| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| Management Control Para (v) | *Ensure that the overall product and service design, development and operations shall strictly follow the core principles of information security i.e., confidentiality, availability and integrity. Further, any of these principles shall not be neglected or violated at any stage or step of the product / service.* | 1. Is the requirement applicable on existing products and services?<br>**Response:** This requirement shall be applicable on existing as well as new products and services.<br><br>2. Are the REs required to conduct scenario based or checklist based review of Confidentiality, Integrity, and Availability (CIA)?<br>**Response:** The REs can decide themselves the methodology of the said review. |
| Management Control Para (vi) | *Implement ISMS using applicable standards of ISO27000 family on the service component.* | 1. Are the REs required to comply with all of the ISO27000 family standards?<br>**Response:** The REs are required to implement an Information Security Management System (ISMS) using the ISO27000 family standards as a guidance.<br><br>2. What shall be the scope of the ISMS implementation?<br>**Response:** The ISMS shall be implemented institution wide and include all products and services. |
| Management Control Para (vii) | *Conduct comprehensive information security reviews of new digital products and services and for any modification in their existing digital products and services including but not limited to people, complete process and technology.* | 1. What should be the baseline of comprehensive Information Security reviews?<br>**Response:** The REs shall develop baselines themselves in accordance with the best practices and their own risk assessment.<br><br>2. Is there any requirement for periodic application security reviews?<br>Response: The REs are required to conduct periodic application security reviews, including vulnerability assessments, penetration testing and source code reviews. Additionally, all identified vulnerabilities must be addressed and rectified in a timely manner. |
| Management Control Para (ix) | *Ensure that the applications, payment cards and channels used by the FIs for such services have to be PCI/DSS and PCI/SSF certified as applicable.* | 1. Are the REs required to undergo accreditation of PCI/DSS and PCI/SSF standards through authorized assessors?<br>**Response:** All REs are required to undergo external accreditation of PCI/DSS and PCI/SSF through authorized assessors. Further, revalidation of the same shall also be required on expiry. In case of unavailability of required accreditation, the requirement shall apply whenever such accreditation is available. |

| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| | | 2. What would be the scope of the PCI/DSS and PCI/SSF?<br>**Response:** The scope of the said accreditation shall include all payment card applications, systems, and related infrastructure. The REs shall not exclude any system involving payment card-related data or its handling from the scope of the said accreditation. |
| Management Control Para (xii) | *Ensure effective mutual coordination by efficient mechanism of sharing required logs and exchange of information to trace illegitimate transfers, payments and withdrawals made through suspected accounts and wherever applicable use such authentic information to resolve customer claims and / or complete legal enforcement actions.* | 1. Who will develop the information sharing mechanism for the exchange of said information?<br>**Response**: The REs shall develop an information sharing mechanism as deemed appropriate after considering all aspects including legal requirements. Until the time of availability of such mechanism, the REs shall consider bilateral and/or multilateral sharing of information in accordance with the applicable laws and regulations. |
| Operational Control Para A(i) | *FIs shall conduct NADRA biometric verification of customers (preferably digitally), with the exception for USSD channel, in the following cases:*<br>*a. At the time of digital banking channels activation/sign–up;*<br>*b. New device registration;*<br>*c. Modification of customer email address and phone numbers.*<br><br>*Alternatively, for the following types of customers/ scenario, FIs shall implement a combination of at least two controls i.e. facial recognition, in-app live original identity document verification, in-app live picture verification, and call back verification shall be implemented:* | 1. In case of in-app biometric verification under this clause, will the existing requirement defined in PSD Circular No. 09 of 2018 clause 4 of activating / re-activating online banking services of customers after biometric verification at any branch, will still be applicable?<br>**Response:** If the RE conducts in-app biometric verification for activation/reactivation of the digital channels, it is not required to conduct the biometric verification at the branch. However, other requirements mentioned in clause 4 of PSD Circular No. 09 of 2018 would remain applicable.<br><br>2. Are the specified controls applicable on all type of accounts?<br>**Response:** The specified controls will also be applicable on all accounts including BB and AMA using digital channels (excluding USSD and payment cards).<br><br>3. Will Robo Call Back or inbound call from customers be permissible as call back verification under this clause?<br>**Response:** The call back verification for the purpose of this clause is limited to manual call back performed by the REs. |

| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| | *a. Non-resident customers;*<br>*b. Customers with physical disabilities (like limbs disability, uneven texture/ erased / unclear fingerprints, etc.);*<br>*c. Customer's having temporary issue (e.g. wounded/ bandaged hands/ mehndi, etc.);*<br>*d. Foreign nationals;*<br>*e. Non-financial services.* | 4. Can the REs use these alternate controls (a combination of at least two controls i.e. facial recognition, in-app live original identity document verification, in-app live picture verification, and call back verification) instead of primary control i.e. NADRA biometric verification?<br>**Response:** The REs are required to implement the controls, as specified i.e. alternate controls should only be used in cases where NADRA biometric verification is not possible.<br><br>5. Can the biometric verification performed at the time of account opening, be used for activation of digital channels in future or for subsequent key account changes?<br>**Response:** The biometric verification performed at the time of account opening cannot be used for activation of digital channels in future or for subsequent key account changes. However, for customers on boarded digitally, biometric verification performed for account opening can be used for activation of digital channels.<br><br>6. Is the biometric verification mandatory for in-person verification or alternative/fallback method can be followed?<br>**Response:** In case where in-person biometric verification cannot be performed due to genuine reasons, the RE may use its alternate / fallback method(s) as prescribed vide Consolidated Customer Onboarding Framework issued vide BPRD Circular No. 01 of 2025.<br><br>7. Are REs required to conduct biometric verification of customers for activation of payment cards?<br>**Response:** The REs are required to follow the payment cards' activation mechanism as mentioned in Para 4.2.4 of the 'Regulations for Payment Cards Security' issued vide PSD Circular No. 05 of 2016.<br><br>8. Can the REs use video calls as an alternative for in-person verification?<br>**Response**: The REs are permitted to use video calls as an alternative for in-person verification. However, the video call must be recorded, reviewed by a relevant staff member (other than the one conducting the video call verification), and the REs must establish appropriate controls to ensure compliance, authenticity, and auditability of the process. Additionally, the video recording shall be treated as part of customer profile information and shall be kept in record with the customer's profile.<br><br>9. Is it mandatory to register the existing device(s) of the customer using the controls specified i.e. NADRA biometric verification? |

| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| | | Response: All customer devices including existing devices are required to be registered using the specified controls i.e. NADRA biometric verification, etc. Failing to do so, the REs shall bear the liability in case of any fraud/scam committed using these accounts.<br><br>10. Can the REs allow exemption from the NADRA biometric verification?<br>**Response:** The REs are not permitted to grant exemption from the NADRA biometric verification (other than specified in sub para 3(I) Other Operational Controls clause iii). |
| Operational Control Para A(iii) | *FIs shall ensure that the credential reset (such as change in user ID/password of mobile banking/internet banking channel of customers) is only performed using customers' registered device.* | 1. What if customer mobile phone or any other registered device is lost/snatched?<br>**Response:** In case of lost/snatched customer device, the customer shall follow the process of registration of new device. |
| Operational Control Para A(vii) | *FIs shall define a reasonable limit on number of accounts accessed per device, and implement additional authentication controls (i.e. CBC, obtaining and recording the justification for exceeding the limit along with customer verification) for devices exceeding the defined limit.* | 1. What is meant by reasonable limit on number of accounts accessed per device?<br>**Response:** The REs shall define the reasonable limit (e.g. no of accounts to be accessed in last 7 days, 30 days and/or 365 days) based on their own internal risk assessment, of how many accounts could be accessed using a single device. |
| Operational Control Para A(viii) | *FIs shall apply a reasonable limit on the maximum number of registered devices. FIs shall implement a 2-hours cooling-off period before activation of mobile apps for newly registered customers. Further, cooling-off period shall also be introduced before implementation of requests for key account changes such as device, customer's mobile number, email ID, transaction limits, password reset etc. Customer may be intimated* | 1. What is meant by reasonable limit on maximum number of registered devices?<br>**Response**: It means the maximum number of registered devices associated with a customer's account.<br><br>2. Are the requirements of this clause applicable on Branchless Banking wallets, Asaan accounts and other account types specified in the Consolidated Customer Onboarding Framework?<br>**Response:** Yes, the requirements of this clause are applicable on all types of accounts, which are accessible through digital channels.<br><br>3. What would be the cooling-off period for key account changes?<br>**Response:** The cooling-off period for key account changes shall be at least 2 hours. |

| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| | *beforehand in this respect through SMS, as well as through alternate channels such as email.* | 4. Is the cooling-off period on digital channel activation or key account changes applicable in cases where the in-app NADRA biometric verification is performed?<br>**Response:** The requirement for cooling-off period shall not be applicable in cases where NADRA biometric verification is performed in-app or through branches of REs. However, cooling off period will be applicable where the said biometric verification is performed through branchless banking agents.<br><br>5. Which functionalities shall be restricted during the cooling-off period?<br>**Response:** During cooling-off period, credit to the customer's account are allowed; however, customer is restricted to perform financial transactions involving debits to their accounts using mobile/internet banking.<br><br>6. Can the RE waive off, the requirement of cooling-off period on digital channel activation and key account changes?<br>**Response:** Other than the scenarios mentioned above (i.e. in-app NADRA biometric verification) for exemption from cooling-off period, the RE may waive off the requirement of cooling off period subject to assuming the liability of any fraud, which may occur during the said period. |
| Operational Controls Para B(ii) | *FIs shall set reasonable default transaction limits on the digital channels and permit the customers to enhance or reduce these limits after due authentication. Further, the customers shall also be provided with the option to manage transaction limits for all digital channels.* | 1. How will REs determine reasonable default transaction limit?<br>**Response:** The REs shall define reasonable default transaction limits based on the risk profile of their customer, and their own internal assessment.<br><br>2. Are these requirements applicable to Branchless Banking (BB) wallets?<br>**Response:** These requirements are also applicable to BB wallets keeping in view the sanctity of regulatory limits prescribed for BB accounts.<br><br>3. Are REs required to provide overall/ umbrella limit to its customers?<br>**Response:** The REs are required to provide options to set overall/ umbrella limit on each Digital Channel, i.e. Mobile Banking/Internet banking, e-commerce, USSD Banking and payment card. |
| Operational Controls Para B(iii) | *FIs shall define and enforce reasonable limits on the number of utility bill payments made to a utility company/ vendor through digital channel from a* | 1. Are the REs required to define bill payment limits on utility companies only?<br>**Response:** The limit shall be applicable on digital channels of a customer for payments to utility companies as well as vendors. |

| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| | *particular account (excluding bill payments by branchless banking agents). However, the said limit may be enhanced upon customer specific request.* | 2. How will the bill payment limits be applied in cases where the RE uses billing aggregator?<br>**Response:** In such cases, the limit as prescribed above in question 1 shall be applicable. |
| Operational Controls Para B(x) | *For branchless banking accounts, FIs, upon receipt of a successful credit, shall allow cash out, on-line purchases or mobile top-up against the transferred funds after two (02) hours. During this period, funds will remain on "in-progress" status. Customer may be intimated beforehand in this respect through SMS, as well as through alternate channels such as email. However, for their trusted customers, beneficiary FI may allow cash withdrawal, online purchases or mobile top-up.* | 1. What is the definition of the trusted customer?<br>**Response:** The REs shall define the criteria for Trusted Accounts. For such accounts, the REs shall assume the liability of any fraud committed using those accounts during the applicable cooling off period. |
| Operational Para C(ii) | *The beneficiary FIs shall temporarily hold the fraudulent proceeds received from the sender FIs where any supplementary/ secondary information in the FTDH dispute request is invalid. In all such cases where supplementary/ secondary information is invalid, the sender FIs shall rectify the supplementary information within reasonable time (not more than 30 minutes from the time FTDH dispute request is marked invalid).* | 1. What shall be the duration of temporarily holding disputed funds in case of invalid supplementary / secondary information?<br>**Response:** The beneficiary REs shall temporarily hold the fraudulent proceeds for three (3) hours. However, in such cases, during that period when returning inward clearing cheques the bank should avoid quoting 'insufficient balance' as a reason. |

| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| Operational Para C(v) | *Beneficiary FIs, upon receipt of dispute in the FTDH shall immediately (not more than 30 minutes after receiving complaint from the customer) block withdrawal of disputed funds and suspend the digital channels to prevent further use of the said account for digital frauds. Subsequently, the relevant FIs shall complete the investigation within ten days of lodgment of dispute in FTDH and after establishing the fraud, reverse the funds within three days to the account of the victim*. | 1. Are the beneficiary REs required to immediately suspend the digital channels of the beneficiary accounts (of the disputes)?<br>**Response:** The beneficiary REs are required to suspend the digital channels of the beneficiary accounts (of the disputes) for three (03) hours. During this period, the said RE shall conduct due diligence and decide to maintain or remove the suspension of the digital channel. In this regard, the REs shall make all possible efforts to minimize the inconvenience to their customers.<br><br>2. What action will the beneficiary RE take to block the withdrawal of the disputed funds?<br>**Response:** The beneficiary RE shall only mark a lien on the disputed funds. The RE shall not block the account or place a debit block on it.<br><br>3. Are sender and beneficiary REs both required to conduct investigation?<br>**Response:** Both sender and beneficiary REs are required to conduct investigations, independently, and prepare formal investigation reports within 10 days of receiving the dispute.<br><br>4. What will be the timeframe for concluding the investigation in case of multiple layering accounts involving several REs?<br>**Response:** Each sender and beneficiary RE in the layering chain is required to conduct and conclude the investigation within 10 days of receiving the dispute.<br><br>5. Is it required to report scam cases in FTDH system?<br>**Response:** Yes, the REs shall report scam cases in FTDH system. Moreover, they shall take measures to enhance consumer awareness regarding social engineering and possible scam scenarios.<br><br>6. Are the beneficiary REs required to mark lien on the disputed funds in cases where the disputed amount is routed to another account (i.e. layered)?<br>**Response:** The beneficiary REs are required to mark lien on the disputed amount irrespective of whether the funds are routed out to another account (i.e. layered). |
| Operational Para C(vi) | *In case of e-Commerce transaction, FIs shall immediately report disputed fraudulent online transactions to respective domestic merchants either* | 1. Are the REs required to conduct a full investigation for e-commerce and card-related frauds involving non-3DS (3D Secure) transactions?<br>**Response**: The REs are also required to conduct comprehensive investigations of all e-commerce and card-related frauds, including both 3DS and non-3DS frauds. In this regard, the RE shall also focus on |

| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| | *directly or through their acquiring institutions after being reported by the customers. The acquiring institution shall ensure that the information about the disputed transaction is conveyed to the merchant immediately with the request to block the shipment of physical goods. Further, the FIs shall also make all possible efforts for recovery of customers' funds.* | reviewing whether there was any unauthorized access to customer's data within its systems prior to the fraud, or any compromise of payment card related information, wherever applicable. |
| Operational Para C(vii) | *FIs shall identify the CNICs and accounts of the fraudsters or collusive beneficiaries (itself not victim(s)) established to be involved in fraudulent activity, after due investigation. The details of such fraudulent accountholders as well as of those who are used in routing fraud proceeds will be shared across the industry for enhanced monitoring.* | 1. Is there any mechanism available for sharing of the said information?<br>**Response:** The banking industry is required to collaborate and develop a mechanism for sharing of such information in line with the applicable laws and regulations. However, this requirement shall be applicable after availability of such a mechanism. Meanwhile, the REs may share the said information through bilateral / multilateral sharing arrangements in compliance with the applicable laws and regulations. |
| Monitoring Controls D(II) | *The scope of real-time fraud monitoring tools and alerts mechanism specified in the PSD Circular No. 09 of 2018 related to payment card systems shall be enhanced to include all digital products. Further, FIs shall implement fraud risk scenarios which shall be periodically reviewed, require additional authentication from the customers based on digital fraud risk score, and for taking timely actions such as suspending transactions/accounts, etc. For this purpose, FIs may use Intelligent* | 1. Are the REs required to capture and store the geolocation of the customer's device?<br>**Response:** The REs are required to capture and store the geolocation of the customer's device at least at the time of device registration, channel activation, and login. |

| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| | *Algorithm based Customer's Transaction Behavior Profiling techniques for detection of suspected transactions.* | |
| Operational Control Para E(i) | *Throughout the service chain at all stages, the customer information should be stored or transmitted in hashed or encrypted as applicable form using non-obsolete cryptographic algorithms, such as AES 256 and SHA256 or the updated versions, duly vetted by subject matter experts.* | 1. What kind of vetting is required for encryption?<br>**Response:** The REs may obtain the said vetting from its Information Security (IS) function. The scope of the vetting shall include attestation that the customer information is stored and transmitted in hashed / encrypted form using non-obsolete cryptographic algorithms as updated from time to time.<br><br>2. What would be the frequency for the required vetting from the subject matter expert?<br>**Response:** The REs shall define the frequency in accordance with their own risk assessment considering major changes in their own technological infrastructure and other internal & external developments. |
| Operational Control Para E(ii) | *FIs shall design the process and application in such a way that the chances of disclosure of customer information - in whole or partially in a manner that makes it possible to be collated to reconstruct - are eliminated or minimized.* | 1. Is the requirement of this clause be applicable on existing applications?<br>**Response**: The requirement of this clause will also be applicable on existing applications. |
| Operational Control Para E(iii) | *FIs shall strictly ensure that the information so collected shall not appear or be disclosed in whole to any individual processing officer/staff/third party and shall appear in partially anonymized/tokenized/hashed/masked form as applicable, while rendering assisted banking services or reporting and management of banking service operations – to minimize its disclosure. Any information required to be* | 1. Are the requirements of this clause applicable on core banking applications as well as at the branch side?<br>**Response:** These requirements are applicable on all applications across the organization. |

| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| | *displayed internally shall be strictly on Need-to-Know basis.* | |
| Call Center F(II) | *The requirement of BC&CPD Circular No. 03 of 2021, regarding call wait times of not more than one minute for card block request shall also apply to blocking request for all digital channels including branchless banking accounts/ wallets, mobile and internet banking channels, etc. Further, the FIs shall also provide self-service IVR based functionality for blocking digital channels through their call centers.* | 1. Are the REs required to log and monitor call wait times in their solutions/systems?<br>**Response**: The REs are required to log and monitor the customer call wait times in their systems for tracking and compliance purposes. |
| Operational Control Para H(i) | *The customers should be provided option to select the languages primarily Urdu and English in which they want to receive the notifications.* | 1. Can the REs send notification in roman Urdu?<br>**Response** The REs may send the notifications in roman Urdu, if opted by the customer. |
| Operational Controls Para H(iii) | *In addition to the existing requirements of PSD Circular Letter No. 01 of 2019 regarding sending free of cost transaction alerts on SMS and email (where email IDs are available), the FIs shall also send instant (free of cost) alerts on: sign-in from a new device not already registered, password reset, failed login attempts and request for availing lending products. FIs shall prioritize these alerts and also arrange for sufficient capacity/bandwidth for instantly sending these alerts.* | 1. Can the REs send in-app notifications instead of SMS?<br>**Response**: The REs are required to at least send SMS notifications for digital channel sign-up/activation, new device registration, credential reset, and key account changes.<br><br>2. Are REs required to send SMS for each transaction carried out using Debit/Credit cards?<br>**Response**: Yes, REs are required to send SMS for each transaction carried out using Debit / Credit cards. |

| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| Operational Control Para I(iii) | *FIs for convenience of their domestic customers travelling overseas and RDA accountholders may exempt certain digital channel controls on customers' request.* | 1. What types of control exemptions are being referred in this clause?<br>**Response:** The REs on the customer's request and as per their own internal risk assessment may grant exemption against any control, which may create operational hindrance and inconvenience to their domestic customers travelling overseas and non-resident Pakistanis. However, the RE shall take appropriate measures to authenticate legitimacy of their customers, specifically addressing the risk of identity theft and impersonation. |
| Other Operational Controls I(I) | *FIs shall conduct comprehensive investigations of the digital banking frauds and prepare formal investigation reports and engage with the customer to transparently present/explain bank's findings. The scope of the investigation shall be end to end (from victim to ultimate beneficiary) and at least include validation of customer assertions, potential of internal staff involvement, role of branchless banking agents (including those responsible for conducting biometric verification), review of PII access logs, gaps or weaknesses in FI's systems, applications and processes, etc. Further, FIs shall take action against the branchless banking agents involved in the digital frauds and staff delinquent in conducting proper KYC and CDD.* | 1. Are the REs required to conduct comprehensive investigations of e-commerce and card frauds?<br>**Response**: The REs are also required to conduct comprehensive investigation of all e-commerce and card-related frauds, including both 3DS and non-3DS frauds. The REs should also focus on reviewing access to customer data within their systems prior to the fraud or any other potential compromise of payment card information, wherever applicable. |
| Other Operational Controls I(II) | *FIs shall implement Data Loss Prevention Controls to prevent compromise of data including specially the customer data.* | 1. Are the REs required to implement a Data Loss Prevention (DLP) solution for the implementation of the data loss prevention controls?<br>**Response:** The REs are required to implement a Data Loss Prevention (DLP) solution, with implementation scope covering the entire organization. |

**Annexure B** - Frequently Asked Questions on Measures to Enhance Security of Digital Banking Products and Services (BPRD Circular No. 04 dated April 14, 2023)

| Reference to the Circular/ Appendix/ Section | Requirement of Circular/ Appendix/ Section | FAQs |
|---|---|---|
| 1 | 2 | 3 |
| Liability Framework Para (iii).d | *All beneficiary FI(s) shall share proportionate liability in case FTDH timelines are breached for marking lien on the suspected beneficiary account and funds are withdrawn.* | 1. How would proportionate liability be determined?<br>**Response:** The REs shall determine the proportionate liability on case of case basis. In case of layering transactions, the liability will be capped at the amount of the layered disputed transaction(s) |
| Liability Framework Para (iv) | *In case of a dispute in branchless banking account referred at para 3-B-vi, the liability will reside with the beneficiary bank.* | 1. Which dispute is the clause referring to?<br>**Response:** This clause is referring to dispute originated pertaining to the following clause mentioned in section 3-B-x<br>"*For branchless banking accounts, FIs, upon receipt of a successful credit, shall allow cash out, on-line purchases or mobile top-up against the transferred funds after two (02) hours. During this period, funds will remain on "in-progress" status. Customer may be intimated beforehand in this respect through SMS, as well as through alternate channels such as email. However, for their trusted customers, beneficiary FI may allow cash withdrawal, online purchases or mobile top-up*." |
| Liability Framework (III) | | 1. Will the customer be liable for the digital frauds where there is no weakness on their part e.g. sharing of credentials or confidential information, etc.?<br>**Response:** Providing safe and secure digital product and services is the responsibility of the REs. Therefore, the customer will not be liable in cases where there is no weakness on their part (e.g., customer has not shared any information/device, customer has not performed the disputed transaction, etc.). In all such cases, the customer's RE will be liable to compensate the customer. |
| | *General Queries* | 1. Is BPRD Circular No. 04 of 2023 applicable on corporate accounts?<br>**Response:** The requirements of this circular shall only be applicable on retail customers |