



ભારતીય રીઝર્વ બેંક

www.rbi.org.in

આર.બી.આઈ. / 2017-18 / 15

DBR.No.Leg.BC.78 / 09.07.005 / 2017-18

જુલાઈ 6, 2017

તમામ અનુસૂચિત કોમર્શિયલ બેંકો (આરઆરબી સહિત)
બધી નાની નાણાક્રિય બેંકો અને પેમેન્ટ બેંકો

પ્રિય સર / મેડમ,

ગ્રાહક સુરક્ષા – અનધિકૃત ઇલેક્ટ્રોનિક બેંકિંગ વ્યવહારોમાં ગ્રાહકોની જવાબદારી મર્યાદિત કરવી

મહેરબાની કરીને કપટયુક્ત (fraudulent) અથવા અન્ય વ્યવહારોથી ઉદ્ભવતા ખોટી ડેબિટના રિવર્સલ રિવર્સલ સંબંધમાં અમારા પરિપત્ર ડીબીઓડી. લીગ.બીસી .86 / 09.07.007 / 2001-02, તા.એપ્રિલ 8, 2002 નો સંદર્ભ લો.

2. નાણાકીય સમાવેશ અને ગ્રાહક સુરક્ષા પર મુકાયેલા વધારાના ભારને કારણે અને તેમના એકાઉન્ટ્સ / / કાર્ડ્સમાં ડેબિટમાં પરિણમે એવા અનધિકૃત વ્યવહારો સંબંધિત ગ્રાહક ફરિયાદોમાં તાજેતરના થયેલ વધારાને ધ્યાનમાં લઈને, આ સંજોગોમાં ગ્રાહકની જવાબદારી નક્કી કરવા માટેના માપદંડની સમીક્ષા કરવામાં આવી છે. આ બાબતે સુધારેલા નિર્દેશો નીચે દર્શાવેલ છે.

સિસ્ટમો અને કાર્યપદ્ધતીઓ મજબૂત કરવી

3. વ્યાપકપણે, ઇલેક્ટ્રોનિક બેંકિંગ વ્યવહારોને બે કક્ષાઓમાં વિભાજિત કરી શકાય છે.

(i) રીમોટ/ઓનલાઈન પેમેન્ટ લેવડદેવડ (કે જે વ્યવહારોમાં લેવડદેવડના સમયે ભૌતિક ચુકવણી સાધનો સાધનો રજૂ કરવા જરૂરી નથી, દા.ત. ઇન્ટરનેટ બેંકિંગ, મોબાઈલ બેંકિંગ, કાર્ડ હાજર નથી (સીએનપી) વ્યવહારો, પ્રી-પેઈડ પેમેન્ટ ઇન્સ્ટ્રુમેન્ટ્સ (પીપીઆઈ), અને

બેંકિંગ રેગ્યુલેશન વિભાગ , સેન્ટ્રલ ઓફિસ, પી.ઓ.બોક્સ નં .1006, 13 મા માળ, સેન્ટ્રલ ઓફિસ બિલ્ડીંગ, શાહિદ ભગત સિંહ માર્ગ, મુંબઈ મુંબઈ 400001, ટેલી નંબર: 91-22-22601000 ફેક્સ નંબર: 91-22-2270 1240, ઇમેઈલ આઈડી: cgmicdbr@rbi.org.in

(ii) ફેસ-ટુ-ફેસ / નિકટતા ચુકવણી વ્યવહારો {proximity payment transactions (વ્યવહારો કે જેમાં ભૌતિક ચુકવણી સાધન જરૂરી છે, જેમ કે એક વ્યવહારોના સમયે કાર્ડ અથવા મોબાઇલ ફોન હાજર હોય છે. દા.ત. એટીએમ, POS, વગેરે) };

4. બેંકોમાં સિસ્ટમો અને કાર્યપદ્ધતીઓ, ઇલેક્ટ્રોનિક બેન્કિંગ વ્યવહારો હાથ ધરવા માટે ગ્રાહકોને સુરક્ષિત લાગે તેવી રીતે રચાયેલ હોવી જોઈએ. આ હાંસલ કરવા માટે, બેંકોએ દાખલ કરવી જોઈએ ;

(i) ગ્રાહકો દ્વારા હાથ ધરવામાં આવેલા ઇલેક્ટ્રોનિક બેન્કિંગ ટ્રાન્ઝેક્શન માં સલામતી અને સુરક્ષાની સુરક્ષાની ખાતરી કરવા યોગ્ય સિસ્ટમો અને કાર્યપદ્ધતીઓ;

(ii) મજબૂત અને ગતિશીલ છેતરપિંડી શોધ અને નિવારણ પદ્ધતિ (Fraud detections and prevention mechanism);

(iii) અનધિકૃત વ્યવહારોથી પરિણમતા જોખમોનું મૂલ્યાંકન કરવાની પદ્ધતિ (ઉદાહરણ તરીકે, બેંકની પ્રવર્તમાન સિસ્ટમ માં રહેલા અવરોધો) અને આવી ઘટનાઓમાંથી ઉદભવતી જવાબદારીઓનું માપ નક્કી કરવું ;

(iv) જોખમ ઘટાડવા માટે અને તેમાંથી ઊભી થતી જવાબદારીઓ સામે તેમનું રક્ષણ કરવા માટે યોગ્ય પગલાં;

(v) ઇલેક્ટ્રોનિક બેન્કિંગ અને ચુકવણી સંબંધિત છેતરપિંડીથી પોતાને કેવી રીતે સુરક્ષિત રાખી શકાય તે અંગે ગ્રાહકોને સતત અને વારંવાર સલાહ આપતી એક પદ્ધતિ.

ગ્રાહકો દ્વારા બેંકોને અનધિકૃત વ્યવહારોની જાણ કરવી

5. ઇલેક્ટ્રોનિક બેન્કિંગ વ્યવહારો માટે બેંકોએ તેમના ગ્રાહકોને એસએમએસ ચેતવણીઓ (sms alerts) માટે અને ઉપલબ્ધ હોય ત્યાં ઈ-મેઇલ ચેતવણીઓ માટે ફરજિયાતપણે રજીસ્ટર કરાવવા કહેવું કહેવું જોઈએ. એસએમએસ ચેતવણીઓ ગ્રાહકોને ફરજિયાત રીતે મોકલવામાં આવશે, જ્યારે રજીસ્ટર રજીસ્ટર થયેલ ગ્રાહક હોય ત્યાં ઈમેઇલ ચેતવણીઓ મોકલી શકાય છે. કોઈ પણ અનધિકૃત ઇલેક્ટ્રોનિક ઇલેક્ટ્રોનિક બેન્કિંગ વ્યવહાર અંગે તેમની બેંકને આવા વ્યવહારની ઘટના પછી સૌથી પહેલાં સૂચિત કરવા કરવા ગ્રાહકોને સલાહ આપવી જોઈએ અને જણાવવું જોઈએ કે બેંકને સૂચિત કરવામાં સમય જેટલો લાંબો હશે તેટલું બેંક / ગ્રાહકને ઊંચા નુકસાનનું જોખમ રહેશે. આને સરળ બનાવવા બેંકોએ ગ્રાહકોને ગ્રાહકોને થઈ ગયેલા અનધિકૃત વ્યવહારોની જાણ કરવા માટે અને / અથવા કાર્ડ જેવા ચુકવણી સાધનની સાધનની ચોરી, ખોવાઈ જવું વગેરે રીપોર્ટ કરવા માટે બહુવિધ ચેનલો (ઓછામાં ઓછું, વેબસાઇટ, ફોન

ફોન બેન્કિંગ, એસએમએસ, ઈ-મેલ, આઈવીઆર, એક સમર્પિત ટોલ-ફ્રી હેલ્પલાઈન, હોમ શાખાને અહેવાલ આપવો વગેરે) દ્વારા 24x7 એક્સેસ સાથે પ્રદાન કરવી આવશ્યક છે બેંકો ગ્રાહકોને એસએમએસ અને ઈ-મેલ ચેતવણીઓને "Reply " દ્વારા તરત જવાબ આપવા સશક્ત કરશે અને ગ્રાહકોને વાંધો, જો કોઈ હોય તો, સૂચવવા માટે કોઈ વેબ પેજ અથવા ઈ-મેલ સરનામાની શોધ કરવાની કરવાની જરૂર ન પડવી જોઈએ. વધુમાં, બેન્કો દ્વારા તેમની વેબસાઈટના હોમ પેજ પર અનધિકૃત ઈલેક્ટ્રોનિક ટ્રાન્ઝેક્શનની જાણ કરવા માટે ચોક્કસ વિકલ્પ સાથે, ફરિયાદો દાખલ કરવા માટેની સીધી કડી સીધી કડી પૂરી પાડવામાં આવશે. નુકસાન / છેતરપિંડીની રિપોર્ટિંગ સિસ્ટમ તેની પણ ખાતરી કરશે કે રજિસ્ટર્ડ ફરિયાદ નંબર સાથે ફરિયાદ સ્વીકારીને ગ્રાહકોને તાત્કાલિક પ્રતિસાદ (ઓટો પ્રતિસાદ સહિત) સહિત) મોકલવામાં આવે. બેંકો દ્વારા ચેતવણીઓ મોકલવા અને તેમના પ્રતિસાદો પ્રાપ્ત કરવા માટે ઉપયોગમાં લેવાતી સંદેશાવ્યવહાર પ્રણાલીઓએ સંદેશ પહોંચાડયાનો સમય અને તારીખ અને ગ્રાહકનો ગ્રાહકનો પ્રતિસાદ, જો કોઈ હોય તો, રેકોર્ડ કરવા જોઈએ. આ બધું ગ્રાહકની જવાબદારીની મર્યાદા મર્યાદા નક્કી કરવામાં મહત્વનું રહેશે. બેંકમાં જે ગ્રાહકો મોબાઈલ નંબર આપતા નથી તેમને એટીએમ થી થી રોકડ ઉપાડ સિવાયની ઈલેક્ટ્રોનિક સુવિધા બેન્કો,ઓફર નહીં કરી શકે. ગ્રાહક પાસેથી અનધિકૃત વ્યવહારનો રિપોર્ટ પ્રાપ્ત થયા પછી ખાતામાં વધુ અનધિકૃત વ્યવહારો રોકવા માટે બેન્કોએ તાત્કાલિક તાત્કાલિક પગલા લેવા જોઈએ.

ગ્રાહકની મર્યાદિત જવાબદારી

(એ) ગ્રાહકની શૂન્ય જવાબદારી

6. નીચેના બનાવોમાં જ્યાં અનધિકૃત વ્યવહાર થાય ત્યાં 'શૂન્ય જવાબદારીનો ગ્રાહકનો અધિકાર' ઊભો ઊભો થશે :

(I) બેન્ક તરફથી હિસ્સેદારી વાળો ફોડ / બેદરકારી / ઉણપ, (ભલે ગ્રાહક દ્વારા તે ટ્રાન્ઝેક્શન અંગે અહેવાલ આપવામાં આવે કે નહીં).

(II) ત્રીજા પક્ષ દ્વારા ઉલ્લંઘન, જ્યાં ઉણપ બેન્કો અથવા ગ્રાહક તરફથી નથી પરંતુ સિસ્ટમમાં અન્ય અન્ય જગ્યાએ છે અને અનધિકૃત વ્યવહાર બાબતે બેંક પાસેથી સંચાર પ્રાપ્ત થવાના ત્રણ કાર્યકારી દિવસની અંદર ગ્રાહક બેન્કને સૂચવે છે

(બી) ગ્રાહકની મર્યાદિત જવાબદારી

7. નીચેના કિસ્સાઓ નાં વ્યવહારો માં અનધિકૃત વ્યવહારના કારણે થતા નુકશાન માટે ગ્રાહક જવાબદાર જવાબદાર રહેશે.

(i) એવા કિસ્સાઓમાં કે જ્યાં ગ્રાહક દ્વારા બેદરકારી ને કારણે નુકશાન થાય છે, જેમ કે જ્યાં તેણે પેમેન્ટ ક્રેડેન્શીયલ્સ (payment credentials) શેર કર્યા છે, જ્યાં સુધી તે બેંકને અનધિકૃત વ્યવહારનું વ્યવહારનું રીપોર્ટિંગ ન કરે ત્યાં સુધી સંપૂર્ણ નુકસાન ગ્રાહક સહન કરશે. અનધિકૃત વ્યવહારનાં રિપોર્ટિંગ રિપોર્ટિંગ પછી થતુ કોઈપણ નુકસાન બેંક સહન કરશે.

(ii) એવા કિસ્સાઓમાં, જ્યાં અનધિકૃત ઇલેક્ટ્રોનિક બેન્કિંગ વ્યવહારો માટેની જવાબદારી બેંક ઉપર કે કે ગ્રાહક ઉપર નથી, પરંતુ સિસ્ટમમાં અન્ય જગ્યાએ રહેલ છે અને જ્યારે આવા વ્યવહારોને બેંકને સૂચિત કરવામાં ગ્રાહકના પક્ષે વિલંબ થાય છે (બેંક પાસેથી સંચાર પ્રાપ્ત કર્યા પછી ચાર થી સાત કામકાજના દિવસો) ત્યાં ગ્રાહકની પ્રતિ ટ્રાન્ઝેક્શન જવાબદારી, ટ્રાન્ઝેક્શન વેલ્યુ સુધી અથવા કોષ્ટક કોષ્ટક (Table -1) માં ઉલ્લેખિત રકમ, બેમાંથી જે ઓછી હશે, ત્યાં સુધી મર્યાદિત રહેશે.

ટેબલ 1

ફકરા 7(ii) હેઠળ ગ્રાહકની મહત્તમ જવાબદારી (₹)

એકાઉન્ટનો પ્રકાર	મહત્તમ જવાબદારી (₹)
• BSBD એકાઉન્ટ્સ	₹5,000
• અન્ય તમામ એસબી એકાઉન્ટ્સ • પ્રિ-પેઇડ પેમેન્ટ ઇન્સ્ટ્રુમેન્ટ્સ અને ગીફ્ટ કાર્ડ્સ • MSME નાં કરન્ટ / કેશ ક્રેડિટ / ઓવરડ્રાફ્ટ એકાઉન્ટ્સ • (છેતરપિંડીની ઘટનાની અગાઉના 365 દિવસ દરમિયાન) કરન્ટ એકાઉન્ટ્સ / કેશ ક્રેડિટ / ઓવરડ્રાફ્ટ એકાઉન્ટોમા વાર્ષિક સરેરાશ બેલેન્સ/ ₹25 લાખ સુધીની લિમિટ લિમિટ ધરાવતી વ્યક્તિઓ • ₹5 લાખ સુધીની મર્યાદા ધરાવતા ક્રેડિટ કાર્ડ	₹10,000

<ul style="list-style-type: none"> • અન્ય તમામ કરન્ટ / કેશ ક્રેડિટ / ઓવરડ્રાફ્ટ એકાઉન્ટ્સ • ₹5 લાખથી વધુની મર્યાદા ધરાવતા ક્રેડિટ કાર્ડ્સ 	₹25,000
---	---------

વધુમાં, જો રિપોર્ટિંગ કરવામાં સાત કામકાજના દિવસોની ઉપર વિલંબ થાય તો, ગ્રાહકની જવાબદારી બેંકનાં બોર્ડની મંજૂર કરેલી નીતિ મુજબ નક્કી કરવામાં આવશે. ખાતાઓ ખોલાવતી વખતે બેંકો આ નિર્દેશોને અનુસરતાં ગ્રાહકોની જવાબદારી બાબતે તેમની નીતિની વિગતો આપશે. વિશાળ પ્રસારણ માટે માટે જાહેર ડોમેઇનમાં બેંકો તેમની મંજૂર કરેલી નીતિ પ્રદર્શિત કરશે. વર્તમાન ગ્રાહકોને વ્યક્તિગત રીતે વ્યક્તિગત રીતે બેંકની નીતિ વિશે જાણ કરવી જોઈએ.

8. તૃતીય પક્ષના ઉલ્લંઘન વખતે જ્યાં ઉણપ બેંકોની કે ગ્રાહકની નથી પરંતુ સિસ્ટમમાં ક્યાંક અન્યત્ર છે અન્યત્ર છે ત્યાં, ગ્રાહકની એકંદર જવાબદારી ઉપર વિગતવાર ફકરા 6(ii) અને ફકરા 7(ii) મુજબ, ટેબલ ટેબલ 2 માં સારાંશ કરેલ છે:

ટેબલ 2

ગ્રાહકની જવાબદારીનો સારાંશ

સંચાર પ્રાપ્ત થયા પછીની તારીખથી 'છેતરપિંડી વ્યવહાર'ની જાણ કરવા માટે લીધેલો સમય	ગ્રાહકની જવાબદારી (₹)
કામકાજના 3 દિવસની અંદર	શૂન્ય જવાબદારી
કામકાજના 4 થી 7 દિવસની અંદર	વ્યવહાર મૂલ્ય અથવા કોષ્ટક 1 માં ઉલ્લેખિત રકમ, બેમાંથી જે ઓછું હોય તે
કામકાજના 7 દિવસથી ઉપર	બેંકના બોર્ડની મંજૂર કરેલ નીતિ અનુસાર

કોષ્ટક 2 માં ઉલ્લેખ કરેલ કામકાજના દિવસોની સંખ્યા, સંચાર પ્રાપ્ત કરવાની તારીખ બાદ કરીને, ગ્રાહકની હોમ શાખાના કાર્ય શેડ્યૂલ મુજબ ગણવામાં આવશે.

ગ્રાહકની શૂન્ય જવાબદારી / મર્યાદિત જવાબદારી માટે રિવર્સલ ટાઈમલાઈન

9. ગ્રાહક દ્વારા સૂચિત થવા પર, આવી સૂચનાની તારીખથી કામકાજના 10 દિવસની અંદર બેંક ગ્રાહકના ખાતામાં અનધિકૃત ઇલેક્ટ્રોનિક ટ્રાન્ઝેક્શનમાં સામેલ રકમ (વીમા દાવાના પતાવટની રાહ જોયા વગર, જો કોઈ હોય તો), જમા (shadow reversal) કરશે. કોઈ અનધિકૃત ઇલેક્ટ્રોનિક બેંકિંગ બેંકિંગ વ્યવહાર કિસ્સામાં ગ્રાહકની બેદરકારીના કિસ્સામાં પણ, બેંકો તેમની મુનસુફી અનુસાર, કોઈ

ગ્રાહકની જવાબદારી જતી કરવાનો નિર્ણય લઈ શકે છે. અનધિકૃત વ્યવહારની તારીખ પ્રમાણે એ મુજબ મુજબ ક્રેડિટ હશે.

10. વધુમાં, બેન્કો તેની ખાતરી કરશે કે:

(i) ફરિયાદ ઉકેલાય અને ગ્રાહકની જવાબદારી, જો કોઈ હોય તો, એટલા સમયની અંદર સ્થાપિત થાય જે બેંકના બોર્ડમાં મંજૂર કરેલ નીતિ માં નિર્દિષ્ટ થયા મુજબ હોય પરંતુ ફરિયાદની પ્રાપ્તિની તારીખથી તારીખથી 90 દિવસથી વધુ નહીં, અને ગ્રાહકને ને ઉપરોક્ત ફકરા 6 થી 9 ની જોગવાઈઓ મુજબ વળતર ચૂકવવામાં આવે ;

(ii) 90 દિવસની અંદર, જ્યાં તે ફરિયાદનો ઉકેલ લાવવા અથવા ગ્રાહકની જવાબદારી, જો કોઈ હોય તો, નિર્ધારિત કરવા અસમર્થ હોય, ગ્રાહકને ઉપરોક્ત 6 થી 9 ફકરાઓમાં સૂચવ્યા અનુસાર વળતર ચૂકવવામાં આવે ; અને

(iii) ડેબિટ કાર્ડ / બેંક ખાતાના કિસ્સામાં, ગ્રાહકને વ્યાજ નું કોઈ નુકશાન થતું નથી અને ક્રેડિટ કાર્ડના કાર્ડના કિસ્સામાં, ગ્રાહક વ્યાજનો કોઈ વધારાનો બોજો સહન કરતા નથી.

ગ્રાહક સુરક્ષા માટે બોર્ડ દ્વારા મંજૂર થયેલ નીતિ

11. ગ્રાહકની બેદરકારી / બેંકની બેદરકારી / બેન્કિંગ સિસ્ટમના ફોડ / તૃતીય પક્ષ ઉલ્લંઘનને લીધે ગ્રાહકના ખાતાઓમાંથી અનધિકૃત ઉપાડથી થતા જોખમોને ધ્યાનમાં લેતા, ખાસ પરિસ્થિતિઓમાં અનધિકૃત વ્યવહારોના કિસ્સામાં બેન્કોએ ગ્રાહકોના અધિકારો અને જવાબદારીઓ સ્પષ્ટપણે વ્યાખ્યાયિત કરવાની જરૂર છે. અનધિકૃત ઇલેક્ટ્રોનિક બેન્કિંગના આવા કિસ્સાઓમાં ઇલેક્ટ્રોનિક બેન્કિંગમાં સંકળાયેલા જોખમો અને જવાબદારીઓ પર ગ્રાહકોની જાગૃક્તા ઉભી કરવાની પદ્ધતિ સહિત, ગ્રાહક સુરક્ષાનાં પાસાંઓ આવરી લેવા બેંકો તેમના બોર્ડની મંજૂરી સાથે, તેમની ગ્રાહક સંબંધ સંબંધ નીતિની રચના / સુધારણા કરશે. આ નીતિ પારદર્શક, બિન-ભેદભાવયુક્ત હોવી જોઈએ અને અનધિકૃત ઇલેક્ટ્રોનિક બેન્કિંગ વ્યવહારો માટે ગ્રાહકોને વળતર ને આપવાની પદ્ધતિ નિયત કરતી હોવી હોવી જોઈએ અને ઉપરોક્ત પેરા 10 માં સમાયેલ સૂચનોને ધ્યાનમાં રાખીને આવા વળતરને આપવા માટેની સમયરેખાઓ પણ નિર્દિષ્ટ કરતી હોવી જોઈએ. આ નીતિ બેંકની વેબસાઈટ પર ફરિયાદ હેન્ડલિંગ હેન્ડલિંગ / એસ્કેલેશન (escalation) પ્રક્રિયાની વિગતો સાથે દર્શાવવામાં આવશે. આ પરિપત્રમાં રહેલી સૂચનાઓ નીતિમાં સામેલ કરવામાં આવશે.

સાબિતીનો બોજો (burden of proof)

12. અનધિકૃત ઇલેક્ટ્રોનિક બેન્કિંગ લેવડદેવડ નાં કિસ્સામાં ગ્રાહક ની જવાબદારી પુરવાર કરવાનો ભાર ભાર બેંક પર રહેશે.

રીપોર્ટિંગ અને મોનિટરિંગ જરૂરીયાતો

13. બોર્ડ અથવા તેની એક સમિતિમાં બેન્કો દ્વારા ગ્રાહક જવાબદારી કેસોનાં અહેવાલ (reporting) (reporting) માટે એક યોગ્ય પદ્ધતિ અને માળખું અમલમાં લાવવામાં આવશે. આ રિપોર્ટિંગ, અન્ય બાબતો સાથે, વોલ્યુમ / કેસોની સંખ્યા અને તેમાં વિવિધ વર્ગોના જેમ કે કાર્ડ પ્રેઝન્ટ વ્યવહારો, કાર્ડ નોટ કાર્ડ નોટ પ્રેઝન્ટ વ્યવહારો, ઈન્ટરનેટ બેન્કિંગ, મોબાઇલ બેન્કિંગ, એટીએમ વ્યવહારો, વગેરે અને કેટેગરીઓમાં વહેંચણી, તથા કુલ મૂલ્યનો સમાવેશ કરશે. દરેક બેન્કમાં ગ્રાહક સેવાની સ્ટેન્ડીંગ કમિટી રહેશે જે ગ્રાહકો દ્વારા રીપોર્ટ થયેલ અથવા અન્યથા, અનધિકૃત ઇલેક્ટ્રોનિક બેન્કિંગ ટ્રાન્ઝેક્શન્સની ટ્રાન્ઝેક્શન્સની સમયાંતરે સમીક્ષા કરશે, તેમજ તેના પર થયેલી કાર્યવાહી, ફરિયાદ નિવારણ પદ્ધતિની પદ્ધતિની કામગીરી અને સિસ્ટમો અને કાર્યપદ્ધતિઓ સુધારવા માટે યોગ્ય પગલાં લેવા. આવા તમામ તમામ વ્યવહારોની બેંકનાં આંતરિક ઓડિટર્સ દ્વારા સમીક્ષા કરવામાં આવશે.

14. આ પરિપત્રમાં રહેલી સૂચનાઓ, ક્રેડિટ કાર્ડ, ડેબિટ કાર્ડ અને રૂપી ડેનોમિનેટેડ કો-બ્રાન્ડેડ પ્રિ-પેઇડ પ્રિ-પેઇડ બેન્કોના કાર્ડ ઓપરેશન્સ તથા ક્રેડિટ કાર્ડ જારી કરતી એનબીએફસી કે જેની પરિશિષ્ટ માં માં વિગતો છે તે અંગેના અમારા જુલાઈ, 1, 2015 ના માસ્ટર સર્ક્યુલર ડીબીઆર નં.એફ.એફ.ડી.બીસી.18 / 24.01.009 / 2015-16 માં સમાયેલ કેટલીક સૂચનાઓને સ્વભાવ કરે છે.

આપનો વિશ્વાસુ,

(પ્રકાશ બલિઆરસિંગ)

ચીફ જનરલ મેનેજર

પરિશિષ્ટ

અમારા માસ્ટર સર્ક્યુલરમાં બેન્ક્સનાં ક્રેડિટ કાર્ડ, ડેબિટ કાર્ડ અને રૂપિયામાં અંકિત સહ-બ્રાન્ડેડ પ્રિ-પેઈડ પ્રિ-પેઈડ કાર્ડ ઓપરેશન્સ (Rupee denominated co-branded pre-paid card operations) અને ક્રેડિટ કાર્ડ જારી કરતી એનબીએફસી (ડીબીઆર નં.એફ.એફ.ડી.બીસી.18 / 24.01.009 / 2015-16, dated જુલાઈ 1, 2015) અંગેની સૂચનાઓ જે અનુસૂચિત કોમર્શિયલ કોમર્શિયલ બેન્કોના સંદર્ભમાં સુધારેલ છે.

ક્રમ	હાલની સૂચનાઓ		આ પરિપત્ર પરિપત્ર માં સુધારેલા સૂચનો (પેરા નં.)
	પેરા નં.	સૂચનાઓ	
1	I.14.1	બેંકો / એનબીએફસીઓ એ ફોડ સામે લડવા અને અગમચેતી (Proactive) ફોડ નિયંત્રણ અને અમલનાં પગલાં લેવા માટે કાયદાઓ ઘડે તે સમિતિઓ / ટાસ્ક ફોર્સ માં સક્રિયપણે ભાગ લેવા માટે આંતરિક નિયંત્રણ પ્રણાલીની સ્થાપના કરવી.	4
2	II.7. (viii) (c)	7. ગ્રાહકોને કાર્ડ્સ ઈશ્યૂ કરવા માટેના નિયમો અને શરતો viii) (સી) શરતો અનુસાર, નીચે મુજબ અવગત થયા પછી તરત જ બેંકને સૂચિત કરવાની જવાબદારી કાર્ડહોલ્ડર પર મૂકવામાં આવશે ; - કાર્ડ નું નુકશાન અથવા ચોરી અથવા કાર્ડની નકલ અથવા એવા સાધનો જે તેનો ઉપયોગ કરવા માટે સક્ષમ કરે છે ; - કાર્ડહોલ્ડરના એકાઉન્ટના રેકોર્ડિંગ પર કોઈપણ અનધિકૃત વ્યવહાર ; અને અને - બેંક દ્વારા તે ખાતાને મેઈન ટેઈન કરવામાં કોઈપણ ભૂલ અથવા અન્ય અનિયમિતતા ;	5

3	II.7. (viii)(ડી)	(viii) (ડી): શરતોમાં સંપર્ક બિંદુને ઉલ્લેખિત કરશે જેને સૂચિત કરી શકાય શકાય છે, આવું સૂચન દિવસના કોઈપણ સમયે અથવા રાતે કરી શકાય છે.	5
4	II.7. (X)	શરતો જાણાવશે કે, બેંકના સીધા નિયંત્રણની અંદર, સિસ્ટમ ખામીને કારણે કાર્ડધારકને થયેલ સીધા નુકસાન માટે બેંક જવાબદાર હશે. જો કે, ઉપકરણ અથવા અન્યથા, જાણીતા ડિસ્પ્લે પર સંદેશ દ્વારા કાર્ડહોલ્ડર માટે સિસ્ટમ સિસ્ટમ માટેનું આ ભંગાણ જાણી શકાય તેવું હોય તો ચુકવણી સિસ્ટમનાં તકનિકી ભંગાણ ને લીધે થયેલ કોઈપણ નુકસાન માટે બેંક જવાબદાર નહીં ગણાય. શરતોને સંચાલિત કરતા ટ્રાન્ઝેક્શનના બિન અમલ અથવા ખામીયુક્ત અમલ માટે બેંક ની જવાબદારી મુખ્ય રકમ અને વ્યાજના નુકસાન પુરતી મર્યાદિત રહેશે.	6 & 7
5	II.9. (I)	બેંક ડેબિટ કાર્ડની સંપૂર્ણ સુરક્ષાને સુનિશ્ચિત કરશે. ડેબિટ કાર્ડની સુરક્ષા તે સુરક્ષા તે બેંકની જવાબદારી રહેશે અને સુરક્ષા તંત્રની નિષ્ફળતા અને સુરક્ષા ભંગને લીધે કોઈ પક્ષને થતું નુકસાન બેંક ભોગવશે.	4, 6 અને 7
6	II.9. (iv)	iv) ચોરી અથવા કાર્ડની નકલ થવાને લીધે, કોઈપણ નુકસાન અંગે બેંકને સૂચના અપાય એ સમય સુધી કાર્ડધારકને નુકસાન સહન કરવું પડશે, પરંતુ માત્ર એક ચોક્કસ મર્યાદા સુધી, (કાર્ડધારક અને બેંક વચ્ચે અગાઉથી સંમત સંમત થયા મુજબ નિયત રકમ અથવા ટ્રાન્ઝેક્શનની ટકાવારી), સિવાય કે જ્યાં કાર્ડધારકે કપટપૂર્વક, જાણી જોઈને અથવા અત્યંત બેદરકારી પૂર્વક પૂર્વક કામ કર્યું હોય.	6 અને 7
7	II.9. (v)	પ્રત્યેક બેંક એવો ઉપાય પૂરો પાડશે જેથી તેના ગ્રાહકો દિવસ અથવા રાત્રિના કોઈ પણ સમયે પેમેન્ટ ઉપકરણોનાં નુકસાન, ચોરી અથવા તેમની નકલની સૂચના આપી શકે.	5
8	II.9. (vi)	નુકસાન, ચોરી અથવા કાર્ડની નકલ અંગેની સૂચનાની પ્રાપ્તિ પર, કાર્ડનો કાર્ડનો કોઈ વધુ ઉપયોગ કરે તે રોકવા માટે બેંક તેની પાસેના ઉપલબ્ધ તમામ પગલાં લેશે.	5