FAQs
QuickPay Powered by DBS
LAST UPDATED: 1 October 2020

1. What is QuickPay Powered by DBS?

   QuickPay™ is a safe and convenient way to pay MCST bills developed by DBS Bank in collaboration with Singapore-based proptech company, IBASE Technology Pte Ltd. Payments are made safely and securely on the FAST network using PayNow QR codes. QuickPay™ helps your estate go paperless and saves cost while at the same time eliminating risk of cash mishandling. Unlike cash or cheques which can be misplaced, digital payments are recorded and tracked electronically.

2. What safeguards are in place to ensure payments are handled safely and securely?

   The payments infrastructure used for QuickPay is regulated under the Payment Services Act, 2019, of Singapore, and QuickPay has a robust governance framework in place with operational controls to manage and mitigate technology risks.

   The Payment Services Act was introduced by the Monetary Authority of Singapore (MAS) as a framework to regulate payment systems and payment service providers and to safeguard funds owed to consumers and/or merchants.

3. How does QuickPay™ save money for my estate?

   Payments collection through offline methods like cash or cheques, or even GIRO and FAST, are inefficient because these require manual data entry and invoice reconciliation. With QuickPay™, transaction details are captured electronically and account balances updated automatically. What used to take up to 5-man days can now be automated almost entirely.

4. What is the role of DBS Bank?

   DBS provides the banking infrastructure to safely and securely route payments from payer to the beneficiary's bank account through the FAST network. SPs and MCSTs can now make and accept payments from any of the local banks and most of the foreign retail banks in Singapore.

5. What is the role of QuickPay™?

   QuickPay™ processes payment instructions from the payer, which happens when a resident uses the Qommunity Resident app or scan a QuickPay QR code to pay.

6. Any upfront fees for signing up for QuickPay™, or for terminating the service?

   There are no sign-up fees whatsoever, as we are recovering development cost from transaction fees spread out among all MCST estates and merchants which collect payments using QuickPay™.

7. Is there a free trial of QuickPay™?

   Yes, there is a free trial for estates on Qornerstone® platform to collect payments through QuickPay™. At the end of the trial period, if the MCST decides not to proceed, the QuickPay QR code can be reverted back to a static PayNow QR code.

8. After the free trial, what are the fees for using QuickPay™?

   MCSTs will be charged at the end of every month based on the actual number of payments collected through QuickPay™.

   For MCSTs operating a DBS account: $0.29 cents per transaction

   For MCSTs operating any other bank account on FAST network: $0.29 cents per transaction and a flat fee of $30 per month.

9. Seems more reasonable to let SPs/Tenants bear the fees if they choose to use QuickPay™ instead of asking the MCST to bear the cost?

   By adopting QuickPay, the MCST benefits from having a more productive managing agent and site staff. Software automation features eliminate manual data entry tasks and free up manpower from cash and cheque handling, issuing receipts and others.

   Payment records are captured and stored electronically on safe and secure Microsoft Azure cloud, with daily back-ups, which eliminates risk of loss of paper receipts. Unlike cash, electronic payments are more secure because there are traceable records.

10. When I scan the QR code, why am I making a payment to IBASE Technology P L instead of my MCST?

    QuickPay is a payment solution developed by IBASE Technology Pte Ltd, a Singapore-based technology company with 21-year track record, in collaboration with DBS Bank. Your payment goes into a special type of account maintained with DBS Bank, called the client services account where it is held briefly before being swept twice daily to the final destination bank account owned by your MCST.

11. Why must the payment go through an intermediate account?

    The intermediate account held at DBS is a special type of account regulated by the Payment Services Act for regulation of payment services. Monies deposited into this account belongs to the MCST it is intended for and cannot be accessed by IBASE for its own use.

12. How can I be sure IBASE, or whoever have access to the intermediate account, will not run away with the money?
    IBASE and our employees are unable to access the intermediate account nor operate it in any way. The only way to move money out of the account is thru automated system-generated instructions sent from our server to Bank's server.

    Monies do not stay long in the intermediate account because there are 2 sweeps to the MCST's account daily. Control reports such as monies, transactions and bank account details help us to review and identify abnormalities

13. Can IBASE employees program change the system at a code level to divert the funds?

   During code development, there is separation of duties where the programmer's code is reviewed and screened by a QA engineer for bugs and back-doors before being approved by our CTO. Any debugging or upgrade work follows the same process. No single employee can access the whole code and data level of QuickPay server and Qornerstone Platform.

14. How can we be sure someone does not change the QR code to divert funds to their own account?

   The QR code is created by the Bank's application and any attempts to tamper with it will render unreadable. The QR codes are dynamically generated by an electronic file from the Bank with pre-set expiry times.

   Unlike cash, with electronic payments there is always an audit trail. If any SP/Tenant claims to have made a payment that was not received by the MCST, we can inspect our audit logs to trace the funds and will then be liable for restitution.

   Also, QuickPay eliminates user data entry errors because users simply scan the QR code to pay and no longer need to key in payment amount, unit details or the destination account number.

15. Can IBASE employees manually divert funds to another account?

   During the onboarding process, the MCST's appointed rep will enter the bank account details directly into the database using an online form, where it is immediately encrypted. IBASE staff are not able to access this database to change the account using system code.

16. What safeguards are in place to ensure MCST's appointed rep enters the right bank account?
   The rep enters bank account details and uploads MCST's bank account statement, which is used for verification by our QA team.

17. What other measures in place to mitigate internal threats (theft by employees)?
   All code is inspected and reviewed by an independent QA team and CTO. Once the bank account is set, any attempts to change it will trigger alerts by SMS to our QA, CTO and company directors, in addition to the 2 SPs appointed as approving authorities.

18. What measures are in place to mitigate external threats?
   Encryption of data transmission between our server with bank server. The database containing account ledgers and bank accounts and the actual application program is hosted on different servers in Microsoft Azure cloud, which hides the addresses of these servers. The servers can only be accessed from pre-approved (or white-listed) IP addresses; if the same programmer on the same laptop tries to access the server from home, for example, they would not be able to. Database is encrypted such that even internal staff are not able to make sense of the data.

   Protocols in place for safeguarding login accounts and credentials with multi-level approvals required to grant access or amend access. Our customers are further protected by cyber-security Insurance taken up by IBASE.

19. What are the security measures built into QuickPay™ for prevention against fraud or unintended errors?

QuickPay™ has been designed from the ground up to mitigate against the risk of fraud, either by our own employees or 3rd parties. Measures are in place to alert IBASE directors, Internal Risk Manager, QA auditor, and IT Director should there be an attempt to tamper with source code.

The Qornerstone® platform is used by various Singapore Government agencies and Enterprise customers, which defray the cost of our security investments. We deploy our solutions for MCSTs with the same Enterprise-grade security measures in place.

Our Data Protection & Security Policy and FAQs are available at Qornerstone.com