# ભારતીય રિઝર્વ બેંક

www.rbi.org.in

આરબીઆઇ/2015-16/229 05 નવેમ્બર 2015

ડીસીબીઆર.બીપીડી.(પીસીબી/આરસીબી) પરિપત્ર સં.6/19.51.026/2015-16

મુખ્ય કાર્યપાલક અધિકારી
સર્વે પ્રાથમિક (શહેરી) સહકારી બેંકો
રાજ્ય તેમજ કેન્દ્રીય સહકારી બેંકો

મહોદયા / પ્રિય મહોદય,

## સહકારી બેંકોના ગ્રાહકો માટે ઈન્ટરનેટ બેંકિંગ સુવિધા

'શહેરી સહકારી બેંકોના ગ્રાહકો માટે ઈન્ટરનેટ બેંકિંગ સુવિધા' ઉપરનો અમારો તારીખ 26 સપ્ટેમ્બર 2015 નો પરિપત્ર સં. યુબીડી.બીપીડી.(એસસીબી).પરિપત્ર સં.1/09.18.300/2011-12 જૂઓ, જેના અંતર્ગત અમુક માપદંડોની પૂર્તિ કરતી અનુસૂચિત શહેરી સહકારી બેંકો (Urban Co-operative Banks - UCBs) ને, રિઝર્વ બેંકની પૂર્વ અનુમતિથી, તેમના ગ્રાહકોને લેણ-દેણ કરી શકવાની જોગવાઈ સાથેની ઇન્ટરનેટ બેંકિંગ સુવિધા પૂરી પાડવાની પરવાનગી આપવામાં આવી હતી અને અમુક શરતોની પૂર્તતા કરતી બધી જ શહેરી સહકારી બેંકોને 'માત્ર દર્શન' ની સગવડ સાથેની ઈન્ટરનેટ બેંકિંગ સુવિધા, ભારતીય રિઝર્વ બેંકની પૂર્વ મંજૂરી વગર, પૂરી પાડવાની પરવાનગી આપતો 'શહેરી સહકારી બેંકોના ગ્રાહકો માટે ઈન્ટરનેટ બેંકિંગ (માત્ર દર્શન)' ઉપરનો તારીખ 13 ઓક્ટોબર, 2014 નો પરિપત્ર સં. યુબીડી.બીપીડી.(પીસીબી).પરિપત્ર સં.21/09.18.300/2014-15 પણ જૂઓ.

2. રાજ્ય સહકારી બેંકો (State Co-operative Banks – StCBs) અને જીલ્લા મધ્યસ્થ સહકારી બેંકો (District Central Co-operative Banks – DCCBs) ને હજી સુધી તેમના ગ્રાહકોને ઈન્ટરનેટ બેંકિંગ સુવિધા પૂરી પાડવા માટેની પરવાનગી આપવામાં આવી નથી. કેટલીક રાજ્ય અને જીલ્લા મધ્યસ્થ સહકારી બેંકોએ (StCBs/DCCBs) ઈન્ટરનેટ બેંકિંગ સુવિધા પૂરી પાડવા માટેની પરવાનગી આપવા માટે વિનંતિ કરતાં, રાજ્ય અને જીલ્લા મધ્યસ્થ સહકારી બેંકો (StCBs/DCCBs) ને પણ તેમના ગ્રાહકોને ઈન્ટરનેટ બેંકિંગ સુવિધા પૂરી પાડવા માટે

પરવાનગી આપવાનો નિર્ણય લેવામાં આવ્યો છે. આ કારણે, શહેરી સહકારી બેંકોને જારી કરવામાં આવેલી માર્ગદર્શિકાઓની સમીક્ષા કરવામાં આવી છે અને આથી શહેરી સહકારી બેંકોને જારી કરવામાં આવેલી અગાઉની માર્ગદર્શિકાઓને દૂર કરીને તેના સ્થાને બધી જ સહકારી બેંકો માટે આ બાબતમાં સમાન માર્ગદર્શિકાઓ હવે જારી કરવામાં આવે છે. બધી જ સહકારી બેંકોને લાગુ પડતી પરિશોધિત માર્ગદર્શિકાઓ નીચે પ્રમાણે છે.

**(I) ઈન્ટરનેટ બેંકિંગ (માત્ર દર્શન) સુવિધા**

3. બધી જ લાઇસંસ ધારણ કરતી રાજ્ય અને જીલ્લા મધ્યસ્થ સહકારી બેંકો (StCBs/DCCBs) અને શહેરી સહકારી બેંકો, જેઓએ કોર બેંકિંગ સમાધાનનો અમલ કર્યો છે, જેઓએ ઈન્ટરનેટ પ્રોટોકલ વર્ઝન 6 (IPv6) અપનાવ્યું છે અને જેઓએ આ પરિપત્રના અનુબંધ-I માં દર્શાવેલી માર્ગદર્શિકાઓની પૂર્તિ કરી છે, તે સર્વે સહકારી બેંકો ભારતીય રિઝર્વ બેંકની પૂર્વ અનુમતિ વગર તેઓના ગ્રાહકોને ઈન્ટરનેટ બેંકિંગ (માત્ર દર્શન) સુવિધા પૂરી પાડી શકશે. જો 'માત્ર દર્શન' સુવિધા અંતર્ગત એવી કોઈ સેવા આપવામાં આવતી હોય જેમાં બે-વખતના પ્રમાણીકરણ (two-factor authentication) અથવા એક વખતના પાસવર્ડ (One Time Password – OTP)ની જરૂર પડતી હોય તો એવા કિસ્સામાં બેંકોને, આવી સેવાઓને યોગ્ય અને અનુરૂપ હોય તેવા, આ પરિપત્રના અનુબંધ-II માં દર્શાવેલા સુરક્ષા અંગેના સૂચનોને અપનાવવા.

4. તેમના ગ્રાહકોને ઈન્ટરનેટ બેંકિંગ (માત્ર દર્શન) સુવિધા પૂરી પાડતી હોય તેવી સહકારી બેંકોએ એ બાબતની ખાત્રી કરવાની રહેશે કે આ સુવિધા થકી ચૂસ્તપણે ફક્ત લેણ-દેણ સિવાયની સેવાઓ જેવી કે ખાતાની બાકી અંગેની પૂછપરછ, ખાતાની બાકિ જોવી, ખાતાનું પત્રક ડાઉનલોડ કરવું, ચેકબૂક માટેની વિનંતિ મૂકવી વિ. જ પૂરી પાડવામાં આવે અને કોઈ પણ પ્રકારના ઓન-લાઈન નિધિ હસ્તાંતર સંબંધિત લેણ-દેણના વ્યવહારો કરવા દેવામાં ન આવે.

5. સહકારી બેંકોએ ઈન્ટરને બેંકિંગ (માત્ર દર્શન) સુવિધા શરૂ કર્યાના એક મહિનામાં ભારતીય રિઝર્વ બેંકની પ્રાદેશિક કાર્યાલયને (StCBs/DCCBs ના કિસ્સામાં NABARDને

પણ)આ બાબત અંગેનો અહેવાલ આપવાનો રહેશે.

**(II) લેણ-દેણની સગવડ સાથેની ઈન્ટરનેટ બેંકિંગ સુવિધા**

6. જેઓએ કોર બેંકિંગ સમાધાનનો અમલ કર્યો છે, ઈન્ટરનેટ બેંકિંગ પ્રોટોકલ વર્ઝન 6 (IPv6) ને અપનાવેલ છે અને નીચ જણાવેલ માપદંડોની પૂર્તિ કરેલ છે તેવી બધી જ લાઇસંસ-ધારક રાજ્ય સહકારી બેંકો, જીલ્લા મધ્યસ્થ સહકારી બેંકો અને શહેરી સહકારી બેંકો (StCBs, DCCBs and UCBs) તેમના ગ્રાહકોને, ભારતીય રિઝર્વ બેંકની પૂર્વ અનુમતિ લીધા બાદ, લેણ-દેણની સગવડ સાથેની ઈન્ટરનેટ બેંકિંગ સુવિધા પૂરી પાડી શકશે.

a) 10 ટકાથી ઓછું નહીં એટલું સીઆરએઆર (CRAR)

b) તરતના અગાઉના નાણાકીય વર્ષની તારીખ 31મી માર્ચે રૂા. ૫૦/- કરોડ અથવા તેથી વધુ શુદ્ધ મૂલ્ય (Net Worth)

c) સકલ અસર્જક મિલકતો (Gross Non Performing Assets - NPAs) 7% થી ઓછી હોવી જોઈએ અને ચોખ્ખી અસર્જક મિલકતો (Net NPA) 3% થી વધુ ન હોવી જોઈએ.

d) બેંકને તરતના અગાઉના નાણાકીય વર્ષમાં ચોખ્ખો નફો (Net Profit) થયેલો હોવો જોઈએ અને એકંદરે અગાઉના ચાર નાણાકીય વર્ષમાંથી કુલ ત્રણ નાણાકીય વર્ષમાં ચોખ્ખો નફો થયેલો હોવો જોઈએ.

e) તરતના અગાઉના નાણાકીય વર્ષમાં બેંકે નગદ્ નિધિ અનુપાત અને વૈધાનિક ચલનિધિ અનુપાત (CRR/SLR)ની જાળવણીમાં કોઈ ચૂક કરેલી ન હોવી જોઈએ.

f) બોર્ડની અંદર ઓછામાં ઓછા બે નિર્દેશક વ્યવસાયિક યોગ્યતાવાળા હોવા જોઈએ અને તેની સાથે બેંકની અંદર સંગીન આંતરિક અંકુશ પદ્ધતિ અમલમાં હોવી જોઈએ

g) બેંકનો ઇતિહાસ વિનિયમનકારી પૂર્તિ (regulatory compliance) સહિતનો હોવો જોઈએ અને જે વર્ષમાં અરજી કરવામાં આવે તેના અગાઉના બે નાણાકીય વર્ષમાં બેંક ઉપર ભારતીય રિઝર્વ બેંકના નિર્દેશો/માર્ગદર્શિકાઓના ભંગ માટે કોઈ નાણાકીય દંડ લાદવામાં ન આવેલો હોવો જોઈએ.

7. ઉપર જણાવેલા માપદંડો ને પરિપૂર્ણ કરતી રાજ્ય સહકારી બેંકો, જીલ્લા મધ્યસ્થ સહકારી બેંકો તેમજ શહેરી સહકારી બેંકો (StCBs, DCCBs and UCBs), જો તેઓ આ પરિપત્ર સાથેના અનુબંધ I અને II માં દર્શાવેલ માર્ગદર્શિકાઓનું અનુપાલન કરતી હોય તો, તેમને લેણ-દેણની સગવડ સાથેની ઈન્ટરનેટ બેંકિંગ સુવિધા પૂરી પાડવા દેવામાં આવશે. તેથી આ માટે વાંચ્છુક એવી રાજ્ય સહકારી બેંકો, જીલ્લા મધ્યસ્થ સહકારી બેંકો તેમજ શહેરી સહકારી બેંકો (StCBs, DCCBs and UCBs), સંબંધિત ભારતીય રિઝર્વ બેંકની પ્રાદેશિક કચેરીને (StCBs/DCCBs ના કિસ્સામાં NABARD દ્વારા), નીચેના દસ્તાવેજો સાથે અરજી કરશે.

(i) બોર્ડ દ્વારા સંમત કરાયેલ ઈન્ટરેનેટ બેંકિંગ પરની નીતિની નકલ જેની સાથે રિઝર્વ બેંકની માર્ગદર્શિકાઓમાં સૂચવવામાં આવેલી આઈટી તેમજ આઈએસ આવશ્યકતાઓનું પાલન કરવામાં આવ્યું છે તે બાબતને પ્રમાણિત કરતું સ્વતંત્ર ઓડિટરનું (CISA યોગ્યતા ધરાવનાર) એક પ્રમાણપત્ર.

(ii) આપવામાં આવેલી સેવાઓ/ઉત્પાદોમાં કોઈ નોંધપાત્ર ફેરફાર હોય તો તે વિષે ભારતીય રિઝર્વ બેંકને જાણ કરવાની બાંહેધરી

(iii) જોખમોનો પ્રબંધ કરવા માટે બેંક દ્વારા અપનાવવામાં આવનાર કારોબાર આયોજન (business plan), ખર્ચ અને લાભનું વિશ્લેષણ (cost and benefit analysis), પરિચલનાત્મક વ્યવસ્થાઓ(operational arrangemets) જેવી કે અપનાવવામાં આવેલ ટેકનોલોજી, કારોબારના ભાગીદાર (business partners), ત્રાહિત પક્ષકાર સેવા પ્રદાતા (third party service providers) તેમજ પ્રણાલી અને અંકુશ ક્રિયાવિધિ (System and Control procedures).

8. બેંક સુરક્ષા પ્રણાલી અને ક્રિયાવિધિમાં થતા દરેક ભંગ તેમજ નિષ્ફળતા અંગેનો અહેવાલ સંબંધિત ભારતીય રિઝર્વ બેંકને સુપ્રત કરશે (StCBs/DCCBs ના કિસ્સામાં NABARDને પણ) અને આરબીઆઈ, તેની મુનસફી મુજબ, આવી બેંકનું ખાસ ઓડીટ/નિરીક્ષણ કરાવશે.

9. પોતાના ગ્રાહકોને પહેલેથી જ ઈન્ટરનેટ બેંકિંગ (માત્ર દર્શન) સુવિધા પૂરી પાડતી StCBs/DCCBs એ તેમની તે સુવિધાની આ માર્ગદર્શિકાઓના સંદર્ભમાં તુરંત સમીક્ષા કરવાની રહેશે અને તેઓ દ્વારા પૂરી પાડવામાં આવતી સેવાઓ તેમજ કેટલી હદ સુધી તેઓ દ્વારા આ માર્ગદર્શિકાઓનું પાલન કરવામાં આવે છે તે અંગેનો અહેવાલ આ પરિપત્ર જારી થયાના એક મહિનાની અંદર ભારતીય રિઝર્વ બેંકની સંબંધિત પ્રાદેશિક કચેરીને સુપ્રત કરવાનો રહેશે. જ્યાં માર્ગદર્શિકાઓથી વિચલન (deviation) થતું હોય તેવા કિસ્સાઓમાં ચોક્કસ સમયમર્યાદામાં પરિપાલન દર્શાવતી કાર્ય યોજના (action plan) સાથેનો અહેવાલ આપવાનો રહેશે.

10. પોતાના ગ્રાહકોને પહેલેથી જ લેણ-દેણની સગવડ સાથેની ઈન્ટરનેટ બેંકિંગ સુવિધા પૂરી પાડતી રાજ્ય સહકારી બેંકો તેમજ જીલ્લા મધ્યસ્થ સહકારી બેંકોને (StCBs/DCCBs) આ પરિપત્રમાં આપવામાં આવેલી સૂચનાઓનું પરિપાલન કરવા માટે તેમજ તેમના બિઝનેસ મોડેલ, ખર્ચ/લાભના આલેખન (projections of cost/benefits) ની વિગતો સુપ્રત કરવા માટે અને આ પરિપત્ર જારી થયાના એક મહિનાની અંદર સંબંધિત ભારતીય રિઝર્વ બેંકની પ્રાદેશિક કચેરીની કાર્યોત્તર અનુમતિ મેળવી લેવા માટે સૂચિત કરવામાં આવે છે. આવી અરજીઓ સૌ પ્રથમ નાબાર્ડને સુપ્રત કરવાની રહેશે અને નાબાર્ડ થકી ભારતીય રિઝર્વ બેંકના પ્રાદેશિક કાર્યાલયને પહોંચાડવાની રહેશે.

ભવદીયા,

(સુમા વર્મા)

પ્રધાન મુખ્ય મહાપ્રબંધક

અનુલગ્નક: ઉપર મુજબ

**અનુબંધ-I**

## સહકારી બેંકોના ગ્રાહકો માટે ઈન્ટરનેટ બેંકિંગની સુવિધા પૂરી પાડવા માટેની માર્ગદર્શિકાઓ

પોતાના ગ્રાહકોને ઈન્ટરનેટ બેંકિંગ સુવિધા પૂરી પાડવા માટે ઇરાદો ધરાવતી લાઇસંસધારક રાજ્ય સહકારી બેંકો, જીલ્લા મધ્યસ્થ સહકારી બેંકો તેમજ શહેરી સહકારી બેંકો (StCBs/DCCBs/UCBs) એ નીચેની શરતોનું પાલન કરવાનું રહેશે.

(i) બેંકે બોર્ડની સંમતિ સાથેની ઈન્ટરનેટ બેંકિંગ અંગેની નીતિ ઘડવી પડશે.

(ii) ઉપરોક્ત નીતિ બેંકની માહિતી પ્રોદ્યોગિકી અને માહિતી સુરક્ષા નીતિ (Information Technology and Information Security Policy)ની સાથે સુસંગત હોવી જોઈએ તેમજ બેંકના દફતર તેમજ સુરક્ષા પ્રણાલીની વિશ્વસનીયતાને સુનિશ્ચિત કરતી હોવી જોઈએ.

(iii) આ નીતિમાં 'આપના ગ્રાહકને ઓળખો' (KYC) બાબતની આવશ્યકતાઓ માટે અનુસરવાની ક્રિયાવિધિ સ્પષ્ટપણે દર્શાવેલી હોવી જોઈએ.

(iv) નીતિમાં પ્રૌદ્યોગિકી તેમજ સુરક્ષા અંગેના માપદંડોનો પણ સમાવેશ થવો જોઈએ અને અનુબંધમાં દર્શાવ્યા મુજબ કાયદાકીય, વિનિયમનકારી તેમજ સુપરવાઈઝરી મુદ્દાઓનું સંબોધન પણ થવું જોઈએ.

(v) બેંકોએ સંગીન આંતરિક અંકુશ પ્રણાલી અમલમાં મૂકવાની રહેશે અને સેવા પૂરી પાડવામાં સમાયેલા પરિચાલનત્મક જોખમો (operational risks) ને ધ્યાનમાં લેવા પડશે.

(vi) ગ્રાહકોને સુવિધા પૂરી પાડતા પહેલા બેંકોએ જોખમો, જવાબદારીઓ અને ઉત્તરદાયિત્વ અંગેની યોગ્ય સ્પષ્ટતા કરવાની રહેશે.

તદનુસાર, બેંકોને અમલ માટે નીચેની માર્ગદર્શિકાઓ જારી કરવામાં આવે છે.

I. **પ્રૌદ્યોગિકી અને સુરક્ષા માટેના માપદંડો:**

a. સહકારી બેંકોની, નિર્દેશકો ના બોર્ડ દ્વારા મંજૂર કરાયેલી, યોગ્ય માહિતી સુરક્ષા નીતિ (Information Security Policy) હોવી જોઈએ. માહિતી પ્રૌદ્યોગિકી વિભાગ (Information Technology Division) તેમજ માહિતી સુરક્ષા વિભાગ (Information Security Division) દ્વારા બજાવવાની ફરજો વચ્ચે સ્પષ્ટ તફાવત હોવો જોઈએ. માહિતી પ્રૌદ્યોગિકી વિભાગ વાસ્તવમાં કોમ્પ્યુટર પ્રણાલીઓ (Computer Systems) ને અમલમાં મૂકશે. એક માહિતી સુરક્ષા અધિકારી (Information Security Officer) અલગથી રાખવો પડશે જે ફક્ત માહિતી સુરક્ષાનું જ કાર્ય સંભાળશે. વધુમાં એક માહિતી સુરક્ષા ઓડિટર (Information System Auditor) માહિતી પ્રણાલીઓનું ઓડિટ કરવાનું કાર્ય સંભાળશે.

b. બેંકોએ એક નેટવર્ક અને ડેટાબેઝ પ્રશાસક (Network and Database Administrator) ને પદનામિત કરવાનો રહેશે અને તેની ભૂમિકા બોર્ડ દ્વારા સંમત માહિતી પ્રણાલી નીતિ (Information System Policy) અનુસાર નક્કી કરવાની રહેશે.

c. માહિતી સંગ્રહ (data), પ્રણાલીઓ (systems), એપ્લીકેશન સોફ્ટવેર (application software), યુટિલિટીસ (utilities), દૂરસંદેશા લાઈનો (telecommunication lines), લાયબ્રેરીઓ (libraries) તેમજ સિસ્ટમ સોફ્ટવેર (system software) વિ. માં પ્રવેશ (access) કરતાં વચ્ચે તર્કપૂર્ણ અંકુશો (logical access controls) મૂકેલા હોવા જોઈએ.

d. બેંકોએ એ બાબતની ખાતરી કરવાની રહેશે કે ઈન્ટરનેટ અને બેંકની પ્રણાલી વચ્ચે કોઈ સીધો સંબંધ ન હોવો જોઈએ.

e. બેંકોએ તેઓની પ્રણાલીઓ/નેટવર્કમાં કોઈપણ પ્રકારની ઘુસણખોરીને રોકવા માટે અસરકારક અગમચેતીરૂપ સુરક્ષાની જોગવાઈઓ કરવી પડશે.

f. એપ્લીકેશન સર્વર (Application Server) માંથી બધી જ બીનજરૂરી સેવાઓ જેવીકે

ફાઇલ ટ્રાન્સફર પ્રોટોકોલ (File Transfer Protocol - FTO), ટેલનેટ (Telnet) વિ. બંધ કરવાની રહેશે. એપ્લીકેશન સર્વરને ઈ-મેઇલ સર્વરથી અલગ કરવાનું રહેશે.

g. આવેલા સંદેશાઓ સહિત બધા જ કોમ્પ્યુટર સંપર્કો(accesses)ની નોંધ થવી જોઈએ. શંકાસ્પદ હોય કે ખરેખર થયેલા હોય તેવા બધા જ સુરક્ષા ભંગના બનાવોની નોંધ રાખવી જોઈએ અને અનુવર્તી કાર્યવાહી કરવી જોઈએ. પ્રણાલીઓ (systems) તેમજ નેટવર્ક ઉપર થતા હુમલાઓ તેમજ ઘુસણખોરી ઉપર ચોકી રાખવા માટેના યોગ્ય સાધનો બેંકે વસાવવા જોઈએ અને બેંકે સુરક્ષા ભંગના બનાવોને અટકાવવા આ સાધનોનો નિયમિત ઉપયોગ કરવો જોઈએ. બેંકોએ તેમના સુરક્ષા માળખા તેમજ સુરક્ષા નીતિની નિયમિત સમીક્ષા કરવી જોઈએ અને પોતાના અનુભવો તેમજ બદલાતી પ્રોદ્યોગિકી (technologies)ને ધ્યાનમાં રાખીને સુરક્ષા માળખા તેમજ સુરક્ષા નીતિને વધુને વધુ શ્રેષ્ઠ બનાવતા રહેવી જોઈએ.

h. માહિતી સુરક્ષા અધિકારીએ અને માહિતી પ્રણાલી ઓડીટરે ચોક્કસ સમયાંતરે પ્રણાલીઓના પ્રવેશ પરીક્ષણો (penetration tests) કરવા જોઈએ જેમાં નીચેનાનો સમાવેશ થવો જોઈએ.

   1. પાસવર્ડ-ભેદનના સાધનોનો ઉપયોગ કરીને પાસવર્ડ્સ મેળવવાના કરવામાં આવતા પ્રયાસો.

   2. પ્રોગ્રામમાં બેક-ડોર ટ્રેપ્સની શોધ ચલાવવી.

   3. ડિસ્ટ્રીબ્યુટેડ ડીનાયલ ઓફ સરવીસ (Distributed Denial of Service – DDoS) તેમજ ડીનાયલ ઓફ સરવીસ (Denial of Service – DoS) હુમલાઓનો ઉપયોગ કરીને પ્રણાલીને ઓવરલોડ કરવામાં આવેલા પ્રયાસો.

   4. સોફ્ટવેરમાં, ખાસ કરીને બ્રાઉઝર અને ઈ-મેઇલ સોફ્ટવેરમાં, જો કોઈ સામાન્ય રીતે જાણમાં હોય તેવા છીદ્રો હોય તો તેની તપાસ કરવી.

   5. બહારના નિષ્ણાતો (બહુધા 'Ethical Hackers'ના નામથી જાણીતા) ની સેવા લઈને પણ પ્રવેશ પરીક્ષણ (penetration testing) કરાવી શકાય.

i. ભૌતિક સંપર્ક અંકુશો (physical access controls) ચૂસ્તપણે અમલમાં મૂકવા જોઈએ. બધી જ માહિતી પ્રણાલીઓ અને જ્યાં તેને રાખવામાં આવેલ છે તેવા બધા જ સ્થાનોને આંતરિક તેમજ બાહ્ય ભયથી રક્ષણ કરવા માટે ભૌતિક સુરક્ષાથી આવરી લેવા જોઈએ.

j. ડેટાનો બેક-અપ લેવા માટે બેંકો પાસે યોગ્ય આધાર સામગ્રી (infrastructure) અને સમયપત્રકો હોવા જોઈએ. બેંકની સુરક્ષા નીતિમાં દર્શાવ્યા મુજબની સમય મર્યાદામાં, કોઈપણ નોંધના નુકશાન વગર, ડેટા પૂરેપૂરો પુન: પ્રાપ્ત થઈ જાય તે બાબતની ખાતરી કરવા બેક-અપ લીધેલ ડેટાનું ચોક્કસ સમયાંતરે પરીક્ષણ કરતા રહેવું જોઈએ. કોરોબારનું સાતત્ય (business continuity) જળવાઈ રહે તે માટે હોનારત પુનરુત્થાન સ્થાનો (Disaster Recovery Sites) ઊભા કરવા જોઈએ અને આ સ્થાનોનું પરીક્ષણ પણ સમયાંતરે કરતાં રહેવું જોઈએ.

k. કાયદેસર હેતુઓ માટે બધા જ એપ્લીકેશન્સની નોંધ રાખવાની સુવિધા (record keeping facilities) હોવી જોઈએ. બધા જ આવતા અને જતા સંદેશાઓ અન્ક્રિપ્ટેડ અને ડીક્રીપ્ટેડ (encrypted and decrypted) સ્વરૂપમાં રાખી મૂકવા જરૂરી છે.

l. ઈન્ટરનેટ બેંકિંગ સોફ્ટવેરને અમલમાં મૂકતા પહેલા બેંકોએ વ્યાપારી/સેવા પૂર્તિકારો (service providers) પાસેથી એપ્લીકેશનની અખંડિતતા અંગેનું નિવેદન (application integrity statement) મેળવવું જરૂરી છે.

m. પ્રણાલીઓ તેમજ એપ્લીકેશન્સ (Systems and Applications)નો ઉપયોગ રોજિંદા પરિચાલનો (normal operations) માટે કરતાં પહેલા સુરક્ષા માળખાનું બરાબર પરીક્ષણ કરી લેવું જોઈએ. વધુ સારી સુરક્ષા અને અંકુશને પ્રાપ્ત કરવાના હેતુથી બેંકોએ સમયાંતરે તેમની પ્રણાલીઓ (systems) ને નવા વર્ઝન (newer versions) થી અપડેટ કરવી જોઈએ.

n. તારીખ 4 ફેબ્રુઆરી 1998ના પરિપત્ર ડીબીએસ.સીઓ.આઈટીસી.બીસી. 10/31.09.001/97-98 તેમજ તારીખ 30 માર્ચ 1998ના પરિપત્ર યુબીડી.સં.

એડીએમએન. 46બી/17.36.00 થકી 'કોમ્પ્યુટર અને દૂરસંચારમાં જોખમો અને અંકુશો (Risks and Controls in Computers and Telecommunication)' વિષય ઉપર ભારતીય રિઝર્વ બેંક દ્વારા જારી કરવામાં આવેલી માર્ગદર્શિકાઓ તથા માહિતી સુરક્ષા, ઈલેકટ્રોનિક બેંકિંગ, પ્રૌદ્યોગિકી જોખમ સંચાલન અને સાયબર ધોખાધડી ઉપર કાર્યકારી દળની ભલામણો (Recommendations of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds)(અધ્યક્ષ: શ્રી ગોપાલકિષ્ના, કાર્યકારી નિર્દેશક) અંગે બેંકોને પાલન કરવાનું સૂચિત કરતો તારીખ 29 એપ્રિલ 2011 નો પરિપત્ર સં. ડીબીએસ.સીઓ.આઈટીસી .બીસી.સં.6/31.02.008/2010-11 પણ ઈન્ટરનેટ બેંકિંગને સમાન ધોરણે લાગુ પડશે.

o. રાજ્ય સહકારી બેંકો તેમજ જીલ્લા મધ્યસ્થ સહકારી બેંકો (StCBs/DCCBs) ના કિસ્સામાં, નાબાર્ડના તારીખ 25 ફેબ્રુઆરી 2015 ના પરિપત્ર એનબી.ડીઓએસ.એચઓ. પીઓએલ.સં.3634/જે-1/2014-15માં દર્શાવેલી 'માહિતી પ્રણાલી ઓડિટ નીતિનો પ્રારંભ (Introduction of IS Audit Policy)' ઉપરની માર્ગદર્શિકાઓ પણ લાગુ પડશે.

II. **કાનૂની મુદ્દાઓ:**

a. બેંક ગ્રાહકને ઈન્ટરનેટ બેંકિંગ સુવિધા તો જ પૂરી પાડશે જો તેણે/તેણીએ તે માટે હકારાત્મક કબુલાત સાથે લેખિત અથવા અધિકૃત ઈલેકટ્રોનિક માગણી કરેલી હોય.

b. પ્રવર્તમાન કાયદાકીય પરિસ્થિતિને ધ્યાનમાં લેતા, બેંકોનું એ કર્તવ્ય બને છે કે તેઓએ ઈન્ટરનેટ બેંકિંગની સુવિધા માટે માગણી કરતા ગ્રાહકની ઓળખ તો પ્રસ્થાપિત કરવી જ પણ સાથે સાથે તેની વિશ્વનીયતા તેમજ શાખ માટે જરૂરી પૂછપરછ પણ કરવી. તેથી, ભલે ઈન્ટરનેટના માધ્યમ દ્વારા ખાતું ખોલવા માટે વિનંતિ સ્વીકારવામાં આવી હોય, પણ ગ્રાહકની ઓળખની પૂરતી ચકાસણી અને આપના ગ્રાહકને ઓળખો (કેવાયસી) અંગેની માર્ગદર્શિકાઓનું પરિપાલન થયા બાદ

જ ખાતું ખોલવું.

c. કાનૂની પરિપ્રેક્ષ્યમાં, યુસર (user)ને અધિકૃત કરવા માટે બેંકો દ્વારા અપનાવવામાં આવેલી સુરક્ષા ક્રિયાવિધિઓ (security procedures), એ હસ્તાક્ષરના વિકલ્પ તરીકે કાયદા દ્વારા માન્ય ગણાવી જરૂરી છે. ઈન્ટરનેટ બેંકિંગ સુવિધા પૂરી પાડતી વખતે માહિતી પ્રૌદ્યોગિકી અધિનિયમ, 2000 (Information Technology Act, 2000) ની જોગવાઈઓ તેમજ અન્ય કાનૂની આવશ્યકતાઓનું ચૂસ્તપણે પાલન થવું જરૂરી છે.

d. હાલના સમયમાં, ગ્રાહકોના ખાતાની તેમજ અન્ય માહિતીની ગુપ્તતા તેમજ વિશ્વસનીયતા જાળવી રાખવી બેંકો માટે અનિવાર્ય છે. ઈન્ટરનેટ બેંકિંગના માહોલમાં ઉપરના કર્તવ્યનું પરિપાલન નહીં કરતી બેંકોનું જોખમ અમુક કારણોને લઈને વધી જાય છે. અગમચેતીના બધા જ વ્યાજબી પગલા લેવા છતાં, હેકીંગ/પ્રૌદ્યોગિકી નિષ્ફળતા (hacking/technological failures)ને કારણે થતાં ગુપ્તતાના ભંગ તેમજ સેવા નકાર વિ. ના બનતા બનાવોને લઈને બેંકોની ગ્રાહકો પ્રત્યેની જવાબદારીનું જોખમ ઘણું વધી જાય છે. આથી બેંકો પાસે જોખમની સંભાળ લેવા માટે જોખમોને અંકુશમાં લેવા માટેના યોગ્ય પગલા લેવાની જોગવાઈ હોવી જરૂરી છે.

## III. આંતરિક અંકુશ પ્રણાલી:

બેંકોએ ઈન્ટરનેટ બેંકિંગ સુવિધા શરૂ કરતા પહેલા સંગીન આંતરિક અંકુશ પ્રણાલી વિકસાવવી જોઈએ. આ પ્રણાલીમાં ઈન્ટરનેટ બેંકિંગ સંબંધિત આંતરિક નિરીક્ષણ(internal inspections)/પ્રણાલીઓ તેમજ ક્રિયાવિધિઓનું ઓડિટ (audit of systems and procedures) તેમજ ડેટાની અખંડિતતા, ગ્રાહકની વિશ્વસનીયતા અને ડેટાની સુરક્ષા જળવાઈ રહે તે માટેના યોગ્ય અગમચેતીરૂપ વ્યવસ્થા અમલમાં છે તેની ખાતરી કરવાની બાબતોનો સમાવેશ થાય છે. ઈન્ટરનેટ બેંકિંગ દ્વારા થતા લેણ-દેણના વ્યવહારો ઉપર નાણાંકીય મર્યાદાઓ નિર્ધારિત કરવાનો પણ બેંકો વિચાર કરી શકે છે. આંતરિક અંકુશ પ્રણાલીમાં નીચેની બાબતોનો સમાવેશ થવો જોઈએ:

a. **કામગીરી અને જવાબદારીઓ/વ્યવસ્થાતંત્રનું માળખું:** આંતરિક અંકુશ પ્રણાલી અસરકારક રીતે પરિચાલિત થતી રહે તેની ખાતરી કરવી, એ નિર્દેશકોના બોર્ડ અને વરિષ્ઠ સંચાલકોનું ઉત્તરદાયિત્વ છે. બોર્ડની ઓડિટ સમિતિમાં માહિતી પ્રણાલીઓ (information systems) અને તે સંબંધિત અંકુશો અને ઓડિટની બાબતોનું જરૂરી જ્ઞાન ધરાવતો એક પદનામિત સભ્ય હોવો જોઈએ.

b. **ઓડિટ નીતિમાં માહિતી પ્રણાલિઓના ઓડિટ (IS Audit) નો સમાવેશ:** માહિતી પ્રણાલીઓનું ઓડિટ એ બેંકના આંતરિક ઓડિટનો એક મહત્વનો હિસ્સો હોવો જોઈએ. બેંકોએ એક એવી પ્રણાલી અમલમાં મૂકવી જોઈએ જેના થકી મજબૂત ઓડિટ ટ્રેઈલનું નિર્માણ થાય જે ઓડિટ કરવામાં સગવડરૂપ થાય, જરૂરિયાતના સમયમાં ફોરેન્સિક પુરાવા પણ પૂરા પાડે અને વિવાદોના ઉકેલમાં સહાયરૂપ થાય.

c. **રિપોર્ટીંગ અને અનુવર્તી કાર્યવાહી:** આમાં કર્મચારીઓ દ્વારા ઉચ્ચ સત્તાવાળાઓને રિપોર્ટીંગ કરવાની પ્રણાલીનો સમાવેશ થાય છે. સુરક્ષા પ્રણાલીઓ અને કાર્યવિધિઓ (information systems and procedures) માં આકાર લેતી કોઈપણ પ્રકારના ભંગ યા નિષ્ફળતાની ઘટનાઓનું રિપોર્ટીંગ ઉચ્ચ સત્તાવાળાઓને તેમજ ઓડિટ સમિતિને કરવું જોઈએ. માહિતી પ્રણાલીઓના ઓડિટરો (IS Auditors) ઓડિટ સમરી મેમોરેન્ડમ તૈયાર કરશે જે આયોજનથી શરૂ કરીને ઓડિટ તારણો સુધીની સમગ્ર ઓડિટ પ્રક્રિયાનું વિહંગાવલોકન કરાવશે અને જેનું ઓડિટ કરવામાં આવ્યું છે તેની જોડે ઓડિટના તારણોની ચર્ચા કરશે અને તેમના પ્રતિભાવો મેળવશે. ઓડિટના તારણોના પરિપાલન માટે સહકારી બેંકોની પોતાની એક સમયબદ્ધ અનુવર્તી નીતિ (time bound follow-up policy) હોવી જોઈએ. સુરક્ષા તેમજ ક્રિયાવિધિઓમાં થતી ગંભીર ચૂકની ઘટનાઓથી નિર્દેશકોના બોર્ડને વાકેફ રાખવું જરૂરી છે.

મોટી સાયબર સુરક્ષાને લગતી ઘટનાઓ વિષે બોર્ડ/ઉચ્ચ સંચાલન/ભારતી રિઝર્વ બેંક/નાબાર્ડને ક્રમશ: વધતા સ્તરે સૂચિત કરવા માટે બેંકો પાસે પોતાની એક સંદેશા-સંચારની યોજના હોવી જોઈએ.

## IV. અન્ય મુદ્દાઓ તેમજ સ્પષ્ટતાઓ:

બેંકો માટેના હાલના વિનિયમનકારી માળખાને (regulatory framework) ઈન્ટરનેટ બેંકિંગ પ્રતિ પણ પ્રસારવામાં આવશે. આ સંદર્ભમાં, બેંકોને સૂચિત કરવામાં આવે છે કે:

a. ઈન્ટરનેટ બેંકિંગ હેઠળના ઉત્પાદો (products) ફક્ત ખાતેદારો પૂરતા જ સીમિત હોવા જોઈએ.

b. સેવાઓમાં ફક્ત સ્થાનિક ચલણના જ ઉત્પાદો (local currency products)નો જ સમાવેશ થવો જોઈએ.

c. ઈન્ટરનેટ થકી ગ્રાહકો દ્વારા કરવામાં આવતા બેંકિંગના વ્યવહારોમાં રહેલા જોખમો અને તે અંગેની તેમની જવાબદારીઓ અને ઉત્તરદાયિત્વ અંગેની સ્પષ્ટતાઓ સહકારી બેંકોએ કરવી જોઈએ.

d. ઈન્ટરનેટ બેંકિંગ સુવિધા પૂરી પાડતી વખતે બેંકોએ આપના ગ્રાહકને ઓળખો (કેવાયસી) માર્ગદર્શિકાઓ /ધન-શોધન નિવારણ ધોરણો તેમજ ધનશોધન નિવારણ અધિનિયમ, 2002ની જોગવાઈઓ તેમજ તે હેઠળ જારી કરવામાં આવેલા નિર્દેશોનું પાલન કરવું જરૂરી છે

**અનુબંધ-II**

**ઈન્ટરનેટ બેંકિંગ – સુરક્ષા આવશ્યકતાઓ:**

1. સહકારી બેંકોએ તેઓની વેબ એપ્લીકેશન્સની સુરક્ષા માટે યોગ્ય પ્રકારના લેવાયા છે તે બાબતની ખાતરી કરવી જોઈએ અને વેબની સુરક્ષા સામેના જોખમોને ડામવા માટેના યોગ્ય શામક પગલા લેવા જોઈએ.

2. ડેટાની અખંડિતતા જોખમાય નહીં તે માટે વેબ એપ્લીકેશનની અંદર એચટીએમએલના પ્રચ્છન્ન ક્ષેત્રોમાં (HTML hidden fields), કૂકીઝમાં (cookies) કે પછી અન્ય કોઈ ગ્રાહક-પક્ષની માહિતી સંગ્રહ (client-side storage) ના સ્થાનમાં કોઈ સંવેદનશીલ માહિતીનો સંગ્રહ ન કરવો. વિશિષ્ટ વેબ એપ્લીકેશન્સ બધી જ ઓન-લાઈન પ્રવૃત્તિઓનું અલ્પતમ એસએસએલ વી૩ (SSL v3) અથવા તો વિકસિત વેલીડેશન – એસએસએલ/ટીએલએસ 1.0 128 (Extended Validation - SSL/TLS 1.0 128)માં એન્ક્રિપ્શન (encryption) કરતુ હોવું જોઈએ.

3. એક ચાલુ સેશનનો ભંગ થયા પછી તેની પુન:સ્થાપના માટે ઉપયોગકર્તા (user) ની ઓળખ, પ્રમાણભૂતતા તેમજ અધિકૃતતા જરૂરી છે. તદઉપરાંત સર્વર પક્ષે મજબૂત વેલીડેશન (server side validation) ઊભું કરવાની પણ જરૂર છે.

4. બધા જ પ્રૌદ્યોગિકી સ્તરે (technology levels) સહકારી બેંકોએ બળવાન સુરક્ષાના પગલાં લઈને ગહન રક્ષણ વ્યૂહને (defense-in-depth) અનુસરવાની જરૂર છે.

**ઈન્ટરનેટ બેંકિંગ માટે પ્રમાણીકરણની કાર્યપ્રણાલી:**

1. પ્રમાણીકરણની રીતોમાં ત્રણ મૂળભૂત 'પરિબળો'નો સમાવેશ થાય છે.
   - કોઈક એવી બાબત જે ઉપયોગકર્તા (user) જાણતો હોય (દા.ત. પાસવર્ડ, પીન)
   - કોઈક એવી બાબત જે ઉપયોગકર્તા પાસે હોય (દા.ત. એટીએમ કાર્ડ, સ્માર્ટ કાર્ડ)
   - કોઈક એવી બાબત જે ઉપયોગકર્તા છે (દા.ત. બાયોમેટ્રિક લક્ષણ જેમકે ફીંગરપ્રીન્ટ)

2. યોગ્ય રીતે ઘડી કાઢવામાં આવેલી અને અમલમાં મૂકવામાં આવેલી બહુવિધ-પરિબળ પ્રમાણીકરણ પ્રથાઓ (multi-factor authentication methods) વધુ આધારભૂત અને બળવાન છેતરપિંડી-પ્રતિબંધક (fraud-deterrent) હોય છે અને તેમાં તડજોડ કરવી મુશ્કેલ હોય છે. દ્વિ-પરિબળ પ્રમાણીકરણ પાછળના બે મુખ્ય ઉદ્દેશો છે. એક તો ગ્રાહકના ખાતાની તેમજ લેણ-દેણની માહિતીની વિશ્વસનીયતા જાળવી રાખવાનો અને બીજો બેંકો અને તેના ગ્રાહકોને નિશાન બનાવતા અનેક પ્રકારના સાયબર હુમલાઓ જેવાકે ફિશીંગ (phishing), કીલોગીંગ (keylogging), સ્પાયવેર/માલવેર (spyware/malware) અને અન્ય ઈન્ટરનેટ આધારિત છેતરપિંડીઓની ઘટનાઓનો પ્રતિકાર કરીને ઈન્ટરનેટ બેંકિંગમાં વિશ્વાસની વૃદ્ધિ થાય તે છે.

**ઈન્ટરનેટ બેંકિંગ માટે દ્વિ-પરિબળ પ્રમાણીકરણ (two-factor authentication) અને સુરક્ષા માટેના અન્ય પગલાંનો અમલ:**

a. સાયબર હુમલાઓની પ્રચૂરતા અને તેના સંભવિત પરિણામોને ધ્યાનમાં લેતા, બેંકોએ ઈન્ટરનેટ દ્વારા નિધિ હસ્તાંતરણ (fund transfer) માટે દ્વિ-પરિબળ પ્રમાણીકરણને અમલમાં મૂકવું જોઈએ.

b. યોગ્ય પ્રમાણીકરણની પ્રથાઓના અમલનો આધાર સંસ્થાની ઈન્ટરનેટ બેંકિંગ પ્રણાલીઓથી ઊભા થતા સંભવિત જોખમોની આકારણી ઉપર રહેલો છે. ગ્રાહકના પ્રકાર (દા.ત. છૂટક અથવા કોર્પોરેટ/વાણીજ્યિક), ગ્રાહકની લેણ-દેણના વ્યવહારની ક્ષમતા (દા.ત. બિલ ચૂકવણી, નિધિ હસ્તાંતરણ), ગ્રાહકની માહિતીની સંવેદનશીલતા તેમજ લેણ-દેણના વ્યવહારોના કદ વિગેરેને ધ્યાનમાં લઈને જોખમોનું મૂલ્યાંકન કરવું જોઈએ.

c. પ્રૌદ્યોગિકી પરિબળ સિવાય, કોઈ એક ચોક્કસ પ્રમાણીકરણની પ્રથાની સફળતાનો આધાર યોગ્ય નીતિઓ (policies), ક્રિયાવિધિઓ (procedures) અને અંકુશો (controls) ઉપર પણ રહેલો છે. અસરકારક પ્રમાણીકરણ પ્રથા ગ્રાહકની સ્વીકૃતિ, ઉપયોગ કરવાની સરળતા, વિશ્વસનીય કામગીરી, વિકસતી પ્રૌદ્યોગિકીનો સમાવેશ કરવાની માપનીયતા

(scalability to accommodate growth) અને બીજી પ્રણાલીઓ સાથે તેની પરિચાલિત ક્ષમતા (interoperability with other systems) વિગેરે બાબતોની ગણના કરે છે.

d. ઇલેકટ્રોનિક લેણ-દેણના વ્યવહારોના પ્રમાણીકરણમાં એસિમેટ્રિક ક્રિપ્ટોસિસ્ટમ (asymmetric cryptosystem) અને હેસ ફંક્શન (hash function) નો ઉપયોગ ન કરવામાં આવે તો તેમાં કાયદાકીય જોખમ રહેલું છે. મહત્વના વ્યવહારો જેવાકે નિધિ હસ્તાંતરણ કરવા માટે બેંકોએ, અલ્પતમ, બળવાન અને ગતિશીલ દ્વિ-પરિબળ પ્રમાણીકરણની પ્રથા અમલમાં મૂકવી જોઈએ જેમાં પહેલા પરિબળમાં ઉપયોગકર્તાનો આઈડી/પાસવર્ડનું સંયોજન અને બીજા પરિબળ તરીકે (a) ડીજીટલ હસ્તાક્ષર (ડીજીટલ પ્રમાણપત્ર અને સાથે ખાનગી કી સહિતના ટોકન દ્વારા, ખાસ કરીને કોર્પોરેટ ગ્રાહકો માટે) અથવા (b) એક સમયના પાસવર્ડ (One Time Password – OTP)/ ગતિશીલ સંપર્ક કોડ (dynamic access code) જેને અનેક પ્રકારે મોકલી શકાય (જેમકે મોબાઈલ ફોન ઉપર એસએમએસ અથવા હાર્ડવેર ટોકન).

e. ઓન-લાઈન થતી પ્રક્રિયાઓની સુરક્ષા વધારવા માટે અમુક પ્રકારના વ્યવહારોમાં જેવાકે પ્રી-સેટ મૂલ્યની ઉપરના વ્યવહારો માટે, નવી એકાઉન્ટ લિંકેજીસ ઉત્પન્ન કરવા માટે, ત્રાહિત પક્ષ આદાતાની વિગતો નોંધવા માટે, ખાતાની વિગતોમાં ફેરફાર કરવા માટે અથવા નિધિ હસ્તાંતરણની મર્યાદાને શંશોધિત કરવા માટે, બીજી સમર્થનકારી ક્રિયાવિધિઓ – confirmatory second channel procedures - (જેવીકે ટેલીફોન, એસએમએસ, ઈ-મેઇલ વિ.) લાગુ કરવી જરૂરી છે. આ પ્રકારની સુરક્ષા વિશેષતાઓ (security features) ની રચના કરતી વખતે બેંકોએ પોતાના સામર્થ્ય તેમજ વિશેષ ઓન-લાઈન સુરક્ષા સંબંધિત ગ્રાહકોની અલગ અલગ પસંદગીને ધ્યાનમાં લેવી જોઈએ.

f. પરસ્પરના પ્રમાણીકરણના શિષ્ટાચાર (mutual authentication protocol) ઉપર આધાર રાખીને ગ્રાહકો પણ અંગત ખાતરીદાયક સંદેશાઓ (personal assurance messages)/પ્રતિમાઓ (images), ચેલેન્જ રીસપોન્સ કોડ્સના વિનિમય (exchange of challenge response security codes), સિક્યોર સોકેટ લેયર સર્વર સર્ટિફીકેટ ચકાસણી

(Secure Sockets Layer – SSL- server certificate verification) જેવી સુરક્ષા કાર્યપદ્ધતિઓનો ઉપયોગ કરીને બેંકની વેબસાઇટનું પ્રમાણીકરણ કરી શકે છે. હાલના સમયમાં, એક્સટેન્ડેડ વેલીડેશન સીક્યોર સોકેટ લેયર (Extended Validation Secure Socket Layer – EV-SSL) પ્રમાણપત્રનો ઉપયોગ વધી રહ્યો છે. આ વિશેષ પ્રકારના એસએસએલ (SSL) પ્રમાણપત્રો છે જે વેબસાઇટની વ્યવસ્થાજન્ય ઓળખને સ્પષ્ટપણે પારખવા માટે ઉચ્ચ કક્ષાની સુરક્ષા સહિતના વેબ બ્રાઉઝરો જોડે કાર્ય કરે છે. પણ એ બાબતની નોંધ લેવી ઘટે કે એસએસએલ ફક્ત નેટવર્ક ટ્રાન્સપોર્ટ લેયર તરફ માર્ગમાં જઈ રહેલ ડેટાને અન્ક્રિપ્ટ કરવા માટે સર્જાયેલ છે. તે એપ્લીકેશન લેયર સુધી એક છેડાથી બીજા છેડા સુધીનું એન્ક્રિપ્શન પૂરું પાડતું નથી.

(Original English Text: Based on mutual authentication protocols, customers could also authenticate the bank's web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes and/or the Secure Sockets Layer (SSL) server certificate verification. In recent times, Extended Validation Secure Sockets Layer (EV-SSL) Certificates are increasingly being used. These are special SSL Certificates that work with high security web browsers to clearly identify a website's organizational identity. It should, however, be noted that SSL is only designed to encrypt data in transit at the network transport layer. It does not provide end-to-end encryption security at the application layer.)

g. કોઈ પણ પ્રમાણિત સેશન (authenticated session), ગ્રાહકની જોડેનો સંવાદ જારી હોય ત્યાં સુધી અખંડ રહેવી જોઈએ. જો વચ્ચે કોઈ હસ્તક્ષેપ થાય તો સેશનનો અંત લાવી દેવો જોઈએ અને અસરગ્રસ્ત લેણ-દેણના વ્યવહારોનો ઉકેલ લાવવો જોઈએ યા તો ઉલટાવી દેવા જોઈએ. ગ્રાહકને, જ્યારે સેશનનો અંત આવે, ત્યારે આવી કોઈ પણ ઘટનાની તરત જાણ કરવી જોઈએ અથવા તો પછીથી ઈ-મેઇલ, ટેલીફોન કે બીજા કોઈ માધ્યમથી જાણ કરવી જોઈએ.

h. ફક્ત શાખા તરફથી વિનંતિ પ્રાપ્ત થાય ત્યારે જ મોબાઈલ ફોન નંબરમાં ફેરફાર કરવો જોઈએ.

i. વર્ચ્યુઅલ કી-બોર્ડ અમલમાં મૂકવું જોઈએ.

j. જ્યારે નવા લાભાર્થીઓનો ઉમેરો કરવામાં આવે ત્યારે નવા લાભાર્થીઓનો ઉમેરો કરવા માટે તેમજ એસએમએસ/ઈ-મેઇલ એલર્ટ માટે કુલીંગ પીરીયડ દાખલ કરવો જોઈએ.

k. ગ્રાહકોને પોતાના અંગત કોમ્પ્યુટરના રક્ષણાર્થે વિવિધ પ્રકારની સુરક્ષા માટેની અગમચેતીઓ તેમજ કાર્યપ્રણાલીઓ અપનાવવા માટે સલાહ આપવી જોઈએ અને તેઓને જાહેર જગ્યાએથી કે ઈન્ટરનેટ કાફેના કોમ્પ્યુટરો ઉપરથી નાણાકીય વ્યવહારો ન કરવા માટે સમજાવવા જોઈએ.

l. જોખમ-આધારિત લેણ-દેણના વ્યવહારો ઉપરનો જાપ્તો અથવા દેખરેખની પ્રક્રિયા, એ બંને સંલગ્ન ગણાવા જરૂરી છે.

m. જો ગ્રાહક પ્રવર્તમાન સેશનને જાળવી રાખવા માટે પુન:પ્રમાણીકરણ ન કરે તો અમુક ચોક્કસ સમયગાળા પછી ઓનલાઈન સેશનનો આપોઆપ અંત આવી જવો જોઈએ. આ પ્રકારની વ્યવસ્થા હુમલાખોરને ઓનલાઈન બેંકિંગ સેશન અનિશ્ચિત સમય સુધી જારી રાખવામાંથી અટકાવે છે.

n. વ્યાખ્યા મુજબ, સાચા બહુપરિબળ પ્રમાણીકરણ (multifactor authentication) માટે બે કે તેથી વધુ ત્રણ પરિબળોના વર્ગમાંથી સમાધાનનો ઉપયોગ આવશ્યક છે. પ્રક્રિયામાં જુદા જુદા ઠેકાણે એક જ વર્ગમાંથી પ્રાપ્ત એવા બહુવિધ સમાધાનોનો ઉપયોગ, એ કદાચ લેયર્ડ સુરક્ષાનો યા અન્ય કોમ્પેનસેટીંગ કન્ટ્રોલ એપ્રોચનો હિસ્સો હોઈ શકે, પણ તે સાચું બહુપરિબળ પ્રમાણીકરણ ઠરતું નથી.

(Original English Version: By definition, true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute a true multifactor authentication.)

o. દ્વિ-પરિબળ પ્રમાણીકરણ શિલ્પના આવશ્યક હિસ્સા રૂપે, બેંકોએ વચેટીયાઓના હુમલાની પ્રત્યેના એક્સપોઝરને ઘટાડવા માટેના યોગ્ય પગલા લેવા જોઈએ જે સામાન્ય રીતે મેન-ઈન-ધી-મિડલએટેક (man-in-the-middle attack – MITM), મેન-ઈન-ધી બ્રાઉઝર (man-in-the browser – MITB) એટેક અથવા મેન-ઈન-ધી-એપ્લીકેશન (man-in-the application) ના નામથી ઓળખાય છે.

p. બેંકોએ મેન-ઈન-ધી-મિડલ હુમલા પ્રત્યેના એક્સપોઝરને ઘટાડવા, જો યોગ્ય લાગે તો, નીચેના અંકુશ અને સુરક્ષા અંગેના પગલા લેવા જોઈએ.

(i) **નવા આદાતા (payee)ને ઉમેરવા માટે વિશિષ્ટ એક વખતના પાસવર્ડ્સ (ઓટીપી-OTPs):** દરેક નવો અદાતા, ગ્રાહક દ્વારા બીજી ચેનલમાંના ઓટીપીના આધારે અધિકૃત થયેલો હોવો જોઈએ જે અદાતાની વિગતો અથવા તો મેન્યુઅલ ક્રિયાવિધિથી મેળવેલા ગ્રાહકના હસ્તાક્ષર પણ દર્શાવે છે જેની બેંક દ્વારા ચકાસણી થાય છે.

(ii) **મૂલ્ય સહિતના વ્યવહારો (ચૂકવણી અને નિધિ હસ્તાંતર) માટે વ્યક્તિગત ઓટીપી:** દરેક મૂલ્ય સહિતના વ્યવહાર અથવા તો ગ્રાહક દ્વારા નિર્ધારિત કરવામાં આવેલ ચોક્કસ મૂદ્રાકીય મર્યાદાથી ઉપરના મૂલ્ય સહિતના વ્યવહારો માટે નવો ઓટીપી જોઈએ.

(iii) **ઓટીપી ટાઈમ વિંડો:** ચેલેંજ-આધારિત અથવા સમય-આધારિત ઓટીપીસ ખૂબ બળવાન સુરક્ષા પૂરી પાડે છે કારણકે તેની માન્યતાના સમય (period of validity)નું સમગ્રપણે બેંક દ્વારા નિયમન થાય છે અને ઉપયોગકર્તાના વર્તન ઉપર તેનો આધાર હોતો નથી. એવી ભલામણ કરવામાં આવે છે કે બેંકોએ ઓટીપી ટાઈમ વિંડોને, સર્વર સમય ની કોઈપણ બાજૂએ (on either side of the server time), 100 સેકંડથી વધુ સમય માટે વધવા ન દેવી જોઈએ કારણકે ટાઈમ વિંડો જેટલી નાની, એટલું ઓટીપીના દુરુપયોગનું જોખમ ઓછું થાય છે.

(iv) **ચૂકવણી અને નિધિ હસ્તાંતર સુરક્ષા:** ચૂકવણી અને નિધિ હસ્તાંતરના વ્યવહારોમાં થતા અનધિકૃત સુધારાવધારા અથવા તો મિડલમેન હુમલા થકી દાખલ થતા વ્યવહારોના ડેટા (injection of transaction data in middleman attack)ને શોધી કાઢવા માટે ડીજીટલ હસ્તાક્ષર અને કી-આધારિત સંદેશા પ્રમાણીકરણ કોડ્સ (Key-based Message Authentication Codes – KMAC) નો ઉપયોગ ધ્યાનમાં લેવો જોઈએ. આવા પ્રકારના સુરક્ષા સમાધાનને વધુ અસરકારક બનાવવા માટે,

હાર્ડવેર ટોકનનો ઉપયોગ કરતો ગ્રાહક એટલો સક્ષમ હોવો જોઈએ કે તે એક વખતના પાસવર્ડ (ઓટીપી) નિર્માણ કરવાની પ્રક્રિયાને, લેણ-દેણના વ્યવહારને ડીજીટલી હસ્તાક્ષરિત કરવાની પ્રક્રિયાથી અલગ તારવી શકે. તે જે ડીજીટલી હસ્તાક્ષરિત કરે છે તે તેના માટે અર્થપૂર્ણ હોવું જોઈએ, એટલે કે ટોકને સ્પષ્ટપણે અદાતા (payee)નો ખાતા નંબર અને ચૂકવણીની રકમ દર્શાવવા જોઈએ જેના ઉપરથી ડીજીટલ હસ્તાક્ષરનું નિર્માણ કરવા માટે હેસ વેલ્યુ (hash value) શોધી શકાય.

(v) ઈન્ટરનેટ બેંકિંગ માહોલમાં, બેંકો માટે ગ્રાહકની ચૂકવણી-રોકો સૂચના (stop-payment instructions) ઉપર કાર્ય કરવા માટે ઘણો જૂજ અવકાશ રહે છે. આથી બેંકોએ ગ્રાહકોને તે સમયગાળો અને સંજોગો અંગેની બરાબર સ્પષ્ટતા કરવી જોઈએ કે જેમાં તે ગ્રાહકની ચૂકવણી-રોકો સૂચનાનો સ્વીકાર કરી શકશે.

(vi) ગ્રાહક સુરક્ષા અધિનિયમ, 1986 (The Consumer Protection Act, 1986) ભારતમાં ગ્રાહકના હક્કોને વ્યાખ્યાન્વિત કરે છે અને તે બેંકિંગ સેવાઓને પણ લાગુ પડે છે. ઈન્ટરનેટ બેંકિંગનો વિકલ્પ પસંદ કરતા ગ્રાહકોને ઈન્ટરનેટ બેંકિંગનો લાભ લેવામાં શું હક્કો પ્રાપ્ત થાય છે અને શું જવાબદારીઓ ઊભી થાય છે તે અંગે સ્પષ્ટપણે સમજાવવા જોઈએ. ગ્રાહક દ્વારા ભોગવવામાં આવતી પરંપરાગત બેંકિંગની કાર્યપ્રણાલીઓ અને હક્કોને ધ્યાનમાં લેતા, બેંકોએ, હેકીંગ તેમજ પ્રૌદ્યોગિકી નિષ્ફળતાને પરિણામે થતા સેવા નકારને કારણે બનતા બિનઅધિકૃત હસ્તાંતરના કિસ્સાઓમાં પોતાના ગ્રાહકો પ્રત્યેની ઊભી થતી જવાબદારીની આકારણી કરવાની જરૂર છે અને ઈન્ટરનેટ બેંકિંગની સેવાઓ પૂરી પાડતી બેંકોએ આવા જોખમો સામે વિમારક્ષણ લેવાની પણ જરૂર છે.

(vii) બેંકોની વેબસાઈટ્સ ઉપરથી હાયપરલીંક્સને પરિણામે વારંવાર શાખની સામે જોખમનો મુદ્દો ઊભો થાય છે. આવી લીંક્સથી ગ્રાહકોને એવી ગેરસમજ પેદા ન થવી જોઈએ કે બેંક તેના બેંકિંગના કારોબાર સાથે સંબંધિત ન હોય તેવા કોઈ ખાસ ઉત્પાદન કે કોઈ કારોબારનું પ્રવર્તન કરે છે. બેંકની વેબસાઈટ ઉપરથી હાયપરલીક્સ એવા જ પોર્ટલ્સ સાથે જોડાયેલી હોવી જોઈએ જેની સાથે બેંકે

ચૂકવણી માટેની વ્યવસ્થા (payment arrangement) કરી હોય. બીજા પોર્ટલો ઉપરથી બેંકની વેબસાઈટ ઉપરની હાયપરલીંક સામાન્ય રીતે બેંકના ગ્રાહકોએ તે પોર્ટલો ઉપરથી કરેલી ખરીદીની માહિતી પહોંચાડવા માટે હોય છે. બીજી વેબસાઈટ્સ ઉપરથી ગ્રાહકોએ કરેલી ખરીદીના સંદર્ભમાં આવતી વિનંતિઓની ચૂકવણી કરતી વખતે બેંકે ભલામણ કરવામાં આવેલી સુરક્ષા માટેની અગમચેતીઓને અનુસરવી જ પડશે.

(viii) **બીજી ચેનલ થકી સૂચના / પુષ્ટિ**: ગ્રાહક દ્વારા નિશ્ચિત કરવામાં આવેલા મૂલ્યથી ઉપરના કોઈપણ ચૂકવણીના કે નિધિ હસ્તાંતરના વ્યવહારની સૂચના બેંકે બીજી ચેનલ દ્વારા ગ્રાહકને આપવાની રહેશે.

(ix) **એસએસએલ સર્વર પ્રમાણપત્ર ચેતવણી**: એસએસએલ અથવા ઈવી-એસએસએલ પ્રમાણપત્ર ચેતવણી (SSL or EV-SSL Certificate warning) સામે કેવી રીતે પ્રતિભાવ આપવો તે અંગે ઈન્ટરનેટ બેંકિંગના ગ્રાહકોને જાગૃત કરવા અને સમજાવવા જોઈએ.

(x) બેંકોએ જોખમયુક્ત વ્યવહારો ઉપર જાપ્તો અને દેખરેખ રાખવા માટેની પ્રક્રિયા અમલમાં મૂકવી જોઈએ. ગ્રાહક દ્વારા કરવામાં આવતા લેણ-દેણના વ્યવહારોનો અભ્યાસ અને કોઈ પણ અનિયમિત વ્યવહારને થતો અટકાવવો અથવા આવા અપવાદરૂપ વ્યવહાર માટે ગ્રાહકોની પૂર્વ મંજૂરી લેવા વિગેરેની જોગવાઈઓ સોફ્ટવેરમાં કરાવવી જોઈએ.