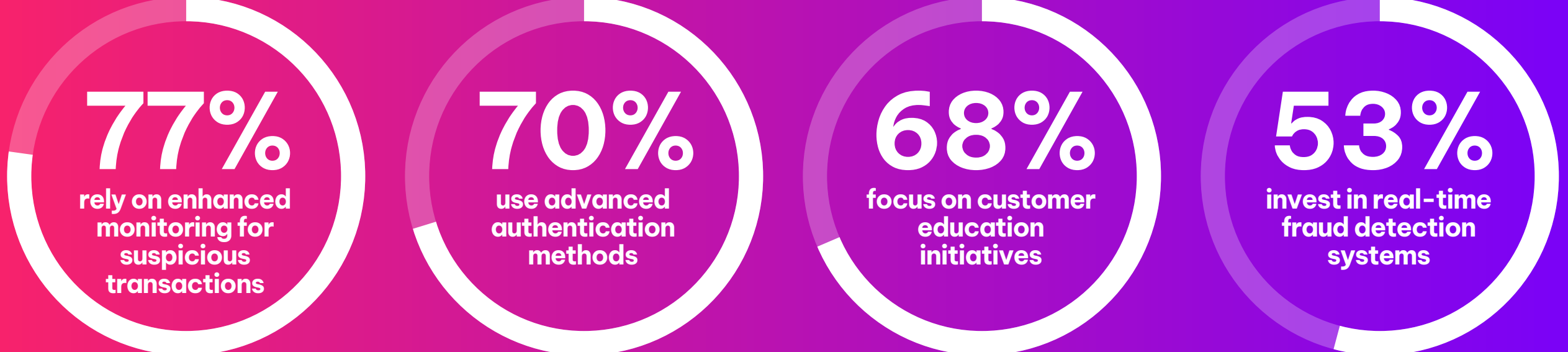
49% of the respondents said their organisations encounter payments and digital banking fraud at least monthly, with

8.5% reporting that they encounter such activity almost daily.

Top 5 Fraud Typologies (Past 12 Months)

Typology	Percentage
Payment / Digital Banking Fraud	66.0%
Phishing / Social Engineering Attacks	63.8%
Identity Theft / Account Takeover	48.9%
Fraudulent Loans / Credit Fraud	42.6%
Insider Threats / Employee Misconduct	34.0%

Most frequently adopted measures respondents use to address the threat of digital banking fraud

77% rely on enhanced monitoring for suspicious transactions

70% use advanced authentication methods

68% focus on customer education initiatives

**53%** invest in real-time fraud detection systems

Over three-quarters of respondents believe their institutions are agile and able to adapt to emerging fraud schemes and tactics, with

36% saying they are **"highly agile"** and
32% saying they are **"moderately agile"**

36% highly agile
32% moderately agile
average/ reactive/ uncertain
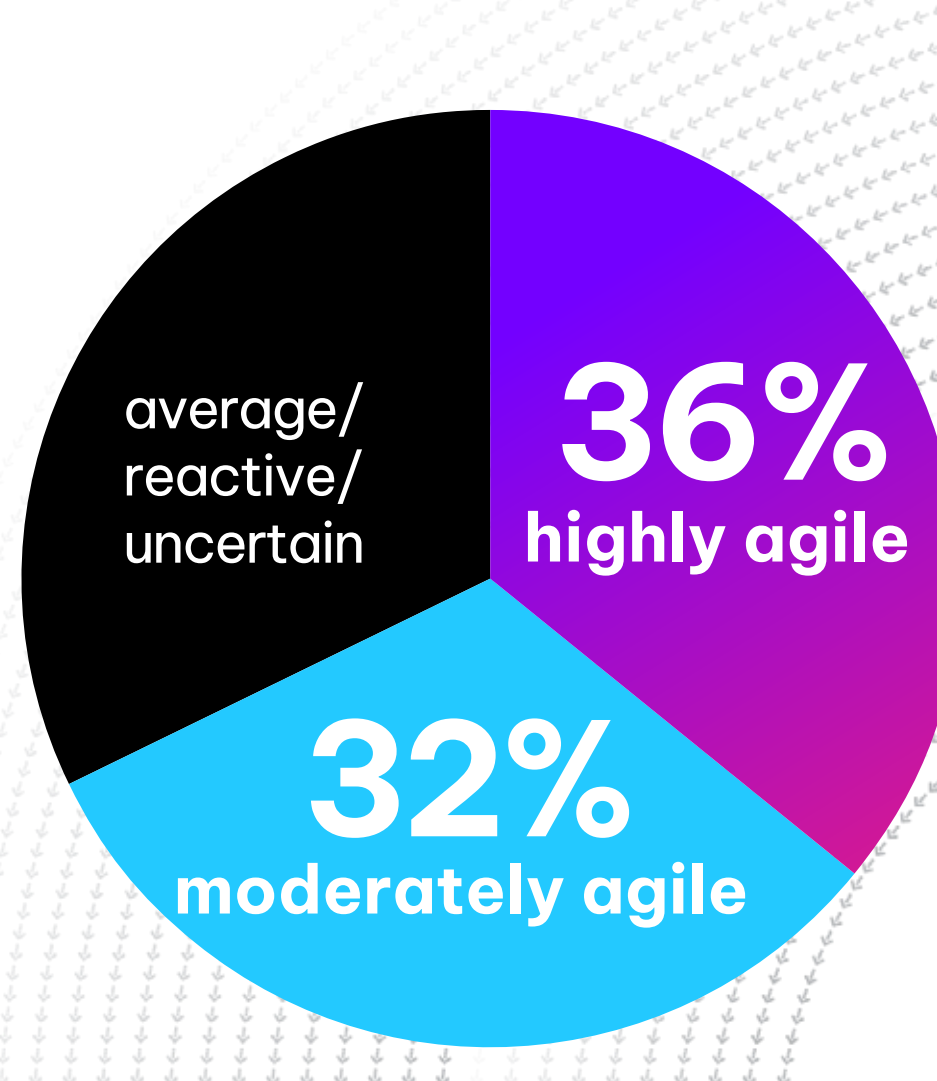
Strategies to prevent ATO

Respondents report conducting regular security awareness training, using enhanced authentication methods, and collaborating with law enforcement agencies and industry partners. **34%** said their fraud strategies involved sharing information with other FIs.
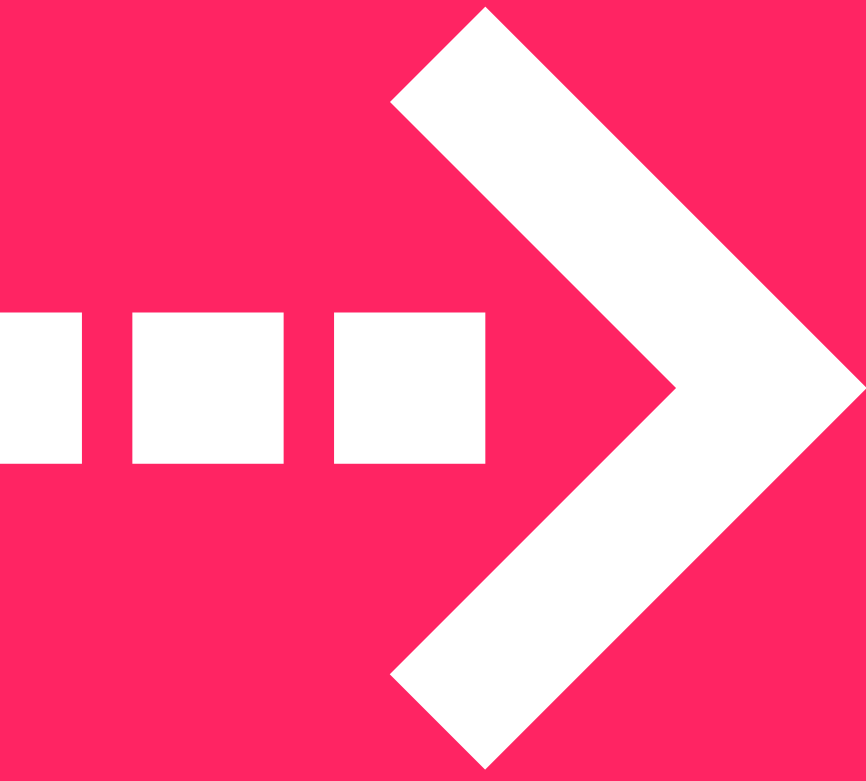
On the regulatory front, there's concern around the introduction of new fraud loss share models in APAC, with Australian respondents expressing unease with proposed new requirements, while other regions are taking a "wait and see" approach until regulations are finalised.

More industry insights are in the latest Fraud Barometer report. Explore the current state of fraud in Asia, efforts being made to enhance fraud detection and prevention capabilities with technology, and the emerging trends and threats in the region.

Get the report ›