



TranServ Limited

(CIN: U93090MH2010PLC211328)

ગ્રાહક સુરક્ષા નીતિ

અનધિકૃત ટ્રાન્ઝેક્શનમાં ગ્રાહકોની જવાબદારી મર્યાદા

પૃષ્ઠભૂમિ

પ્રીપેડ પેમેન્ટ ઇન્સ્ટ્રુમેન્ટ્સ (PPIS) નો ઉપયોગ કરીને વ્યવહારોમાં વધારો એ સંકળાયેલા જોખમો માં ગુણોત્તર વધારો કરે છે અને તેથી અનધિકૃત ઇલેક્ટ્રોનિક ચુકવણી વ્યવહારો સામે ગ્રાહક સુરક્ષાને વધુ મહત્વ આપવામાં આવ્યું છે. રિઝર્વ બેંક ઓફ ઈન્ડિયા (RBI) એ અનધિકૃત ઇલેક્ટ્રોનિક પેમેન્ટ ટ્રાન્ઝેક્શનમાં ગ્રાહકોની જવાબદારી નક્કી કરવા માટેની જોગવાઈઓ નિર્ધારિત કરી છે જેના પરિણામે તેમના વોલેટ/કાર્ડમાં ડેબિટ થાય છે.

ઉદ્દેશ્ય

RBI એ PPI જારી કરનારાઓને ગ્રાહક સુરક્ષાના પાસાઓને આવરી લેતી નીતિ ઘડવાની જરૂરીયાત જણાવેલ છે, જેમાં જોખમો અને જવાબદારીઓ અને અનધિકૃત ઇલેક્ટ્રોનિક વ્યવહારોના ચોક્કસ સંજોગોમાં તેમના વોલેટ/કાર્ડમાંથી ડેબિટ થવાના પરિણામે ગ્રાહકની જવાબદારી અંગે ગ્રાહક જાગૃતિ પેદા કરવાની પદ્ધતિનો સમાવેશ થાય છે.

આ પોલિસીનો ઉદ્દેશ્ય TranServ દ્વારા જારી કરાયેલા Dhani Pay PPISનો ઉપયોગ કરીને કરવામાં આવેલ કોઈપણ અનધિકૃત વ્યવહારોના કિસ્સામાં ગ્રાહકોને સુરક્ષિત રાખવા માટે એક વ્યાપક માર્ગદર્શિકા પ્રદાન કરવાનો છે.

વ્યવહારોની શ્રેણીઓ

Dhani Pay PPI નો ઉપયોગ કરીને ઇલેક્ટ્રોનિક ચુકવણી વ્યવહારોને બે શ્રેણીઓમાં વિભાજિત કરવામાં આવે છે:

- I. રિમોટ/ઓનલાઈન પેમેન્ટ વ્યવહારો (વ્યવહારો કે જેમાં વ્યવહારના દૃષ્ટિએ ભૌતિક PPIS રજૂ કરવાની જરૂર હોતી નથી જેમાં વોલેટ્સ, કાર્ડ ની હાજરી જરૂરી નથી (CNP) વ્યવહારો, વગેરે.
- II. રૂબરૂ/પ્રોક્સિમિટી પેમેન્ટ ટ્રાન્ઝેક્શન્સ (વ્યવહારો કે જેમાં કાર્ડ્સ અથવા મોબાઇલ ફોન જેવા ભૌતિક PPIS જેવા કે વ્યવહારના સ્થળે હાજર રહેવું જરૂરી છે. દા.ત. ATM પરના વ્યવહારો, પોઈન્ટ ઓફ સેલ, મોબાઇલ એપ દ્વારા કરવામાં આવેલા વ્યવહારો વગેરે.)

TranServ ની ભૂમિકાઓ અને જવાબદારીઓ

- i. TranServ એ સુનિશ્ચિત કરશે કે ગ્રાહક સુરક્ષા નીતિ વેબસાઇટ પર તેમજ ગ્રાહકોના મોબાઇલ એપ સંદર્ભ પર ઉપલબ્ધ થાય .
- ii. TranServ ગ્રાહકોને સંવેદનશીલ માહિતીઓ ની જાહેરાત ન કરવા માટે ઇમેલ મોકલીને સુરક્ષિત ઇલેક્ટ્રોનિક વ્યવહારો કરવા અંગે જાગૃતિ આચરશે જેમ કે પાસવર્ડ , PIN, OTP, જન્મ તારીખ, વગેરે.
- iii. TranServ ઉલ્લેખિત તમામ ચુકવણીના વ્યવહારો માટે SMS ચેતવણીઓ અને ઇમેઇલ ચેતવણીઓની ખાતરી કરશે તેમજ અનધિકૃત વ્યવહારોની જાણ કરવા અથવા વાંધાઓની જાણ કરવા માટે સંપર્ક ની વિગતો આપશે.
- iv. TranServ ગ્રાહકોને કોઈપણ અનધિકૃત ટ્રાન્ઝેક્શનને વહેલામાં વહેલી તકે સૂચિત કરવા સલાહ આપશે, જેથી TranServ ને જાણ કરવામાં વિલંબ થવાને કારણે નુકસાનના જોખમને ટાળી શકાય.
- v. TranServ ગ્રાહકોને કોઈપણ અનધિકૃત વ્યવહારો અને/અથવા PPI ના ખોવાઈ જવા અથવા ચોરીની જાણ કરવા માટે વેબસાઇટ/sms/e-mail દ્વારા 24x7 ઍક્સેસ કરવા માટેની સુવિધા આપશે. આવા કોઈપણ વ્યવહાર ની જાણ કરવા માટે TranServ મોબાઇલ એપ/હોમ પેજ પર એક વિકલ્પ પણ પ્રદાન કરશે.
- vi. TranServ નોંધાયેલ ફરિયાદ ની સ્વીકૃતિ તરીકે તાત્કાલિક પ્રતિસાદની ખાતરી કરશે. સિસ્ટમ ફરિયાદની પ્રાપ્તિની તારીખ અને સમય રેકોર્ડ કરશે.
- vii. TranServ એ પણ સુનિશ્ચિત કરશે કે ગ્રાહક દ્વારા અનધિકૃત ટ્રાન્ઝેક્શનની ફરિયાદ નોંધાવ્યા બાદ જ્યાં સુધી ફરિયાદ નું નિરાકરણ ન થાય ત્યાં સુધી કોઈ વ્યવહાર કરવામાં ન આવે.
- viii. 10 દિવસની અંદર TranServ ગ્રાહકની લાગુ જવાબદારી મુજબ એક નેશનલ ક્રેડિટ પાસ કરશે. TranServ 90 દિવસની અંદર ફરિયાદનું નિરાકરણ કરશે અને ગ્રાહકને ચુકવવા પાત્ર રકમ ચૂકવશે.
- ix. 90 દિવસની અંદર ગ્રાહકની જવાબદારી નક્કી કરવાનો ઠરાવ ન થાય તો ગ્રાહક વળતર માટે પાત્ર બનશે.
- x. તપાસ દરમિયાન, જો એવું જણાયું કે ગ્રાહકે ખોટી રીતે દાવો કર્યો છે અથવા માન્ય વ્યવહાર પર વિવાદ કર્યો છે, તો TranServ નેશનલ ક્રેડિટ ને રદ કરવાનો અને વોલેટ/કાર્ડને બ્લોક કરવા સહિત નિવારક પગલાં લેવાનો અધિકાર અનામત રાખે છે.

ગ્રાહકની જવાબદારીઓ

- ગ્રાહકોએ તમામ જરૂરી દસ્તાવેજો જેવા- ગ્રાહક વિવાદ ફોર્મ, ટ્રાન્ઝેક્શનની સફળતા/નિષ્ફળતા નો પુરાવો પ્રદાન કરવી જોઈએ અને પોલીસ ફરિયાદ પણ કરવી જોઈએ અને તેની એક નકલ TranServ ને આપવી જોઈએ.
- ગ્રાહકોએ TranServ તપાસ ટીમને સહકાર આપવો જોઈએ અને તમામ સહાય પૂરી પાડવી જોઈએ.
- ગ્રાહકોએ TranServ સ્ટાફ સહિત કોઈપણ એન્ટિટી સાથે સંવેદનશીલ માહિતી (જેમ કે કાર્ડની વિગતો અને PIN, CVV, વપરાશકર્તા આઈડી અને પાસવર્ડ, OTP, ટ્રાન્ઝેક્શન પિન, પડકાર પ્રશ્નો) શેર કરવી જોઈએ નહીં.
- ન્યૂનતમ એક્સપોઝર સુનિશ્ચિત કરવા માટે ગ્રાહકોએ ટ્રાન્ઝેક્શન મર્યાદા સેટ કરવી આવશ્યક છે.
- ગ્રાહકે ઉપકરણ પર નવીનતમ એન્ટિવાયરસ સોફ્ટવેર અપડેટ સહિત શ્રેષ્ઠ પ્રથા અનુસાર તેમના ઉપકરણોને સુરક્ષિત કરવું આવશ્યક છે (ઉપકરણ માં સ્માર્ટફોન, ફીચર ફોન, લેપટોપ, ડેસ્કટોપ અને ટેબલેટ સમાવેશ થાય છે) ગ્રાહકે એકાઉન્ટ સ્ટેટમેન્ટ માંથી સમયાંતરે વ્યવહાર ની વિગત ચકાસવી જોઈએ અને TranServ સાથે કોઈપણ અસંગતતા ના કિસ્સામાં શક્ય તેટલી વહેલી તકે ક્વેરી અથવા ફરિયાદ કરવી જોઈએ.
- ગ્રાહકો TranServ દ્વારા મોકલવામાં આવેલ વિવિધ સૂચનાઓ અને જાગૃતિ સંદેશાવ્યવહાર મેળવશે.

ગ્રાહકની જવાબદારી

a) ગ્રાહકની શૂન્ય જવાબદારી

નીચેની ઘટનાઓમાં જ્યાં અનધિકૃત વ્યવહાર થાય છે ત્યાં ગ્રાહકની શૂન્ય જવાબદારીનો અધિકાર ઊભો થશે:

TranServ તરફથી ફાળો આપનાર છેતરપિંડી/બેદરકારી/ઉણપ (ગ્રાહક દ્વારા ટ્રાન્ઝેક્શનની જાણ કરવામાં આવી હોય કે નહીં તેને ધ્યાનમાં લીધા વગર)..

તૃતીય પક્ષ નો ભંગ કે જ્યાં ખામી ન તો TranServ પાસે છે કે ન તો ગ્રાહકની પરંતુ સિસ્ટમમાં અન્યત્ર છે, અને ગ્રાહક વ્યવહાર સંચારની પ્રાપ્તિના ત્રણ (3) દિવસની¹ અંદર TranServ ને સૂચિત કરે છે.

અનધિકૃત વ્યવહારોની જાણ કર્યા પછી થતી કોઈપણ ખોટ.

b) ગ્રાહકની મર્યાદિત જવાબદારી

અનધિકૃત ટ્રાન્ઝેક્શન ને કારણે થતા નુકસાન માટે ગ્રાહક ની જવાબદારી જ્યાં ખામી ન તો TranServ પાસે છે કે ન તો ગ્રાહકની પરંતુ સિસ્ટમમાં અન્યત્ર છે (તૃતીય પક્ષ ભંગ), અને ગ્રાહક ત્રણ (3) દિવસ પછી અને સાત (7) ની અંદર TranServ ને સૂચિત કરે છે.) ટ્રાન્ઝેક્શન કમ્યુનિકેશનની પ્રાપ્તિના દિવસો ટ્રાન્ઝેક્શન મૂલ્ય અથવા રૂ. 10,000 પ્રતિ ટ્રાન્ઝેક્શન, બેમાંથી જે ઓછું હોય તેટલા હશે.

¹ ઉલ્લેખિત દિવસોની સંખ્યા ટ્રાન્ઝેક્શન માટે સંદેશા વ્યવહાર પ્રાપ્ત કરવાની તારીખ ને બાદ કરતાં ગણવામાં આવશે- ગ્રાહક સુરક્ષા નીતિ

ગ્રાહકની સંપૂર્ણ જવાબદારી

ગ્રાહક એવા કિસ્સાઓમાં સંપૂર્ણ નુકસાન સહન કરશે જ્યાં:

નુકસાન ગ્રાહકની બેદરકારીને કારણે છે, દા.ત. જ્યાં ગ્રાહકે ચુકવણી ઓળખપત્ર અથવા એકાઉન્ટ/ટ્રાન્ઝેક્શન વિગતો શેર કરી હોય, જેમ કે. યુઝર આઈડી અને પિન, ક્રેડિટ કાર્ડ પિન/ઓટીપી અથવા મોબાઈલ/લેપટોપ/ડેસ્કટોપ જેવા ગ્રાહક ઉપકરણો પર અયોગ્ય સુરક્ષાના કારણે માલવેર/ટ્રોજન અથવા ફિશિંગ/વિશિંગ એટેક તરફ દોરી જાય છે. આ છેતરપિંડી કરનાર દ્વારા સિમ નિષ્ક્રિય કરવાને કારણે પણ હોઈ શકે છે

ઉણપ ન તો TranServ પાસે છે કે ન તો ગ્રાહકની પરંતુ સિસ્ટમમાં અન્યત્ર છે અને ગ્રાહક વ્યવહાર સંચારની પ્રાપ્તિના સાત (7) દિવસ પછી TranServ ને સૂચિત કરે છે. કંપની, તેના વિવેકબુદ્ધિથી, ગ્રાહકની બેદરકારીના કિસ્સામાં પણ અનધિકૃત ઈલેક્ટ્રોનિક ચુકવણી વ્યવહારોના કિસ્સામાં ગ્રાહકની કોઈપણ જવાબદારી અને માફ કરવાનો નિર્ણય લઈ શકે છે.

ગ્રાહક જવાબદારીનો પુરાવો

RBI દ્વારા નિયમન મુજબ, TranServ પાસે તમામ કાર્ડ વ્યવહારો માટે બીજા પરિબળ પ્રમાણીકરણની પ્રક્રિયા છે. બે પરિબળ પ્રમાણીકરણની પુષ્ટિ કરવા માટેના તમામ લોગ / પુરાવા / અહેવાલ ઉપલબ્ધ છે તે સાબિત કરવાની જવાબદારી TranServ પાસે છે. કોઈપણ અનધિકૃત ટ્રાન્ઝેક્શન કે જે ફક્ત ગ્રાહકને જ જાણતા બીજા પરિબળ પ્રમાણીકરણ પછી પ્રક્રિયા કરવામાં આવી હોય તે વ્યવહાર પ્રભાવિત કરવામાં ગ્રાહકની સંડોવણી/સંમતિ ના પૂરતા પુરાવા તરીકે ગણવામાં આવશે.

રિપોર્ટિંગ અને મોનીટરીંગ

TranServ બોર્ડ અથવા તેની સમિતિ ને ગ્રાહક જવાબદારીના કેસોની જાણ કરવા માટે એક પદ્ધતિ સ્થાપિત કરશે. રિપોર્ટિંગ માં અન્ય બાબતોની સાથે, કેસની સંખ્યા/સંખ્યા અને સામેલ એકંદર મૂલ્ય અને કેસની વિવિધ શ્રેણીઓ માં વિતરણ નો સમાવેશ થશે..

વધુમાં, આવા વ્યવહારોની સમીક્ષા ને સક્ષમ કરવા અને લીધેલા પગલાંની અસરકારકતાની તપાસ કરવા માટે TranServ એક મિકેનિઝમ સ્થાપિત કરશે. કંપની ઓછામાં ઓછા છેલ્લા 6 મહિના માટે એકાઉન્ટ સ્ટેટમેન્ટ જનરેટ/પ્રાપ્ત કરવાનો વિકલ્પ આપશે. એકાઉન્ટ સ્ટેટમેન્ટ, ઓછામાં ઓછું, વ્યવહારની તારીખ, ડેબિટ/ક્રેડિટ ની રકમ, નેટ બેલેન્સ અને વ્યવહારનું વર્ણન જેવી વિગતો પ્રદાન કરશે. વધુમાં, કંપની ઓછામાં ઓછા 10 વ્યવહારો માટે ટ્રાન્ઝેક્શન ઇતિહાસ પ્રદાન કરશે.

નીતિની સમીક્ષા

સમીક્ષા બોર્ડ દ્વારા વાર્ષિક ધોરણે અથવા જ્યારે જરૂર પડે ત્યારે નીતિની સમીક્ષા કરવામાં આવશે, જેમાં વ્યવસાય અથવા નિયમનકારી વાતાવરણના ફેરફાર ના કિસ્સાઓનો સમાવેશ થાય છે.