DAY -39, DAILY REPORT, 11 -01 -2021 (TUESDAY)

Today, I had an experience. When I woke up in the morning, it gave me a positive vibe and the cab came to the apartment and I went to the company or office. In the morning session I have continued the book called Securing digital payments like Real-time payment (RTP) technology that allows for instant settlement of digital transactions between individuals and/or businesses without needing to wait for clearance. In recent years, it's been generating buzz in the U.S., primarily for its efficiency, and may become the next big trend in payment technology in 2022. Recently, 130 financial institutions are working on implementing real-time payments into their existing infrastructures and the Federal Reserve plans to use the RTP platform in 2023. For individuals, real-time payments can mean not having to wait to move funds from a mobile payment app to a bank account. For retailers and businesses, it can mean faster payroll processing or the ability to liquify funds in an instant. s mobile, invisible and real-time payments all increase in popularity, protecting against theft and fraud will be top of mind for institutions and individuals. To protect against cyber-attacks and identity theft, more organizations are turning to mobile biometric technologies. Biometric authentication will secure $2 trillion in mobile and in-store transactions by 2023, according to Juniper Research. Smartphones using biometric hardware like facial recognition and iris scanning are expected to exceed 1 billion devices over the next five years, according to Juniper

Research. Biometric technologies are finding new ways to verify payments. Amazon has begun implementing palm-scanning verification technology in its brick-and-mortar shopping experiences. These trends represent major shifts in the payments space and we're only scratching the surface of what's to come. Payment security involves **the steps businesses take to make sure that their customers' data is protected and to avoid unauthorized transactions and data breaches**. Important aspects of payment security include following protocols such as PCI Compliance and 3-D Secure (3DS) and the Payment security has multiple layers and different requirements depending on the type of business you operate. With eCommerce showing no signs of slowing down, it's more important than ever for credit card issuers *and their merchant customers* to implement robust payment security. Multiple layers of payment security are required to protect your business from processing fraudulent transactions, for which you could be liable. Compliance plays a critical role in how payment security is designed and implemented. Let's explore how one of the most common standards shapes payment security requirements. Payment Card Industry Data Security Standard (PCI DSS) is a standard that aims to make payment security consistent worldwide. Any organization that processes, transmits, or stores cardholder data must comply with PCI DSS requirements. These requirements shape how payment security is implemented and evolve to reflect changes in new fraud prevention techniques. How your business proves PCI compliance will depend on how

many transactions you process annually. There are four merchant levels businesses can fall into, with Level 1 having the strictest requirements and Level 4 having the least. For instance, at Level 4, merchants can demonstrate their compliance through a self-assessment, while Level 1 requires them to submit to an external audit conducted by a certified security assessor. Different integrations with payment gateways can lower a merchant's required compliance level if the transaction takes place in the payment processor's environment versus on the merchant's own website. No matter how many transactions you process, having the right payment security in place will help you pass PCI compliance and prevent fraudulent transactions in your business.Types of Payment Security - Tokenization - Tokenization secures transactions by replacing payment information with randomly generated strings of characters. These tokens allow businesses to provision customer accounts, set up scheduled payments, and manage payment settings without handling sensitive cardholder information each time. Tokens use a public and private key to work. The public key allows for token creation, while the private key allows the merchant to issue single or recurring payments. This form of payment security helps ensure cardholder data is stored securely and reduces the amount of times payment information is transmitted over the internet. Thank you, that's all for today.