

NEWSLETTER

GAMETECH- A RISING STAR IN THE FINTECH

#1

It's quarantine, and Sam is busy playing Among Us with his friends. As he progressed through levels, Sam wanted to upgrade his avatar to match his friends. That's when he came across the in-app buy button. As he had linked his cards to Google, Sam immediately purchased the avatar and continued his gaming journey.

Now you might be wondering, why is gaming featured in a fintech newsletter? Well, here is our unique angle to it:

GameTech is a fresh vertical that combines financial technology and the gaming industry into one.

With the onset of the pandemic, Gamification has integrated itself with our lives. Paradoxically, this lockdown also saw increased connections with the family through heritage games like ludo. However, many had also turned to mobile gaming as part of their lockdown activities.

Most online games offer in-app purchases that enhance a player's gaming experience, like upgrade their avatar or unlocking bonus features that help them advance in the game. This means that thousands of gamers are now opening their digital wallets to take advantage of the slashed prices and limited offers that are often irresistible to pass up.

This is why online gaming is now a part of the fintech ecosystem.

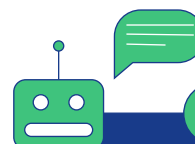
According to Newzoo, the games market will account for \$174.9 billion by the end of this year. This figure is a \$15.6 billion increase from a forecast done in the beginning stages of COVID.

On a global scale, online gaming was once dependent on credit cards and ATMs for purchases. But since then, the gaming industry had rolled out a robust payment structure to streamline gamers' transactions.

India's gaming market is projected to be \$1 billion by 2021, a significant increase from \$260 million in 2016. Indian gamers view it as a competing platform to bond with their friends. This mindset has run deep in India's Tier 2 and Tier 3 cities, where the adoption of apps and in-app purchases is the highest. A result of this consumer behavior has led to revenue generated from customizable avatars and virtual coin packs arising from the apps. Revenue was also generated from ads that gamers needed to watch to receive extra features in the game.

This response has prompted e-gaming businesses to change their models from download volumes to one engineered on consumer engagement and experience. With more than 400 gaming start-ups trying to make online games interactive for India's 500 million smartphone users, the game tech industry looks at two-folding investments within a few years.

Gametechnology in India is a market worth tapping into for its immense potential. With the current scenario, we hope to see India become a key player in online gaming in the coming years.



FINTECH FACTS

Chatbots will save banks \$7.3 billion by 2023.



<https://twitter.com/poweredbyyap>



<https://www.linkedin.com/company/yapfromm2p/>



<https://medium.com/m2p-yap-fintech>

PCI DSS - A QUICK GUIDE TO ITS LEVELS

#2

PCI DSS stands for Payment Card Industry Data Security Standard. A collaboration between top reputed credit card brands such as American Express, Discover, JCB, Mastercard, and Visa in 2004 resulted in PCI DSS launch. Organizations who store or process, or transmit the cardholder data either as clear or in an encrypted manner should comply with PCI regulations.

A short survey showed that most people give the above description when quizzed about PCI-DSS. When we further probed about the levels present in this compliance, we came up short. So, here is a quick read of the PCI-DSS compliance levels.

PCI DSS Compliance levels

Divided into four levels, the PCI Compliance levels are based on the number of credit or debit card transactions processed by a business annually. These levels determine what needs to be done by an enterprise to remain compliant.

Level 1:

Applies to merchants who process more than six million real-world credit or debit card transactions annually. An authorized PCI Qualified Security Assessor will conduct an annual internal audit and an on-site evaluation of the organization to:

- Authenticate the assessment's scope;
- Evaluate technical information and documentation;
- See whether the PCI-DSS standards are being met
- Assist and guide the compliance process and
- Also, evaluate the compensating controls

On successful evaluation, the QSA will present an RoC (Report on Compliance) to the organization's acquiring bank, thereby demonstrating its compliance.

Level 2:

Applies to merchants who process between one and six million real-world credit or debit card transactions. Security testing reports on network hosts and applications should be completed on a defined frequency. The RoC is also applicable for level 2 organizations.

FINTECH FACTS

Consumers who do not use payment apps cite the ease of traditional payment methods as the main reason for sticking with them.

Level 3:

Applies to merchants who process annually between 20,000 and one million e-commerce transactions. A yearly assessment must be done using the relevant SAQ (Self-Assessment Questionnaire) along with a quarterly PCI scan.

Level 4:

Applies to merchants who process annually fewer than 20,000 e-commerce transactions or those who process up to one million real-world transactions. They must complete a yearly assessment using the SAQ and a quarterly PCI scan

What is this Self-assessment questionnaire?

PCI-DSS lists several kinds of SAQs for every level, and it is also based on how the merchant processes card information. Given below are some of the types of SAQs applicable to levels 2-4:

SAQ A: Merchants who outsource their entire card data processing to certified third parties. The transactions also include e-commerce transactions.

SAQ A-EP: Applies to E-commerce merchants who outsource their payment processing but not the site's administration.

SAQ B: Applies to E-commerce merchants who don't receive cardholder data, but they have control over the process through which data is redirected to a third-party payment processor.

SAQ B-IP: It applies to merchants who don't store cardholder data in electronic form but will use IP-connected point-of-interaction devices. These merchants may handle either card-present or card-not-present transactions.



SAQ C-VT: Applies to merchants who process cardholder data via a virtual payment terminal.

You must select the right SAQ because every level has compliance requirements based on how payment card data is processed.

How to become a PCI DSS compliant:

The PCI DSS specifies six control objectives for an organization to achieve compliance:

- Build and maintain a secure network
- Implementing strong access control measures
- Protect cardholder data
- Regular monitoring and testing of networks
- Maintaining a vulnerability management program
- Maintaining an information security policy

The penalties of non-compliance:

As cardholder data is considered personal data, a PCI DSS breach can also be regarded as equal to a GDPR breach. If PCI regulations are not adhered to, organizations will face severe financial penalties or even lose their facility to accept card payments.

In short, PCI-DSS is a standard that ensures trust, business continuity, and safety of the cardholder data

REGION WISE FINTECH UPDATES

#3

UK

After the recent fundraising events, the Buy Now Pay Later pioneer, Klarna, has bagged a hefty valuation of \$10B, making it one of the world's top 5 highly valued private fintech firms. To stir a healthy competition in the European BNPL ecosystem, the Australian Fintech pinnacle, AfterPay, acquires Spanish firm Pagantis.

USA

CX is the next big game for Californian FinTechs like Robinhood. It's time for teens to get a grip on financial literacy, says Founder of Step, CJ MacDonald. From 60K to 4M Gen-Z and millennial users, Cleo has rapidly grown its user base, with more than 95% of customers prevailing in the USA.



FINTECH FACTS

Digital banking services are taking over: 46% of people exclusively use digital channels for their financial needs.

CHINA

The new risk control mandates reiterate that the core finance remains the same for both banks and fintechs. As a result, CBIRC (China banking insurance & regulation commission) and its central bank pose a pause for the long-awaited IPO of Ant Financial.

FINTECH FACTS

82% of traditional financial companies plan to increase collaboration with fintechs in the next 3-5 years.



MENA

The central bank of the UAE, along with ADGM, has opened its new Fintech office and kicked off a wholesale central bank digital currency project ABER, focusing on developing advanced cross-border payments. Finally, Amazon rebrands PAYFORT as Amazon payment services to start offering businesses competitive online payment processing.



“ Security is not an act, it is a habit ”

- Kannan Raju,
Vice-President, IT infrastructure