सुरक्षित ऑनलाइन बैंकिंग बनाम ग्राहक सुविधा - अवसर और चुनौतियाँ *

जी. पद्मनाभन

मुझे प्रसन्नता है कि आज मुझे आपके बीच सुरक्षित बैंकिंग के वार्षिक सम्मेलन - वर्ष 2011 में उपस्थित होने और इस विषय पर अपने विचारों को आपके साथ बाँटने का अवसर प्राप्त हुआ है । मैं भारतीय बैंक संघ (आइबीए) एमपीटीएफसीएल, जो सम्मेलन के सह-आयोजक हैं, को मुझे यह अवसर प्रदान करने के लिए धन्यवाद देता हूँ ।

2. जैसाकि हम सभी जानते हैं, बैंकिंग एक व्यावसायिक कार्यकलाप होता है जो विश्वास का समानार्थी होता है और बैंकिंग में सुरक्षा उसमें विश्वास के लिए सर्वोपरि परिकल्पना होती है । बैंकिंग में ऐसी सुरक्षा की अवधारणा और बोध में कालक्रम से घोर परिवर्तन हुआ है जो बैंकिंग व्यवसाय के संचालन में हुए परिवर्तनों के आगे-पीछे के क्रम में हुआ है । बैंकों की आस्तियों का रखरखाव उन्हें भौतिक रूप में रखने की अपेक्षा डिजिटल रूप में किया जाता है, लेन देनों का निष्पादन प्रौद्योगिकी समर्थित प्लैटफार्म /एप्लीकेशन द्वारा किया जाता है और तत्संबंधी संप्रेषण इलेक्ट्रॉनिक तरीके से किया जाता है । भौतिक, भौगोलिक और उत्पाद सीमाएँ अब बैंकिंग व्यवसाय की वृद्धि के लिए अवरोधक नहीं रह गयी हैं और यह व्यवसाय द्रुत गति से विस्तारित हो रहा है । अब उत्पाद और सुपुर्दगी के नये माध्यम आ गये हैं । नेटवर्क के वातावरण ने ग्राहक के घर तक बैंकिंग की सेवाएँ पहुँचाये जाने मे मदद की है । कहीं भी कभी भी बैंकिंग और सुपुर्दगी की नये माध्यमों यथा, एटीएम, ऑनलाइन बैंकिंग, आदि ने ग्राहक को बैंकिंग की सुविधा प्रदान की है और बड़ी संख्या में लोग अपने कारोबार और दैनिक जीवन में इंटरनेट बैंकिंग की सुविधा और उसके आसान उपयोग पर भरोसा करते हैं । लेकिन इससे सुरक्षा सहित दक्ष सुपुर्दगी के बारे में ग्राहक की अपेक्षा भी बढ़ती है । ग्राहक की निष्ठा बनाये रखना और इस प्रकार एक अति प्रतिस्पर्धात्मक इलेक्ट्रॉनिक उद्योग में व्यवसाय करना ग्राहक अपेक्षा के अनुसार सुपुर्दगी करने में निहित होता है।

3. आइटी समर्थित बैंकिंग वातावरण में यह बात ध्यान में रखनी होगी कि धोखाधड़ी की संभावना अंतरराष्ट्रीय स्तर पर हो गयी है । जैसाकि अक्सर कहा जाता है, एक श्रृंखला में यह ऐसी कमजोर कड़ी है, जो सर्वाधिक असुरक्षित होती है । अतः आरंभ में ही एक सुरक्षित प्लैटफार्म बना लेना न केवल महत्वपूर्ण होता है बल्कि यह भी आवश्यक है कि तथाकथित 'सुरक्षा' को अंतरराष्ट्रीय मानकों पर लगातार निर्देश-चिह्न के रूप में बनाये रखा जाये । ऐसे परिदृश्य में, सूचना की सुरक्षा के सभी तीन गुण यथा, गोपनीयता, अखंडता और उपलब्धता प्रवेश, भंडारण तथा लेन देन के सभी प्रासंगिक चरणों पर काफी महत्वपूर्ण हो जाते हैं । अतः बैंकिंग में सुरक्षा के बारे में बोध और उसके प्रति अनुक्रिया में आमूलचूल परिवर्तन हुआ है ।

4. इस संदर्भ में जिन आशंकाओं से हम सब परेशान हैं वे अनेक प्रकार के हैं जो पासवर्ड हैकिंग, कार्ड कॉपीइंग /क्लोनिंग से ले कर लेन देन, सूचना भंडारण और संचरण प्रक्रमों के विविध स्तरों पर आँकड़ों तथा पहचान की चोरी कर लिये जाने तक फैली हुई हैं । सुरक्षा का प्रबंध करना अन्य माध्यमों की तुलना में ऑनलाइन और फोन बैंकिंग में अधिक चुनौतीपूर्ण होता है । ऑनलाइन आशंकाएँ फाइसिंग अटैक, स्पाइवेयर. वायरस, ट्रोजन्स, की-लॉगर्स के रूप में अक्सर होती हैं । एटीएम से आशंका के रूप एटीएम स्किमिंग, ईव्सड्रॉपिंग, स्पूफिंग, सेवा-नकारना आदि होते हैं । इलेक्ट्रॉनिक लेन देन में पहचान चुराया जाना एक बढ़ता साइबर अपराध होता है । हैकिंग और पहचान चुराये जाने की नयी पद्धतियाँ नियमित रूप से सामने आती हैं और बैंकिंग उद्योग को अपना व्यवसाय और ग्राहक हित की रक्षा करने के लिए तत्परतापूर्वक कार्रवाई करनी होती है ।

5. सीएसआइएस (सेंटर फॉर स्ट्रेटेजिक एंड इंटरनैशनल स्टडीज) द्वारा प्रकाशित जानकारी के अनुसार मार्च 2010 और अप्रैल 2011 के बीच एफबीआइ ने ऐसी बीस घटनाओं की पहचान की जिनमें छोटे से लेकर मझौले आकार वाले अमरीकी कारोबारियों के ऑनलाइन बैंकिंग प्रत्यय को संकट में डाला गया । अप्रैल 2011 में धोखाधड़ी के प्रयासों में शामिल राशि 20 मिलियन अमरीकी डॉलर थी; वास्तविक पीड़ित व्यक्तियों की हानि 11 मिलियन अमरीकी डॉलर की हुई । मैं इस मुद्दे का संकेत इस तथ्य को उजागर करने के लिए कर रहा हूँ कि हैकरों ने बड़े संगठनों द्वारा क्रियान्वित बढ़ते सुरक्षा मानकों को देखते हुए छोटे और मझौले आकार वाले संगठनों को शिकार बनाना आरंभ कर दिया

* मुम्बई में 29 जुलाई 2011 को सुरक्षित बैंकिंग के संबध में वार्षिक सम्मेलन-2011 के अवसर पर श्री जी.पद्मनाभन, कार्यपालक निदेशक भारतीय रिजर्व बैंक द्वारा की गयी टिप्पणी । इन टिप्पणियों को तैयार करने में दी गयी सहायता के लिए हम श्री के.शिवरामन और श्री पी.के.चोफला के प्रति आभारी है ।

है । पुनः, वे अलग-अलग क्षेत्रों में उन असुरक्षित ठिकानों को निशाना बनाते हैं जहाँ सुरक्षा कम होती है ।

6. उपर्युक्त के अतिरिक्त, ग्राहक जागरूकता का अभाव अपने आप में एक महत्वपूर्ण चिंता है जो सुरक्षा के प्रति आशंका को बढ़ा देती है । एक सर्वेक्षण के निष्कर्षों के अनुसार, जो डीएससीआइ और केपीएमजी द्वारा भारतीय बैंकिंग में आँकड़ों की सुरक्षा और गोपनीयता की स्थिति के संबंध में वर्ष 2010 में कराया गया था, 'सर्वेक्षण में बैंकों द्वारा बतायी गयी सर्वाधिक महत्वपूर्ण सूचना सुरक्षा चुनौतियों में से एक चुनौती यह है कि सूचना सुरक्षा के बारे में ग्राहक जागरूकता का अभाव है और असुरक्षित ग्राहक लेन देनों से आशंका उत्पन्न होती है' । सीमाहीन साइबर स्पेस बैंकों को अंतरराष्ट्रीय स्तर पर किये जाने वाले संगठित अपराधों और नये युग की आशंकाओं के प्रति असुरक्षित बना देता है । पुनः, बैंक अन्य पक्षों के साथ अधिक व्यवहार करते हैं और इस प्रक्रिया में व्यवसाय संबंधी सूचना के बाँटे जाने से अन्य पक्ष जोखिमों का प्रबंध करना भी एक चुनौतीपूर्ण कार्य हो जाता है ।

7. अब मैं अपने अब तक के कथन के प्रमाणस्वरूप कुछ उदाहरण प्रस्तुत करता हूँ ।

8. आप जानते हैं कि भारतीय रिज़र्व बैंक ने लगभग दो वर्ष पहले सभी कार्ड नॉट प्रेजेंट लेन देनों के लिए सेकंड फैक्टर ऑफ ऑथेंटिकेशन की प्रणाली आरंभ की थी । इस उपाय ने ऑनलाइन कार्ड लेन देनों में अधिक सुरक्षा सुनिश्चित की है और ऑनलाइन धोखाधड़ियों की घटनाएँ काफी कम हो गयी हैं । सर्वाधिक महत्वपूर्ण बात यह है कि इसके परिणामस्वरूप इस तरीके में कार्ड लेन देनों में महत्वपूर्ण वृद्धि हुई है जो ग्राहक भरोसे के बढ़े हुए स्तर को प्रतिबिंबित करता है । शायद इसके परिणामस्वरूप, धोखाधड़ी करने वालों का ध्यान कार्ड प्रेजेंट लेन देनों की ओर चला गया है । उदाहरण के लिए चंडीगढ़ में कार्ड डाटा - उसके पिन सहित - कुछ एटीएम में चुरा लिये गये । चुरायी गयी जानकारी का उपयोग देश भर में विविध स्थानों से नकदी आहरित करने के वास्ते कार्डों का क्लोन बनाने में किया गया । निश्चित रूप से उन एटीएम में जहाँ से डाटा की चोरी हुई, सुरक्षा भंग हुई थी। यह बात महत्वपूर्ण है कि बैंकों को यह सोचना होगा कि इस मुद्दे से जूझने के लिए किस प्रकार प्रौद्योगिकी का उपयोग किया जाये ।

9. अपनी ओर से रिज़र्व बैंक ने 1 जुलाई 2011 से सभी कार्ड लेन देनों के लिए अलर्ट प्रणाली लागू की है भले ही इसमें किसी भी चैनल का प्रयोग किया जाये । इस प्रकार की प्रणाली से धोखाधड़ी रोक पाने में निश्चित रूप से मदद मिलेगी । तथापि, यह बैंकों की जिम्मेवारी है कि इस प्रणाली को कारगर बनाने के लिए यह सुनिश्चित करें कि उनके ग्राहक अपना मोबाइल फोन नंबर उनके पास रजिस्टर करायें ताकि उन्हें अलर्ट किया जा सके ।

10. धोखाधड़ी करने वालों का तकनीकी ज्ञान न केवल काफी अच्छा होता है बल्कि वे बैंकों में प्रचलित प्रणालियों और क्रियाविधियों की स्पष्ट जानकारी रखते हैं । कोयंबटूर में ऐसी घटनाओं की रिपोर्ट की गयी है, जहाँ पीओएस टर्मिनल केवाईसी अपेक्षाओं का अनुपालन करने के बाद स्थापित किये गये थे और इन टर्मिनलों में लेन देन के लिए धोखाधड़ी करने वालों द्वारा चुराये गये कार्डों का उपयोग किया गया । (मेरा मानना है कि धोखाधड़ी करने वालों ने अंतरराष्ट्रीय स्तर पर परिचालित ऑनलाइन ई-भुगतान योजना के माध्यम से खरीदे गये कार्डों से चुराये गये ब्यौरों का उपयोग ऐसी जानकारी प्राप्त करने के लिए किया ।)

11. हैदराबाद में धोखाधड़ी करने वालों ने व्यापारी का ढोंग रचते हुए केवल 50 रुपये का भुगतान किये जाने पर 250 रुपये के टॉकटाइम वाला बॉस्किन रॉबिन्स /मोबाइल रिचार्ज वाउचर देने का प्रस्ताव किया जिसमें शर्त यह थी कि इसके लिए केवल डेबिट कार्ड स्वीकार किये जाते । इसके लिए उपयोग की जाने वाली कियोस्क मशीन को इस प्रकार से बनाया गया था कि वह पिन बता देती और एक चार्ज स्लिप को प्रिंट कर देती जिसमें बताया गया होता कि बैक द्वारा लेन देन का अनुमोदन कर दिया गया है । मैग्नेटिक स्ट्राइप कार्ड डाटा और पिन का प्रग्रहण असंदेही ग्राहकों से कर लिया जाता और बाद में उनका उपयोग नकदी निकालने के लिए जाली कार्ड बनाने में किया जाता । इसकी प्रतिक्रिया में ग्राहकों का विशिष्ट जवाब यह होता कि 'लेकिन यह तो बैंकों का प्राथमिक दायित्व होता है कि वे मेरे धन की सुरक्षा सुनिश्चित करें । यह दायित्व वे ग्राहकों पर नहीं छोड़ सकते हैं' । इसी तरह की कार्यप्रणाली राँची के एक पेट्रोल पंप पर अपनायी गयी; केवल इस बार मोबाइल रिचार्ज वाउचर के बदले ग्राहकों को एक कार वाश लिक्विड और एयर फ्रेशनर दिये गये थे । बैंकों का यह तर्क हो सकता है कि इसमें उनकी प्रणाली की सुरक्षा में कोई भंग नहीं हुआ था और ये सब ग्रहकों के लालच से प्रेरित थे । इस तथ्य को स्वीकार करते हुए इन घटनाओं का उल्लेख करने का मेरा उद्देश्य इस बात पर प्रकाश डालना है कि ग्राहकों को लगातार शिक्षित किया जाना जरूरी है । जबकि बैंकों द्वारा ग्राहकों को अधिक से अधिक इलेक्ट्रॉनिक तरीके से भुगतान के प्रति प्रोत्साहित किया जा रहा है, इस तथ्य को महसूस करना आवश्यक है कि उन्होंने जिस प्रणाली को स्थापित किया है वह कितनी भी तगड़ी और सुरक्षित क्यों न हो, अंत में ग्राहकों का बोध सर्वोपरि होता है ।

12. यह उल्लेख करना असंगत नहीं होगा कि भारतीय रिज़र्व बैंक ने हाल ही में पूरे देश में विभिन्न एटीएम पर दी जाने वाली ग्राहक सेवा का सर्वेक्षण कराया था । जबकि राष्ट्रीय स्तर पर एटीएम के उपयोग से संतुष्टि 1-10 के पैमाने पर 7 पायी गयी, यह उत्तर प्रदेश, गुजरात और चंडीगढ़ जैसे राज्यों में राष्ट्रीय औसत से काफी कम थी । तथापि,

इस सर्वेक्षण से यह प्रकट हुआ कि शिकायत निवारण तंत्र में सुधार की गुंजाइश है । 52 प्रतिशत से अधिक उत्तर दाताओं ने यह रिपोर्ट की कि उनकी शिकायतों का समाधान करने में लगभग दो सप्ताह या उससे अधिक समय लगा । लेकिन बेचैन करने वाली बात यह है कि 43 प्रतिशत से अधिक मामलों में शिकायत के उचित समाधान के बारे में बैंकों का उत्तर यह था कि 'वे आरबीआई के दिशा-निर्देशों का पालन कर रहे हैं' । मैं सोचता हूँ कि यह आवश्यक है कि ग्राहकों से संपर्क रखने वाले कार्मिकों को अधिक स्पष्टता से ग्राहकों का मार्गदर्शन करने के लिए पर्याप्त प्रशिक्षण दिया जाये ।

13. जबकि सम्मेलन में सुरक्षित बैंकिंग के ऊपर ध्यान केंद्रित किया गया है, यह सुनिश्चित करना पर्याप्त नहीं है कि सभी प्रकार के बैंकिंग लेन देन विधिवत प्राधिकृत हों और ग्राहकों के हितों की रक्षा हो । बैंकों के लिए इस बात को महसूस करना महत्वपूर्ण है कि उनकी भूमिका और दायित्व यह सुनिश्चित करने में है कि युक्तियुक्त जोखिम प्रबंधन उपाय किये गये हैं, विशेष रूप से धनशोधन और आतंकियों को वित्तपोषित करने से संबंधित मुद्दों पर ध्यान देने के लिए । मुझे स्मरण है कि एक वर्ष या उससे पहले हमने जाँच करने पर यह पाया था कि समुद्रपार जारी किये गये लगभग 3-4 कार्डों का व्यापक उपयोग एक बैंक के एटीएम में किया गया था, और तीन महीनों की छोटी अवधि में 200 करोड़ रुपये से अधिक की राशि आहरित की गयी थी । स्पष्टतः जिस किसी ने भी कार्ड का उपयोग किया वह कोई पर्यटक नहीं होगा जो खरीदारी के लिए निकला हो । जब यह बात बैंक के ध्यान में लायी गयी, तब उन्होंने स्वीकार किया कि जोखिम समाप्ति के उचित उपायों का सहारा ले कर इन लेन देनों की पहचान की जा सकती थी और उपचारात्मक कार्रवाई आरंभ की जा सकती थी । इस संबंध में रिज़र्व बैंक में हमने यह भी देखा कि समुद्रपार का एक बैंक पूर्वदत्त कार्ड प्रदान करता था जिन्हें भारत में कुरियर द्वारा सुपुर्द किया जाता था । जबकि हमें समुद्रपार अपने ग्राहक को जानिये (केवाईसी) पहलुओं के बारे में कुछ भी पता नहीं था, भारत में नकदी के आहरण के लिए किसी भी एटीएम में इन कार्डों का उपयोग किया जा सकता था । ऐसी प्रणाली का निहितार्थ हमारे देश के लिए क्या है इसकी कल्पना करना कठिन नहीं है । जबकि रिज़र्व बैंक ने भारत में इन कार्डों के उपयोग को रोकने के लिए हस्तक्षेप किया है, बैंकों के लिए यह महत्वपूर्ण है कि वे इस प्रकार की घटनाओं के लिए सतर्क रहें और यदि आवश्यक हो तो युक्तियुक्त अधिकारियों को सावधान कर दें ।

14. चिंता का जो अन्य क्षेत्र उभर कर सामने आया है उसका संबंध धोखाधड़ी करने वालों से है जो असंदेही ग्राहकों को ई-मेल में लिंक के माध्यम से ऐसे किसी वेबसाइट की ओर निदेशित करते हैं जो किसी प्रामाणिक संस्था का लगता है । यह तब भी हुआ है जब आम लोगों द्वारा ऐसे मेल प्राप्त किये गये कि उनके नाम एक बड़ी धनराशि प्राप्त हुई है और भारतीय रिज़र्व बैंक में रखी हुई है । उन्हें एक लिंक बताया गया जो रिज़र्व बैंक वेबसाइट का छद्म रूप लगता था और उन्हों कहा गया कि वे अपने खातों के ब्यौरे दें । जबकि रिज़र्व बैंक ने आम जनता को मीडिया में विज्ञापनों के जरिए सावधान किया है, बैंकों को भी इस पर नजर रखने की आवश्यकता है । लेकिन एक महत्वपूर्ण सवाल जिसका जवाब चाहिए, यह है कि इनमें से अनेक मामलों में असंदेही लोगों द्वारा धन बैंक खातों में दिये गये हैं, जहाँ से उन्हें निकाल लिया गया है । पहली बात तो यह है कि ये खाते किस प्रकार खोले गये ? क्या बैंक केवाईसी अपेक्षाओं का पालन नहीं करते हैं ? क्या एक बार जब मशीनें वे काम करने लगी हैं जो पहले हाथ से किये जाते थे तब निगरानी तंत्र अधिकाधिक निस्तेज होता गया है ?

15. अन्य चुनौती जिसका सामना उद्योग द्वारा किया जा रहा है, वह है अन्य पक्ष वेंडरों द्वारा सिस्टम, डाटा और और प्रक्रियाओं का प्रबंध किया जाना, जो आज एक आवश्यकता बन चुका है और इन वेंडरों / सेवाप्रदाताओं के कार्यों पर कारगर नियंत्रण रखने की आवश्यकता है। यह आंतरिक आशंकाओं के अतिरिक्त है, क्योंकि अक्सर कंप्यूटर-अपराधी उसी संगठन के कर्मचारी होते हैं । अतः बाहरी आशंकाओं से अवगत होते हुए भी बैंकों के सामने नयी आशंका उपस्थित है वह है स्थिर डाटा से संबंधित आंतरिक उल्लंघनों की है। आज-कल के कर्मचारी आसानी से संवेदनशील फाइलों और सूचनाओं को ई-मेल, एफटीपी द्वारा आसानी से या आँकड़ों को पोर्टेबल मीडिया में कॉपी करके बाहर भेज सकते हैं । बैंकों को उन स्थानों पर नियंत्रण रखना होगा जहाँ उनकी संवेदनशील सूचना रखी जाती है, किस प्रकार इसका उपयोग किया जाता है और इसे कौन प्राप्त करता है । (उदाहरणार्थ, सिटी एकाउंट ऑनलाइन, हुंडई कैपिटल और सोनी में ग्राहक संबंधी डाटा की चोरी हुई) ।

16. बैंकिंग उद्योग सुरक्षा के प्रति चुनौतियों के बारे में सजग रहा है और इस संदर्भ में सभी पणधारियों यथा, सरकार, विनियामक, बैंक और प्रौद्योगिकी प्रदाताओं द्वारा प्रशंसनीय प्रयास किये जा रहे हैं । जैसाकि आप जानते हैं, रिज़र्व बैंक द्वारा जी.गोपालकृष्ण, कार्यपालक निदेशक, भारतीय रिज़र्व बैंक, की अध्यक्षता में एक कार्यदल सूचना-सुरक्षा, इलेक्ट्रॉनिक बैंकिंग, प्रौद्योगिकी जोखिम प्रबंधन और साइबर धोखाधड़ी के संबंध में गठित किया गया था जो आइटी नियंत्रण, सूचना-सुरक्षा, आइटी परिचालन, सूचना प्रणाली लेखापरीक्षा, साइबर धोखाधड़ी, व्यवसाय सातत्य आयोजना, ग्राहक शिक्षा और आइटी उपयोग से उत्पन्न विविध मुद्दों से संबंधित क्षेत्र में विस्तृत सुझाव देता है ।

17. इस दल ने सिफारिश की है कि आवश्यकता को बैंकों द्वारा किये गये कार्यकलाप के स्वरूप और क्षेत्र तथा बैंक में प्रचलित प्रौद्योगिकी वातावरण एवं व्यवसाय प्रक्रियाओं को प्रौद्योगिकी द्वारा दिये गये सहयोग पर आधारित होना चाहिए । प्रमुख सिफारिशों का संबंध आइटी नियंत्रण, आइटी परिचालन, साइबर धोखाधड़ी, व्यवसाय सातत्य योजना, ग्राहक शिक्षा और विधिक मुद्दों से है ।

18. दल ने इन नीतियों की सिफारिश की है जो ऊपर उद्धृत क्षेत्रों में अपनायी जानी चाहिए और बैंकों द्वारा सर्वोत्तम व्यवहारों को अपनाया जाना चाहिए ताकि प्रौद्योगिकी का इष्टतम लाभ सुरक्षित ढंग से प्राप्त किया जा सके । जबकि इन सिफारिशों को कार्यान्वित किये जाने की जाँच-पड़ताल आइबीए द्वारा गठित एक कार्यदल द्वारा की जा रही है, बैंक इन सिफारिशों की तुलना में अपनी स्थिति का स्व-मूल्यांकन करके अच्छी कोशिश कर सकते हैं और युक्तियुक्त उपाय आरंभ कर सकते हैं ।

19. अपने उपर्युक्त कथन में मैं यह भी जोड़ना चाहता हूँ कि इस वातावरण में वास्तविक चुनौती केवल अतिरिक्त प्रौद्योगिकी समाधान देने और अधिकाधिक जटिल सुरक्षा संस्तरों को प्रदान करने से कहीं अधिक होती है और इसका रूपांतरण सुरक्षित बैंकिंग सेवा प्रदान करते हुए उसे ग्राहक सुविधा संबंधी जरूरतों में संतुलन स्थापित करने में होता है जो विनियामकों और सुरक्षा को क्रियान्वित करने वालों को दुविधाग्रस्त करता है । मैं इनमें से कुछ दुविधाओं को नीचे गिनाता हूँ :

- लेन देनों को सुरक्षित रखने के लिए वन-टाइम पासवर्ड /टू फैक्टर प्रमाणन एक तरीका होता है । तथापि, ग्राहक के रजिस्टर्ड मोबाइल पर ऐसी ओटीपी भेजे जाने की अनिवार्य अपेक्षा से अनेक मुद्दे /असुविधाएँ उत्पन्न होती हैं जिनका कारण कुछ कारक होते हैं यथा, नेटवर्क का उपलब्ध न होना, किसी खास फोन नंबर पर प्रतिबंध, उस समय सेवा का उपलब्ध नहीं होना, जब ग्राहक विदेश की यात्रा पर हो, ओटीसी संचरण की धीमी गति के चलते ऑनलाइन लेन देनों का टाइम-आउट हो जाना, आदि । ग्राहक के लिए इसका लागत संबंधी निहितार्थ होता है क्योंकि उसे अंतरराष्ट्रीय आँकड़ा संचरण प्रशुल्क पर प्रभारों का भुगतान करना पड़ता है ।
- लॉग-इन पासवर्ड, ट्रैंजेक्शन पासवर्ड के जरिए बहुस्तरीय सुरक्षा और कुछ गोपनीय डाटा पुष्टीकरण लेन देनों को बेहतर ढंग से सुरक्षित रखा जा सकता है । लेकिन इसमें ऐसे मुद्दे होते हैं, यथा बहुविध पासवर्डों, स्लोगनों, चित्रों, प्रश्नों के उत्तर, आदि को याद रखना और कुछ लेन देन इन समस्याओं के कारण अवरुद्ध हो जाते हैं और यहाँ तक कि कभी-कभी ऑनलाइन पहुँच भी अवरुद्ध हो जाती है । इसके साथ जुड़ी समस्याएँ हैं पहुँच रि-ऐक्टिवेशन में लगने वाला समय, पासवर्ड जेनरेशन आदि, जो कभी-कभी लंबी/समय-साध्य प्रक्रिया होती है और इससे ग्राहक को झुँझलाहट और असुविधा होती है ।
- मोबाइल बैंकिंग में, लेन देन की राशि की सीमा को तय करने की, जहाँ तक अनइन्क्रिप्टेड डाटा को भुगतान /निधि अंतरण के लिए भेजा जा सकता है, चुनौती होती है । यदि सीमाओं को अत्यधिक कठोर बनाया जाता है तो उसका लागत और दक्षता संबंधी निहितार्थ हो सकता है जबकि इन्हें अधिक शिथिल किये जाने से सूचना के चोरी हो जाने की जोखिम हो सकती है ।
- निगरानी कैमरे एटीएम लेन देनों को अधिक सुरक्षित बनाने में मदद करते हैं लेकिन इसमें गोपनीयता के मुद्दे उठते हैं और इसके अतिरिक्त ग्राहक को इससे असुविधा होती है ।

20. समग्रतः देखा जाये तो जबकि सुरक्षा के प्रति चुनौतियाँ दुःसाध्य हैं और दिन-ब-दिन बढ़ती जाती हैं, आशंकाओं के बीच अस्तित्व बचाये रखना अधिक महत्वपूर्ण होता है । इसमें संसाधन - मानवीय और मौद्रिक - मनोवृत्ति एवं अभिरुचि, शामिल होते हैं । कार्ड नॉट प्रेजेंट लेन देनों को उचित रूप से सुरक्षित कर लेने के बाद रिज़र्व बैंक ने कार्ड प्रेजेंट लेन देनों की सुरक्षा बढ़ाने के उपाय खोजने आरंभ कर दिये हैं । यदि हम यह मान लें रिकार्डों के साथ छेड़-छाड़ न केवल एटीएम में हो सकती है बल्कि आधा मिलियन और उससे भी बड़ी संख्या में पीओएस टर्मिनलों में की जा सकती है तो यह काम अत्यंत कठिन हो जाता है । इससे यह सवाल खड़ा हो सकता है कि कि क्या चिप-आधारित कार्ड-प्रणाली की ओर जाना स्किमिंग और क्लोनिंग की जोखिम के विरुद्ध एकमात्र समाधान हो सकता है ? अथवा क्या इससे कम खर्चीला विकल्प यथा, सभी कार्ड प्रेजेंट लेन देनों के लिए सेकंड फैक्टर ऑथेंटिकेशन है ? क्या 2एफए को स्थिर या गतिशील होना चाहिए ? इससे किस प्रकार मदद मिलती है, यदि स्थिर 2एफए के साथ छेड़-छाड़ की जाती है ? क्या एक गतिशील ओटीपी व्यापारिक परिचालनों को प्रभावित किये बिना और ग्राहकों को असुविधा पहुँचाये बिना वास्तव में कार्य करता है ? जैसाकि आप जानते होंगे, भारतीय रिज़र्व बैंक ने इन मुद्दों पर ध्यान देने के लिए एक कार्यदल का गठन किया था । इस दल की रिपोर्ट, जिसे सार्वजनिक पहुँच के लिए जारी किया गया था, को अब संसाधित किया जा रहा है । दल ने यह नोट किया है कि आधार बायोमेट्रिक डाटा सेकंड फैक्टर ऑफ ऑथेंटिकेशन के रूप में मैग्नेटिक स्ट्राइप कार्डों के लिए भी कार्य करेगा जिससे इएमवी चिप और पिन कार्ड पर स्विच लगाने की आवश्यकता नहीं होगी जिसका लागत संबंधी

निहितार्थ इस उद्योग के लिए होता है । दल ने यह सिफारिश की है कि इएमवी चिप कार्ड की ओर अभियान पर 18 महीनों बाद विचार किया जा सकता है जो आधार की प्रगति पर निर्भर होगा । जबकि रिपोर्ट का संसाधन भारतीय रिज़र्व बैंक द्वारा किया जा रहा है, हम एक सुरक्षित 2एफए का लक्ष्य सभी कार्ड प्रेजेंट लेन देनों के लिए रखते हैं जिसमें हमने इस प्रयोजन के लिए नियोजित की जाने वाली प्रौद्योगिकी के बारे में कोई आदेश नहीं दिया है ।

21. उद्योग द्वारा नवोन्मेषी सोच और रचनात्मक समाधान, ग्राहक जागरूकता बढ़ाये जाने पर ध्यान केंद्रित करना जिसके साथ सुरक्षा-जोखिम शमन के लिए उपयुक्त प्रौद्योगिकी में अपेक्षित निवेश जुड़ा है, युक्तियुक्त ग्राहक सुविधा के साथ बैंकिंग सुरक्षा के इष्टतम स्तर को सुनिश्चित करने के लिए अनिवार्य है ।

22. सुरक्षित और सुविधाजनक ऑनलाइन बैंकिंग सेवा प्रदान करने के आपके प्रयास में रिज़र्व बैंक आपके साथ है ।