Customer Protection

Limiting Liability of Customers in Unauthorized Electronic Banking Transactions

Board Approved Document for Private Bank (PB) and Corporate Bank (CB)

1. Purpose

The purpose of this document is to outline the process to be followed on the Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions offered by Deutsche Bank India ("hereafter, the Bank') through its business unit, namely Private Bank (PB) and Corporate Banking (CB) as per the "*Board Approved Document". It is also a regulatory requirement as per RBI circular RBI/2017 18/15 DBR.No. Leg.BC.78/09.07.005/2017 18 dated July 6, 2017.
The document is transparent, nondiscriminatory, stipulates the mechanism of compensating the customer for the unauthorized electronic banking transactions, and prescribe the timeline for effecting such compensation.

2. Scope

The electronic banking payment transactions can be initiated by client through:

Private Bank

- Remote/ online payment transactions (transactions that do not require physical payment instruments to be presented at the point of transactions e.g. internet banking, mobile banking, card not present (CNP) transactions), and UPI.
- Face-to-face/ proximity payment transactions (transactions which require the physical payment instrument such as a card or mobile phone to be present at the point of transaction e.g. ATM, POS, etc.) third party products / services permissible under the para-banking guidelines of the Reserve Bank of India.

Corporate Bank

- Deutsche Bank Direct Internet
- Deutsche Bank Direct Connect
- Autobahn App Market.

3. Channels available for customers to report unauthorised transactions

Private Bank

Current Channels available 24*7 for registering customer complaint	
Mode	**Availability**
Phone Banking	Yes
Interactive voice response	Yes
Dedicated toll-free helpline	Yes
Reporting to home branch** (During Bank working hours.)	No
SMS	Yes
Email	Yes
Online Banking	Yes
Mobile Banking	Yes
Bank Website	Yes

Corporate Bank

Mode	**Availability**
Email	Yes

4. Systems and Procedures

To make customers feel safe about carrying out electronic banking transactions, the Bank endeavor to put in place:

i. Appropriate system and procedures to ensure safety and security of electronic banking transactions carried out by customer.
ii. Robust and dynamic fraud detection and prevention mechanism.
iii. Mechanism to assess the risks resulting from unauthorised electronic banking transaction and measure the liabilities arising out of such events.
iv. Appropriate measures to mitigate the risks and protect itself against the liabilities arising there from.
v. A system of continually and repeatedly advising customers on how to protect themselves from electronic banking payments related fraud.

5. Roles and Responsibilities of the Bank

i. The customers are advised to notify the Bank of any unauthorised electronic banking transaction at the earliest after the occurrence of such transaction. The longer the time taken by the customers to notify the Bank, the higher will be the risk of loss to the Bank/customer.
ii. On receipt of report of an unauthorised electronic banking transaction from the customer, the Bank takes immediate steps to prevent further unauthorised electronic banking transactions in the account.
iii. The Bank regularly conduct awareness on safe electronic transactions to its staff and customers. Merchants.
iv. This is available on the Banks' website. Such information includes rights and obligation of the customers as well as non-disclosure of sensitive information. Awareness communication includes aspect such as situations in which customer is entitled for compensation, how, when and to whom unauthorised electronic banking transaction is to be reported, the need for immediate reporting in view of risk of increasing loss, definition of unauthorised electronic banking transaction, the need for disclosure of sensitive information example password, PIN, OTP, date of birth, details of transactions, etc.
v. The Bank conduct detailed investigation and ensure that it can clearly identify cause of the incident and the entity responsible.
vi. The Bank share its decision based on the outcome of its investigation with the customer.
vii. This policy to be read in conjunction with the Customer Grievance Redressal Policy and Customer Compensation Policy of the Bank.
viii. In case during investigation or based on external feedback received, if it is found that the customer has falsely claimed or disputed a valid transaction, the Bank reserve its right to take due preventive action in the same.

For Private Bank:

ix. The Bank advises its customers to mandatorily register for SMS alerts and as well as e-mail alerts, for electronic banking transactions. The SMS alerts should mandatorily be sent to the customers, wherever mobile number is registered. The Bank also send e-mail alerts to the customers, wherever e-mail id is registered.
x. The Bank provides customers with 24x7 access through multiple channels [like website, customer care, SMS, IVR and reporting to any branch (during branch working hours)] for reporting unauthorised electronic transactions.
xi. The Bank also enable a direct link on the Bank's website for lodging the complaints, with specific option to report unauthorised electronic transactions. The Bank also ensure immediate response (including auto response) is sent to the customers acknowledging the complaint. The communication systems used by the Bank records the time and date of delivery of the message and receipt of customer's response.

xii. The customer will not be allowed digital transaction if found that contact details are not updated in the Bank records.

6. Obligations

Customer is bound by following obligations whenever they use or are likely to use the physical card, card information or mobile/net banking or any other electronic mode to conduct financial transactions. The obligations of the customer include but not limited to:

i. Record their complaint through any of multiple modes available like- SMS, customer care, e-mail ID, branch, and website.
ii. Mandatorily register for SMS alerts (electronic transactions)
iii. Update their registered contact details as soon as such details are changed. Bank will only reach out to customer at the last known e-mail id/mobile number. Any failure of the customer to update the Bank with changes will be considered as customer negligence.
iv. Provide all necessary documentation - customer dispute form, proof of transaction success/failure and should also file a police complaint and provide copy of the same to the Bank.
v. Co-operate with the Bank's investigating authorities and comply with the Bank's reasonable requirements towards obtaining details of transactions, investigation purposes etc.
vi. Share relevant documents as needed for investigation viz. customer dispute form, copy of passport in case of international transactions and police complaint.
vii. Authorise the Bank to block their account(s) to reduce likelihood of additional loss Not to share sensitive information [such as Card number, 3D secure PIN, ATM PIN, Unique Registration Number (URN), Debit Card PIN, Card Verification Value (CVV), Mobile login PIN, Net Banking user id and password, One Time Password (OTP), etc.] to any entity including bank staff.
viii. Protect their device as per best practices specified in the Bank's website (device includes smart phone, feature phone, laptop, desktop, and TAB).
ix. Abide by the process mentioned on the following link Safe Online Banking - Deutsche Bank – Deutsche Bank India
x. Set limits on their transaction to ensure that the exposure is minimized.
xi. Verify their transactions from time to time in the bank and or card statement and raise query with the Bank as soon as possible in case of any error Go through various instructions and awareness communication sent by the Bank or check on the Bank's website at https://www.deutschebank.co.in on a regular basis Change ATM PIN frequently, at least once a month.
xii. Memorize their PIN and not to share the PIN or card with anyone, not even their friends or family.
xiii. Not to take help from strangers for using the ATM card or handling their cash Press the 'Cancel' key before moving away from the ATM and should remember to take the card and transaction slip.
xiv. Report lost/stolen ATM card to card-issuing bank immediately.
xv. Not to save confidential information such as debit card numbers, CVV numbers or PINs on the mobile phone.

7. General approach from Deutsche Bank towards customer liability

Deutsche Bank - Client Reimbursement Chart for Fraudulent Transactions

Client Reports Fraudulent Transaction		
Category 1	**Category 2**	**Category 3 – Private Bank**
Client Negligence	**Bank Negligence**	**Where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system**
100% Client Liability	100% Bank Liability	100% Bank Liability
Zero liability on customer for transactions done post informing the Bank	Zero liability on customer for transactions done post informing the Bank.	Zero liability on customer for transactions done post informing the Bank.

* In exceptional scenarios the Bank may consider not being lenient on category 3 type of cases.

Client Negligence:

A customer will be liable for the loss occurring due to unauthorised transactions in the following cases: i. In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorised transaction to the bank.

Bank Negligence:

Unauthorized Electronic Banking Transaction happened due to Contributory fraud / negligence / deficiency on the part of the Bank (either committed by Bank staff or Bank vendor) – (irrespective of whether or not the transaction is reported by the customer)

Private Bank:
Where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system:

Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorized transaction.

**Third party breaches:

Third party breaches would cover following unauthorised transactions without customer knowledge.

1. SIM duplication – Cloning of original SIM to create duplicate SIM
2. Skimming/Cloning – Collect data from the magnetic strip of the card and copying the information onto another plastic.

8. Reversal Timeline for Zero Liability/Limited Liability of customer.

On being notified by the customer, the bank will attempt to conclude the fraud investigation within 10 working days, however in case if the fraud investigation is not concluded within 10 working days, a shadow credit (of the disputed amount) will be provided to the customer with value date.

The shadow credit will be processed by the home branch with a value date and a lien will be applied on the shadow credit amount.

No approvals will be required for such entries as this is a regulatory instruction.

Upon conclusion of the investigation the below process will be followed:

1. If established as "customer liability" then investigation team will outcall the customer and share the response which the Bank has concluded as per laid down process. Bank will reverse the shadow credit from customer's account.

2. If established as a "bank liability" Bank to procure the requisite documents from the customer to proceed for reversal. Till the time reversal is not settled lien will not be removed. Once the amount is settled branch will be instructed to remove the lien. No additional compensation will be paid in case of Bank liability as the credit to the customer will be value dated

3. If established as "where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system" Bank to procure the requisite documents from the customer to proceed for reversal. Till the time reversal is not settled lien will not be removed. Once the amount is settled branch will be instructed to remove the lien.

9. Monitoring

The Standing Council on Customer Service will review the unauthorised electronic banking transactions reported by customers on a quarterly interval along with the action taken thereon, the functioning of the grievance redressal mechanism and take appropriate measures to improve the systems and procedures. All such transactions will be reviewed by the Bank's internal auditors.

10. Deutsche Bank ensures that:

(i) On receiving the complaint from the customer, Bank will immediately act and block client`s account/card and start the investigation. For CB clients, the respective user accesses and/ or client internet banking be disabled.
(ii) Bank will consider "Date of notification" as date of 1st complaint received by the bank from the client.
(iii) Bank to investigate the complaint within 10 working days & conclude the case. If Bank investigation proves the transaction is fraudulent, Bank will reverse the transaction with shadow credit* in client`s account within 10 working days from date of notification. For CB clients the investigation will be carried out by the respective client service teams.
(iv) The shadow credit will be value dated as of date of fraudulent transaction(s).
(v) Working days are considered as per banking calendar of home branch of the customer.
(vi) After posting shadow credit, bank will ask client to submit documentary evidence (i.e., Insurance documents).
    a. Filled Insurance claim form.

b. Complaint letter to the bank infirming the fraudulent transaction/s.
c. Police complaint copy or FIR copy.
d. Complete passport copy including blank pages in case of overseas fraud.

(vii) In case the client fails to provide documentary evidence as per the Bank's requirements within 90 working days of reporting the fraud, in order to enable the Bank to determine the liability, the Bank will reverse the shadow credit from the client's account at the expiry of 90 working days from the date of receipt of client complaint and it will be deemed as a case of "Full liability of the client".

(viii) Bank will resolve any customer complaint within 90 working days of raising of complaint. If not able to resolve within the timeline, then the customer's liability will be considered as zero.

(ix) The burden of proving customer liability in case of unauthorized electronic banking transactions will lie on the bank.

(x) In case we are not able to complete the investigation within 10 working days due to some technical error or manual error or oversight at our end, Bank will consider the case as "Fraudulent" & reimburse the client as per reimbursement chart along with the applicable penalty as per Bank`s compensation policy.

(xi) Due to non-corporation from the client (i.e. no response from client for queries raised by us or client is not contactable to discuss or investigate) In case we are not able to complete the investigation within 10 working days, we will close the case as "Not fraudulent". In case the same client comes back to us post 10 working days, we will consider date of notification as date on which client has responded to our query.

* Shadow credit stands for – Posting credit entry in client`s account with lien marked on the amount posted.