चर्चा पत्र

धोखाधड़ी रोकने के लिए डिजिटल भुगतान में सुरक्षा उपायों का अन्वेषण

भुगतान और निपटान प्रणाली विभाग

भारतीय रिजर्व बैंक

I. पृष्ठभूमि

पिछले दशक में, भारत में डिजिटल भुगतान अभूतपूर्व गति से बढ़े हैं, जो व्यक्तियों और व्यवसायों द्वारा वित्तीय लेनदेन करने के तरीके में संरचनात्मक परिवर्तन को दर्शाते हैं। डिजिटल लेनदेन की मात्रा में 38 गुना वृद्धि हुई है, जबकि लेनदेन के मूल्य में तीन गुना से अधिक वृद्धि हुई है। इस अवधि के दौरान डिजिटल भुगतान की चक्रवृद्धि वार्षिक वृद्धि दर (सीएजीआर) क्रमशः मात्रा और मूल्य के मामले में लगभग 53% और 13% है।

ii. उपरोक्त वृद्धि को क्रेडिट और डेबिट कार्ड, यूनिफाइड पेमेंट्स इंटरफेस (यूपीआई), इमीडिएट पेमेंट सर्विस (आईएमपीएस), नेशनल इलेक्ट्रॉनिक फंड्स ट्रांसफर (एनईएफटी), रियल टाइम ग्रॉस सेटलमेंट (आरटीजीएस), मोबाइल वॉलेट और नेट बैंकिंग से बने विविध और अंतरसंचालनीय भुगतान पारिस्थितिकी तंत्र द्वारा समर्थित किया गया है। मज़बूत सिक्योरिटी आर्किटेक्चर—जिसमें अनिवार्य अतिरिक्त प्रमाणीकरण कारक (एफए),लाभार्थी के नाम की जाँच की सुविधाएँ और ट्रांज़ैक्शन कंट्रोल शामिल हैं, इसके साथ-साथ तेज निपटान चक्र ने यूज़र का भरोसा बढ़ाया है और बिना किसी रुकावट के डिजिटल इस्तेमाल को बढ़ावा दिया है।

iii. हालांकि, डिजिटल भुगतानों की क्षमता धोखाधड़ी से संबंधित शिकायतों से बाधित होती है। डिजिटल भुगतानों के माध्यम से एक सामान्य धोखाधड़ी में प्रणालियों का तकनीकी समझौता शामिल नहीं होता है, बल्कि अधिकांशतः सामाजिक इंजीनियरिंग, बलपूर्वक दबाव या अन्य व्यक्ति के रूप में बनकर कार्य करने के माध्यम से उपयोगकर्ताओं को धोखा देकर किया जाता है। धोखे में आकर, पीड़ित खुद ही ट्रांज़ैक्शन शुरू करते हैं और प्रमाणीकृत करते हैं, जिससे 'अधिकृत' पुश-भुगतान (एपीपी) धोखाधड़ी होती है। एनईएफटी,आरटीजीएस,यूपीआई और आईएमपीएस जैसी प्रणालियों के माध्यम से भुगतानों की तात्कालिक प्रकृति के कारण, समय पर हस्तक्षेप और धन की वसूली का अवसर सीमित हो जाता है।

II. डिजिटल भुगतान को सुरक्षित करने के लिए विनियामक उपाय

iv. पिछले कुछ वर्षों से, रिजर्व बैंक ने डिजिटल भुगतान की सुरक्षा और आघात सहनीयता को मजबूत करने के लिए कई उपाय शुरू किए हैं। डिजिटल भुगतान लेनदेन में दो-कारक प्रमाणीकरण अनिवार्य किया गया था। भुगतान श्रृंखला में किसी भी संस्था द्वारा वास्तविक कार्ड डेटा के भंडारण को कार्ड जारीकर्ता के अलावा अन्य सभी एजेंटों से प्रतिबंधित करने के लिए डिवाइस टोकनाइजेशन (2019) और कार्ड-ऑन-फाइल टोकनाइजेशन (2021) के माध्यम से कार्रवाई की गई थी। कार्ड में ग्राहक द्वारा नियंत्रण को 2020 में अनिवार्य किया गया था, जिससे कार्डधारकों को अपनी ओर से सभी प्रकार के लेनदेन — देशी और अंतरराष्ट्रीय, पीओएस/ ऑनलाइन लेनदेन/ संपर्क रहित लेनदेन

आदि — के लिए स्विच ऑन/ऑफ और लेनदेन सीमा सेट/ संशोधित(यदि कार्ड जारीकर्ता द्वारा सेट किया गया कुल कार्ड सीमा है, तो उसके भीतर) करने की शक्ति मिली।

v. बैंकों (2021) और गैर-बैंक पीएसओ (2024) के लिए डिजिटल भुगतान प्रणाली नियंत्रण संबंधी निर्देश जारी किए गए थे, जिनमें सूचना प्रणालियों और साइबर सुरक्षा जोखिमों की पहचान, मूल्यांकन, निगरानी और प्रबंधन के लिए शासन तंत्र, साथ ही डिजिटल भुगतान लेनदेन के लिए सुरक्षित और संरक्षित प्रणाली सुनिश्चित करने के लिए आधारभूत सुरक्षा उपाय शामिल हैं। 2025 में, बैंक ने नए प्रमाणीकरण कारकों के परिचय को प्रोत्साहित करने के लिए तकनीकी विकास का लाभ उठाने और जारीकर्ताओं को धोखाधड़ी जोखिम धारणा के आधार पर न्यूनतम दो-कारक प्रमाणीकरण से अतिरिक्त जोखिम-आधारित जांच अपनाने की अनुमति देने के लिए एक सिद्धांत-आधारित डिजिटल भुगतान लेनदेन के प्रमाणीकरण के लिए ढांचा जारी किया।

vi. जैसा कि 2016 में जारी निर्देशों में उल्लेख किया गया है, ग्राहक की देयता अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन के मामले में सीमित है।

vii. आरबीआई ने विभिन्न प्रणाली भागीदारों को दिशानिर्देश भी जारी किए हैं ताकि वे दूरसंचार विभाग (डीओटी) द्वारा विकसित डिजिटल इंटेलिजेंस प्लेटफॉर्म (डीआईपी) पर उपलब्ध मोबाइल नंबर रिवोकेशन लिस्ट (एमएनआरएल) का उपयोग कर सकें, ताकि अपने ग्राहक डेटाबेस की निगरानी और शुध्दि की जा सके। भारतीय दूरसंचार नियामक प्राधिकरण (टीआरएआई) ने लेनदेन या सेवा-संबंधी प्रावधानों के बारे में ग्राहकों को कॉल करने के लिए '1600xx' श्रृंखला से शुरू होने वाले फोन नंबरों का उपयोग करने के लिए दिशानिर्देश जारी किए हैं। इसके अलावा, कोई भी विपणन या प्रचार विज्ञापन कॉल '1400xx' श्रृंखला के नंबरों से की जानी चाहिए। ये उपाय उपभोक्ताओं को वैध कॉल और धोखेबाजों द्वारा किए गए संभावित धोखा प्रयासों के बीच अंतर करने में मदद करने के लिए हैं।

viii. भारतीय साइबर अपराध समन्वय केंद्र (I4सी) ने राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (एनसीआरपी) पर दर्ज शिकायतों के साथ निपटने के लिए मानक परिचालन प्रक्रिया जारी की है।

ix. 2024 में, रिजर्व बैंक की पूर्ण स्वामित्व वाली सहायक कंपनी - रिजर्व बैंक इनोवेशन हब (आरबीआईएच) ने बैंकों द्वारा मूल बैंक खातों का त्वरित और प्रभावी पता लगाने के लिए म्यूलहंटर.एआई बनाया है। रिजर्व बैंक वर्तमान में आरबीआईएच के साथ मिलकर एआई/एमएल जैसी उन्नत तकनीकों का उपयोग करके भुगतान धोखाधड़ी जोखिमों को कम करने के लिए डिजिटल भुगतान बुद्धिमत्ता प्लेटफॉर्म (डीपीआईपी) के प्रोटोटाइप की स्थापना करने पर काम कर रहा है। प्रेषक बैंक के लिए, प्लेटफॉर्म का उद्देश्य वास्तविक

समय में, लेनदेन के अनुसार, लाभार्थी के प्रोफाइल के बारे में जानकारी प्रदान करना है, भले ही लेनदेन को अभी तक निष्पादित नहीं किया गया हो।

III. आगे की कार्रवाई की गुंजाइश

x. आरबीआई के मार्गदर्शन में बैंकों द्वारा उठाए गए दृढ कदमों की वजह से, 'अकाउंट टेक-ओवर' से जुड़े फ्रॉड अब न के बराबर रह गए हैं। अब ज़्यादातर फ्रॉड 'ऑथराइज़्ड पुश पेमेंट्स' (एपीपी) से जुड़े होते हैं। ये फ्रॉड ऐसे माहौल में पनपते हैं जहाँ भुगतान करना बहुत आसान और बिना किसी रुकावट के होता है; ऐसे में ग्राहक (जो इन फ्रॉड के शिकार बनते हैं) बहुत कम मेहनत से ही तुरंत पैसे हस्तांतरण कर देते हैं, और उन्हें इस बात का एहसास तब होता है जब वे ठगे जा चुके होते हैं।

xi. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (एनसीआरपी) के आंकड़ों से पता चलता है कि डिजिटल भुगतान से संबंधित धोखाधड़ी बढ़ रही है। नीचे दिए गए आंकड़ों से यह देखा जा सकता है:

वर्ष	रिपोर्ट की गई धोखाधड़ी की संख्या	धोखाधड़ी का मूल्य (₹ करोड़ में)
2021	2.6 लाख	551
2022	6.9 लाख	2,290
2023	13.1 लाख	7,465
2024	24 लाख	22,848
2025	28 लाख	22,931

धोखेबाज नकली कॉल सेंटर, डीपफेक-चालित अनुकरण धोखे और मूल खाता नेटवर्क जैसे विभिन्न तरीकों का उपयोग कर रहे हैं। समाज के लगभग सभी वर्ग, विशेष रूप से बुज़ुर्गों जैसे कमज़ोर समूह, ऐसे एपीपी धोखाधड़ी का शिकार बन गए हैं। इसलिए, इन मुद्दों को संबोधित करने के लिए प्रणालियों और प्रक्रियाओं को लागू करने की तत्काल आवश्यकता है। यह चर्चा पत्र हितधारकों से अतिरिक्त सुरक्षा उपायों को लागू करने की आवश्यकता पर दृष्टिकोण मांगता है।

xii. चर्चा पत्र निम्नलिखित चार विकल्पों को रखता है, अर्थात्,

1) निम्न मूल्य के अलावा अधिकृत पुश भुगतान के लिए विलंबित क्रेडिट;

2) समाज के कमजोर वर्गों द्वारा उच्च मूल्य के डिजिटल लेनदेन के लिए विश्वसनीय व्यक्ति द्वारा अतिरिक्त प्रमाणीकरण.

3) केवल उन खातों को बड़े क्रेडिट प्राप्त करने की अनुमति दी जाएगी जिनकी अतिरिक्त समीक्षा संतोषजनक हो;

4) ग्राहक-प्रेरित नियंत्रण

इन विकल्पों का उद्देश्य व्यापक लक्ष्यों को प्राप्त करना है, जैसे: डिजिटल भुगतानों की चुनिंदा श्रेणियों में विलंब लाना (प्रक्रिया-स्तर पर बदलाव या अतिरिक्त 'ड्यू डिलिजेंस' आवश्यकताओं के माध्यम से)—जिससे ग्राहकों और पीएसओ, दोनों को ही धोखाधड़ी वाले लेन-देनों को होने से रोकने या उनसे प्राप्त राशि को तेज़ी से हस्तांतरित होने से रोकने के लिए पर्याप्त समय मिल सके; और, ग्राहकों को उनकी ज़रूरत के अनुसार तैयार किए गए नियंत्रण उपलब्ध कराकर उन्हें सशक्त बनाना।

हर विकल्प के बारे में आगे आने वाले खण्ड में विस्तार से बताया गया है, साथ ही उन खास सवालों का भी ज़िक्र है जिन पर स्टेकहोल्डर्स से राय मांगी जा रही है। स्टेकहोल्डर्स से अनुरोध है कि वे हर विकल्प की उपयोगिता और व्यावहारिकता पर अपनी राय दें—चाहे वह विकल्प अपने आप में हो या फिर दूसरे संभावित तरीकों के साथ मिलाकर—और ऐसा करते समय उन उपायों को भी ध्यान में रखें जो पहले से लागू हैं या जिन पर काम चल रहा है।

विकल्प 1: अधिकृत पुश भुगतान के लिए विलंबित क्रेडिट

व्यापारियों को इलेक्ट्रॉनिक भुगतान आमतौर पर बैंकों और भुगतान एग्रीग्रेटर (पीए) द्वारा व्यापारियों की आवश्यक देखरेख के बाद सक्षम किए जाते हैं। ऐसे मामलों में, भुगतान नेटवर्क आमतौर पर विवाद समाधान ढांचे के हिस्से के रूप में चार्जबैक तंत्र प्रदान करते हैं। खाते से खाते हस्तांतरण के मामले में कोई तुलनीय सुरक्षा उपाय नहीं है। इसलिए, व्यक्ति के बैंक खाते या एकल स्वामित्व या साझेदारी फर्म के खाते में कुछ एपीपी हस्तांतरण के लिए एक समय विलंब शामिल करना, दोनों भुगतानकर्ता और भुगतान प्राप्तकर्ता के अंत में, एक प्रभावी धोखाधड़ी-निवारण उपाय के रूप में कार्य कर सकता है।

1.1 अंतरराष्ट्रीय अनुभव:

1) **यूनाइटेड किंगडम (यूके):** यूके ने एक औपचारिक तंत्र (भुगतान सेवाएं (संशोधन) विनियम 2024 के माध्यम से) शुरू किया है जो संदिग्ध धोखाधड़ी मामलों में आउटबाउंड खाते-से-खाते भुगतानों को देरी करने की अनुमति देता है। इस ढांचे के तहत, भुगतान सेवा प्रदाता (पीएसपी) एक आउटबाउंड भुगतान को 72 घंटे (लगभग तीन कार्य दिवस) तक रोक सकते हैं यदि भुगतान निर्देश धोखे या बेईमानी से प्रेरित होने के संशय के लिए उचित कारण हैं। इस देरी अवधि के दौरान, धन भुगतानकर्ता के खाते में जमा रहता है, और पीएसपी को भुगतानकर्ता को सूचित करना चाहिए और कारण स्पष्ट करना चाहिए। पीएसपी इस समय का उपयोग लाभार्थी के बैंक या कानून प्रवर्तन से संपर्क करने के लिए भी कर सकते हैं।

2) **सिंगापुर:** सिंगापुर ने एक ऐसा निवारक तरीका अपनाया है जो 'कूलिंग-ऑफ पीरियड' और 'डायनामिक ट्रांज़ैक्शन सेफ़गार्ड' पर आधारित है। सिंगापुर की मॉनेटरी अथॉरिटी (एमएएस) और एसोसिएशन ऑफ़ बैंक्स इन सिंगापुर द्वारा शुरू किए गए 'एन्हांस्ड एंटी-स्कैम फ्रेमवर्क' (ईएएसएफ) और 'शेयर्ड रिस्पॉन्सिबिलिटी फ्रेमवर्क' (एसआरएफ) के तहत, बैंकों को कुछ खास तरह के ज़्यादा जोखिम वाले काम करने पर ग्राहक के लिए कम से कम 12 घंटे का 'कूलिंग-ऑफ पीरियड' लागू करना ज़रूरी है – उदाहरण के लिए, किसी नए डिवाइस पर डिजिटल बैंकिंग शुरू करना, खाते की ज़रूरी जानकारी (क्रेडेंशियल्स) को रीसेट करना, या किसी नए व्यक्ति को पहली बार पैसे भेजना। इस दौरान, उस खाते से बाहर जाने वाले लेनदेन को रोका या सीमित किया जा सकता है, जिससे किसी भी अनाधिकृत पहुँच या धोखाधड़ी की कोशिशों का पता लगाने और उन्हें रोकने का समय मिल जाता है।

3) **स्वीडन:** मई 2024 में, स्वीडिश बैंकर्स एसोसिएशन ने धोखाधड़ी से निपटने के लिए एक समन्वित पैकेज की घोषणा की। इसमें 'कूलिंग-ऑफ पीरियड' (सोचने-समझने का समय) जोड़ना, नए प्राप्तकर्ताओं के लिए अतिरिक्त पुष्टि के चरण और असामान्य रूप से

बड़े या अलग तरह के लेन-देन पर सीमाएँ तय करना शामिल था। इन विशिष्ट उपायों को लागू करने का तरीका, बैंक की अपनी विशेष परिस्थितियों के आधार पर, अलग-अलग बैंकों पर छोड़ दिया गया था।

1.2 संभावित दृष्टिकोण:

भुगतान करने वाले के छोर पर थोड़ा विलंब रखना महत्वपूर्ण है, क्योंकि यही वह चरण है जहाँ फंड हस्तांतरण करने का निर्णय लिया जाता है और जहाँ सोशल-इंजीनियरिंग की तरकीबें इस्तेमाल की जाती हैं। डेबिट के निष्पादन से पहले थोड़ी देर का विलंब एक निवारक नियंत्रण के रूप में काम कर सकता है; यह धोखेबाज़ के पीड़ित पर पड़ने वाले मनोवैज्ञानिक प्रभाव को बाधित करता है और भुगतान करने वाले को लेन-देन पर पुनर्विचार करने का अवसर देता है।

यह सुनिश्चित करने के लिए कि कम मूल्य वाले लेन-देन बिना किसी रुकावट के चलते रहें, ऐसे 'लैग मैकेनिज्म' (विलंब तंत्र) को केवल एक तय सीमा से ऊपर के एपीपी लेन-देन पर ही लागू करने का प्रस्ताव है। प्रति लेन-देन ₹10,000 की सीमा को उचित माना जा सकता है। नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल (एनसीआरपी) के पास उपलब्ध जानकारी के अनुसार, ₹10,000 से अधिक के लेन-देन, रिपोर्ट किए गए धोखाधड़ी के मामलों में संख्या के हिसाब से लगभग 45 प्रतिशत हैं, लेकिन मूल्य के हिसाब से लगभग 98.5 प्रतिशत हैं।

इस तरीके के तहत, जब कोई ग्राहक (जिसमें अकेले मालिक और पार्टनरशिप फ़र्म भी शामिल हैं) ₹10,000 से ज़्यादा का एपीपी हस्तांतरण शुरू करता है, तो एक घंटे का इंतज़ार का समय (lag period) लागू किया जा सकता है। यह इंतज़ार का समय पैसे देने वाले (payer) की तरफ़, पैसे पाने वाले (payee) की तरफ़, या दोनों तरफ़ लागू किया जा सकता है। इसे लागू करने में आसानी के लिहाज़ से, यह सुझाव दिया जाता है कि यह इंतज़ार का समय सिर्फ़ पैसे देने वाले की तरफ़ ही लागू किया जाए। इस दौरान, पैसे देने वाले का बैंक ग्राहक के खाते से अस्थायी रूप से पैसे काट लेगा, और पैसे देने वाले के पास किसी भी कारण से लेन-देन रद्द करने का विकल्प बना रहेगा। प्रस्तावित एक घंटे की समय-सीमा धोखाधड़ी-जोखिम प्रबंधन में "गोल्डन आवर" सिद्धांत के अनुरूप है, जिसके तहत किसी धोखाधड़ी वाले लेन-देन के बाद का शुरुआती समय, पैसों को गलत हाथों में जाने से रोकने के लिए बहुत महत्वपूर्ण होता है। इस दौरान, यदि पैसे देने वाले का बैंक किसी लेन-देन को असामान्य या अलग तरह का पाता है, तो वह पैसे देने वाले से दोबारा पुष्टि मांग सकता है; साथ ही, वह संदेह की प्रकृति के बारे में उचित जानकारी साझा करेगा और पैसे देने वाले को सचेत भी करेगा। यदि पैसे देने वाला, दी गई जानकारी की समीक्षा करने के बाद भी लेन-देन को आगे बढ़ाने का निर्णय लेता है, तो पैसे देने वाले का बैंक उस लेन-देन को पूरा कर देगा।

इसके अलावा, यह मानते हुए कि कुछ लेन-देन समय-संवेदनशील हो सकते हैं, भुगतानकर्ता को यह विकल्प दिया जा सकता है कि वह किसी खास लेन-देन के लिए देरी (lag) को, उसे स्पष्ट रूप से अधिकृत करके—उदाहरण के लिए, व्हाइटलिस्टिंग तंत्र के माध्यम से—नज़रअंदाज़ कर दे। ऐसे मामलों में, देरी को बाईपास किया जा सकता है। व्हाइटलिस्टिंग लेनदेन की अनुमति देने के बजाय या इसके अतिरिक्त, लाभार्थियों को भुगतानकर्ता द्वारा व्हाइटलिस्ट किया जा सकता है। ऐसे व्हाइटलिस्ट किए गए लाभार्थियों को भुगतान विलंब के अधीन नहीं होंगे।

फायदे और नुकसान:

फायदे:

(i) धोखेबाज आमतौर पर पीड़ित पर लगातार मनोवैज्ञानिक दबाव बनाकर उसे तत्कालता का एहसास दिलाते हैं ताकि वह विचार-विमर्श न कर सके। भुगतानकर्ता के अंत में देरी शामिल करने से धोखेबाज का मनोवैज्ञानिक नियंत्रण टूट जाता है।

(ii) लाभार्थी के अंत में देरी एक अतिरिक्त सुरक्षा परत के रूप में कार्य करती है, भले ही भुगतानकर्ता की ओर से नियंत्रण बाईपास या विफल हो जाए।

(iii) निधियों के संचलन को धीमा करके, यह तंत्र पता लगाने और हस्तक्षेप करने के लिए उपलब्ध समय-सीमा को बढ़ा देता है।

(iv) स्पष्ट और प्रभावी सुरक्षा उपाय उपयोगकर्ताओं को यह भरोसा दिलाते हैं कि भुगतान प्रणाली सुरक्षित है और धोखाधड़ी के जोखिमों के प्रति सजग है। नए उपयोगकर्ताओं को जोड़ने और डिजिटल भुगतान करते समय मौजूदा उपयोगकर्ताओं के बीच विश्वास और भरोसे को बनाए रखने के लिए यह विशेष रूप से महत्वपूर्ण है।

नुकसान:

(i) लैग (lag) को लागू करने के लिए बैंक प्रणालियों और भुगतान प्रणाली के बुनियादी ढांचे में बदलाव की आवश्यकता होगी, जिसमें लेनदेन की कतार (queuing), रद्दीकरण तंत्र आदि शामिल हैं। इन बदलावों में पारिस्थितिकी तंत्र के लिए लागत और प्रयास लगेंगे।

(ii) कुछ लेन-देनों के लिए विलंब (lag) लागू करना, डिजिटल भुगतानों के तात्कालिकता के मूल डिज़ाइन सिद्धांत के साथ विरोधाभासी हो सकता है।

(iii) जो यूज़र्स तुरंत लेन-देन के आदी हैं, उन्हें यह समझना मुश्किल लग सकता है कि कुछ भुगतान में देरी क्यों होती है, जबकि दूसरों में नहीं। इस भ्रम से बचने के लिए, साफ़-साफ़ बातचीत और नियमों का लगातार पालन करना बहुत ज़रूरी होगा।

(iv) चूंकि लेनदेन को व्हाइटलिस्ट करने का विकल्प उपलब्ध होगा, धोखेबाज पीड़ितों को इस सुरक्षा को बाईपास करने के लिए राजी कर सकते हैं, जिससे इसकी प्रभावशीलता कम हो जाएगी।

1.4 संक्षिप्त रूपरेखा:

क्षेत्र	· व्यक्तियों द्वारा किए गए एपीपी लेनदेन (व्यवसाय खातों सहित, जैसे - एकल स्वामित्व, साझेदारी फर्में), नीचे सूचीबद्ध अपवादों को छोड़कर।
अपवाद और व्हाइटलिस्टिंग	· सभी व्यापारी लेनदेन (किसी भी मोड के माध्यम से, उदाहरण के लिए - यूपीआई, कार्ड, नेट बैंकिंग आदि)। दोहराव वाले भुगतान (जैसे ई-मैंडेट, एनएचसी आधारित भुगतान) और चेक के माध्यम से भुगतान को छूट दी जानी चाहिए। · भुगतानकर्ता एक विशिष्ट लेनदेन को भी व्हाइटलिस्ट कर सकता है, यदि वह समय-संवेदनशील है और / या एक विशिष्ट लाभार्थी है।
थ्रेशोल्ड	₹10,000 और उससे अधिक
लैग अवधि	भुगतानकर्ता बैंक की ओर से 1 घंटे का अनिवार्य समय, सिवाय उन लेन-देन/भुगतान प्राप्तकर्ताओं के जो 'व्हाइटलिस्ट' में शामिल हैं। इस अवधि के दौरान, भुगतानकर्ता लेन-देन को रद्द कर सकता है।
भुगतानकर्ता बैंक से अपेक्षित कार्रवाई	यदि लेनदेन संदिग्ध लगता है तो भुगतानकर्ता से पुनर्पुष्टि मांगने और अपने ग्राहक को लेनदेन रद्द करने की सुविधा प्रदान करने के लिए।

प्रश्न 1: *डिजिटल भुगतानों की सुरक्षा और सुंरक्षा सुनिश्चित करने के लिए आरबीआई द्वारा शुरू किए गए विभिन्न उपायों और पत्र में प्रस्तावित कुछ अन्य उपायों को देखते हुए, क्या लागत-लाभ के दृष्टिकोण से उपरोक्त विकल्प शामिल करने की आवश्यकता है?*

प्रश्न 2: *क्या लेनदेन / खाते की कोई श्रेणी इस दृष्टिकोण से छूट दी जानी चाहिए?*

प्रश्न 3*: क्या ₹10,000 का प्रस्तावित थ्रेशोल्ड धोखाधड़ी जोखिम कम करने और ग्राहक सुविधा के बीच संतुलन बनाने के लिए पर्याप्त है?*

प्रश्न 4*: धोखाधड़ी कम करने की आवश्यकता और डिजिटल भुगतान लेनदेन की दक्षता का समर्थन करने के बीच संतुलन बनाने के लिए भुगतानकर्ता के अंत में प्रस्तावित अनिवार्य लैग आवश्यक है या यह लेनदेन के अंतर्निहित जोखिम के आधार पर वैकल्पिक होना चाहिए जैसा कि भुगतानकर्ता बैंक द्वारा निर्धारित किया जाता है?*

***प्रश्न 5**: भुगतानकर्ता बैंक के अंत में एक घंटे की प्रस्तावित अनिवार्य देरी उचित है?*

***प्रश्न 6**: व्हाइटलिस्टिंग के संबंध में आपके विचार क्या हैं? क्या यह लेनदेन विशिष्ट या लाभार्थी विशिष्ट या दोनों होना चाहिए?*

विकल्प 2: कमजोर वर्गों के लिए उच्च मूल्य वाले डिजिटल लेनदेन के लिए विश्वसनीय व्यक्ति द्वारा अतिरिक्त प्रमाणीकरण

समाज के कुछ खास वर्ग, जैसे कि एक निश्चित उम्र से ज़्यादा के नागरिक या दिव्यांग व्यक्ति (विकलांगता वाले लोग), 'सोशल इंजीनियरिंग' पर आधारित धोखाधड़ी के प्रति विशेष रूप से संवेदनशील हो सकते हैं। ऐसी धोखाधड़ी में अक्सर परिवार के सदस्यों का रूप धारण करना, या मेडिकल, कानूनी या अन्य आपात स्थितियों से जुड़े झूठे हालात खड़े करना शामिल होता है। इस तरह की लक्षित घटनाओं के कारण अक्सर बहुत ज़्यादा आर्थिक नुकसान होता है, जो इस बात पर ज़ोर देता है कि ग्राहकों के इस वर्ग के लिए, लगातार जागरूकता अभियानों के साथ-साथ, सुरक्षा के बेहतर उपायों पर भी विचार किया जाना चाहिए।

2.1 अंतरराष्ट्रीय अनुभव

i. स्वीडन: स्वीडिश बैंकर्स एसोसिएशन द्वारा मई 2024 में पेश किए गए पैकेज के एक हिस्से के तौर पर, यह समझा जाता है कि बैंक ग्राहकों को यह सलाह दे सकते हैं कि किसी खास लेन-देन को ग्राहक के किसी भरोसेमंद व्यक्ति द्वारा मंज़ूरी दी जानी चाहिए।

ii. संयुक्त राज्य अमेरिका: कुछ बैंक अपने ग्राहकों को विश्वसनीय संपर्क व्यक्ति की सुविधा प्रदान करते हैं ताकि बैंक धोखाधड़ी की संदेह के मामले में इन विश्वसनीय लोगों से संपर्क कर सकें। एक विश्वसनीय संपर्क व्यक्ति बैंक के ग्राहक के खाते तक पहुंच सकता है, बशर्ते बाद वाले ने वित्तीय पावर ऑफ अटॉर्नी प्रदान की हो।

iii. आयरलैंड: कोई भी ग्राहक, जो एक व्यक्ति है, किसी 'विश्वसनीय संपर्क व्यक्ति' को नॉमिनेट करने का विकल्प चुन सकता है। वित्तीय संस्थान इस विश्वसनीय संपर्क व्यक्ति से तब संपर्क करेगा, जब ग्राहक से संपर्क न हो पा रहा हो, या जब किसी वित्तीय दुरुपयोग—जिसमें धोखाधड़ी भी शामिल है—का संदेह हो। हालाँकि, इस विश्वसनीय व्यक्ति के पास कोई भी निर्णय लेने का अधिकार नहीं होता है, और यह केवल एक सहायक के रूप में कार्य करता है।

2.2 संभावित दृष्टिकोण:

इस पॉलिसी फ्रेमवर्क में सुरक्षा के बेहतर उपायों के लिए खास प्रावधान बताए गए हैं। इनका मकसद उन संवेदनशील ग्राहकों को सुरक्षित रखना है जो कुछ खास तरह के डिजिटल पेमेंट हस्तांतरण करते हैं। ये उपाय 70 साल या उससे ज़्यादा उम्र के नागरिकों और दिव्यांग लोगों के लिए अनिवार्य हो सकते हैं, जबकि बाकी सभी ग्राहकों के लिए ये वैकल्पिक रहेंगे। इस तरह की प्राथमिकता यह पक्का करती है कि उम्र या दिव्यांगता की

वजह से धोखाधड़ी या शोषण के ज़्यादा जोखिम वाले लोगों को उनकी ज़रूरत के हिसाब से सुरक्षा मिले, और साथ ही बाकी सभी ग्राहकों को भी अपनी मर्ज़ी से चुनने की छूट बनी रहे।

यह नियम मुख्य रूप से उन एपीपी लेन-देनों पर लागू होता है, जिन्हें संवेदनशील ग्राहकों द्वारा शुरू किया जाता है। खास बात यह है कि मर्चेंट लेन-देन (जिनमें यूपीआई, कार्ड-आधारित और नेट बैंकिंग भुगतान शामिल हैं), आवर्ती भुगतान (जैसे ई-मेनडेट,एनएसीएच) और चेक-आधारित लेन-देन को इन ज़रूरतों से स्पष्ट रूप से छूट दी जा सकती है। यह अंतर यह सुनिश्चित करता है कि सुरक्षा उपाय उच्च-जोखिम वाले पीयर-टू-पीयर हस्तांतरणों पर केंद्रित हों, जिससे नियमित वाणिज्यिक या स्वचालित भुगतान कार्यप्रवाहों में कोई बाधा न आए।

सुरक्षा का यह बेहतर तंत्र, किसी संवेदनशील ग्राहक द्वारा नामित "विश्वसनीय व्यक्ति" के रूप में हो सकता है। यह विश्वसनीय व्यक्ति, ज़्यादा मूल्य वाले लेन-देन—जैसे कि ₹50,000 से अधिक के लेन-देन—के लिए प्रमाणीकरण की एक अतिरिक्त परत के रूप में कार्य करता है। यह ध्यान देने योग्य है कि एनसीआरपी में रिपोर्ट किए गए धोखाधड़ी के मामलों में से लगभग 92% का मूल्य इस सीमा से अधिक होता है। इस प्रकार, यह सीमा छोटे लेन-देन के लिए परिचालन दक्षता और बड़े मूल्य वाले हस्तांतरणों के लिए मज़बूत सुरक्षा के बीच संतुलन बनाती है।

किसी भी भरोसेमंद व्यक्ति को बदलने की अनुमति केवल 24 घंटे की अनिवार्य 'कूलिंग पीरियड' (सोचने-समझने के समय) के बाद ही दी जा सकती है, ताकि यह सुनिश्चित हो सके कि ऐसे निर्णय सोच-समझकर और पूरी जानकारी के साथ लिए गए हैं।

चुनाव से बाहर निकलने के लिए, कमजोर ग्राहक अपने अनुरोध के बाद 24 घंटे की प्रतीक्षा अवधि के बाद सुरक्षा प्रणाली से वापस ले सकते हैं। बैंकों को ऐसे अनुरोधों को प्रसंस्कृत करने से पहले ग्राहक को संबंधित जोखिमों के बारे में स्पष्ट रूप से समझाना चाहिए, जिससे सूचित निर्णय लेना सुनिश्चित हो। साथ ही, इन ग्राहकों के लिए किसी भी समय भविष्य में सुरक्षा प्रणाली में पुनर्पंजीकरण के लिए एक सुगम डिजिटल मार्ग प्रदान किया जाना चाहिए, जिससे सुरक्षा को नुकसान पहुंचाए बिना एक्सेसिबिलिटी और लचीलापन बनाए रखा जा सके। यह दृष्टिकोण ग्राहक की स्वायत्तता को प्राथमिकता देता है, साथ ही संभावित ज़ोर-ज़बरदस्ती या जल्दबाज़ी में लिए गए निर्णयों के विरुद्ध सुरक्षा उपाय भी सुनिश्चित करता है।

2.3 फायदे और नुकसान

फायदे:

· एक स्वतंत्र विश्वसनीय व्यक्ति द्वारा एक अतिरिक्त सत्यापन परत प्रदान करता है जो खाता धारक के समान जबरदस्ती, तत्कालता या सामाजिक इंजीनियरिंग दबाव के अधीन नहीं होगा।

· विशेष रूप से उन खाता खंडों के लिए उपयोगी है जिनमें बड़े शेष हैं, जहां धोखाधड़ी लेनदेन से होने वाला संभावित वित्तीय नुकसान महत्वपूर्ण हो सकता है।

नुकसान:

· मौजूदा बैंकिंग प्रथा के अनुसार, किसी खाते के वैध परिचालक के रूप में केवल खाताधारक (या खाताधारक) अथवा अधिकृत हस्ताक्षरकर्ताओं को ही मान्यता दी जाती है। इस व्यवस्था के अंतर्गत, अतिरिक्त प्रमाणीकरणकर्ता का उस खाते में न तो कोई कानूनी हित होता है और न ही कोई लाभकारी हित; फिर भी, प्रमाणीकरण की अनिवार्यता के चलते, वह खाते से होने वाले बाहरी लेन-देनों के निष्पादन को प्रभावी ढंग से प्रभावित कर सकता है।

· यदि विश्वसनीय व्यक्ति तुरंत उपलब्ध नहीं है तो लेनदेन निष्पादन में देरी हो सकती है।

2.4 संक्षिप्त रूपरेखा:

लागूता	अनिवार्य रूप से: · 70 वर्ष और उससे अधिक आयु के नागरिक · दिव्यांग व्यक्ति वैकल्पिक रूप से: कोई भी अन्य ग्राहक (व्यक्ति)
क्षेत्र	· कमजोर वर्गों द्वारा बैंक खातों में किए गए एपीपी लेनदेन। · व्यापारी लेनदेन (किसी भी मोड के माध्यम से, उदाहरण के लिए – यूपीआई, कार्ड, नेट बैंकिंग आदि), दोहराव वाले भुगतान (जैसे ई-मैंडेट, एनएचसी आधारित भुगतान) और चेक के माध्यम से भुगतान को छूट दी जानी चाहिए।
थ्रेशोल्ड	₹50,000 से अधिक
बढ़ी हुई सुरक्षा	कमज़ोर ग्राहक द्वारा पहचाने गए किसी विश्वसनीय व्यक्ति के माध्यम से एक अतिरिक्त प्रमाणीकरणकर्ता। विश्वसनीय व्यक्ति में किसी भी बदलाव की अनुमति केवल 24 घंटे की कूलिंग अवधि के बाद ही दी जाएगी।

ऑप्ट-आउट	कमज़ोर वर्ग के लोग, ऐसी अनुरोध मिलने के 24 घंटे बाद इस सुविधा से ऑप्ट-आउट कर सकते हैं। ऐसे मामलों में, बैंक को ऑप्ट-आउट की अनुमति देने से पहले, इससे जुड़े जोखिमों के बारे में स्पष्टता से समझाना चाहिए। ऐसे ग्राहक को, उसके बाद कभी भी इस सुविधा के लिए दोबारा ऑप्ट-इन करने का एक डिजिटल रूप से आसान तरीका भी उपलब्ध कराया जाना चाहिए।

प्रश्न 7: *क्या समाधान का व्याप्ति पर्याप्त है या किसी अन्य जनसंख्या खंड को अनिवार्य रूप से शामिल किया जाना चाहिए? क्या आयु सीमा उचित है? क्या सभी विकलांग व्यक्तियों को शामिल किया जाना चाहिए या केवल उनका एक निश्चित खंड और यदि हां, तो चयन का आधार क्या होना चाहिए?*

प्रश्न 8: *अतिरिक्त प्रमाणीकर्ता की भूमिका के संबंध में कोई कानूनी, अनुबंध या उपभोक्ता सुरक्षा संबंधी चिंताएं हैं?*

प्रश्न 9: *एक अतिरिक्त प्रमाणीकर्ता की जांच के लिए किस स्तर और रूप की देखभाल निर्धारित की जानी चाहिए जो बैंक के साथ ग्राहक संबंध नहीं रखता है? क्या बैंकों को ग्राहक घोषणा और सहमति पर मुख्य रूप से भरोसा करने की अनुमति दी जानी चाहिए, या क्या अतिरिक्त प्रमाणीकर्ता की स्वतंत्र जांच आवश्यक है?*

प्रश्न 10: *₹50,000 से अधिक का प्रस्तावित थ्रेशोल्ड उचित है?*

प्रश्न 11: *कमजोर वर्गों के हितों की रक्षा के लिए जो सुविधा से बाहर निकलने का चयन करते हैं, उनके लिए कौन सी गाडरिल्स तय की जानी चाहिए?*

विकल्प 3: बैंकों के साथ संबंध की प्रकृति के अनुरूप खातों को श्रेय दिया जाना चाहिए

केवाईसी प्रक्रिया के एक हिस्से के तौर पर, बैंक के लिए यह ज़रूरी है कि वह ग्राहक के कारोबार की प्रकृति और उसकी वित्तीय स्थिति से जुड़े सहायक दस्तावेज़ हासिल करे। इसके अलावा, बैंक को किसी खाते की लगातार समुचित सावधानी भी करनी होती है, ताकि यह सुनिश्चित किया जा सके कि उस खाते में होने वाले लेन-देन बैंक के पास मौजूद ग्राहक की जानकारी, उसके कारोबार और जोखिम प्रोफ़ाइल, तथा ग्राहक द्वारा घोषित धन/संपत्ति के स्रोतों आदि के अनुरूप ही हों। इन दिशानिर्देशों को और अधिक मज़बूत बनाने के लिए, और डिजिटल धोखाधड़ी से हासिल की गई रकम को आगे भेजने के लिए बैंक खातों का इस्तेमाल 'म्यूल' (बिचौलिए) के तौर पर होने से रोकने के लिए, एक ऐसा नियामक उपाय लाने का प्रस्ताव है जिसके तहत, संतोषजनक कारोबारी संबंधों की अतिरिक्त समीक्षा किए बिना, किसी खाते में जमा होने वाली कुल रकम (क्रेडिट) की एक सीमा तय कर दी जाएगी।

3.1 संभावित दृष्टिकोण:

आरबीआई किसी बैंक खाते में सालाना कुल क्रेडिट के लिए एक सीमा (मान लीजिए ₹ 25 लाख) तय करेगा, जिसके लिए ग्राहक से ज़्यादा कुल क्रेडिट की वास्तविक ज़रूरत के समर्थन में कोई अतिरिक्त प्रमाण नहीं लिया जाएगा (जिसे इसके बाद 'कम क्रेडिट टर्नओवर खाता' कहा जाएगा)।

एक बैंक ऐसे निम्न श्रेय टर्नओवर खातों के लिए एक सीमा निर्धारित कर सकता है, जो अपने अंतर्निहित जोखिम प्रबंधन के आधार पर इस प्रस्तावित सीमा से अधिक नहीं होगी,

सभी बैंक खातों—चाहे वे पुराने हों या नए—के साथ एक 'फ़्लैग' जुड़ा होगा। यदि खाता 'लो क्रेडिट टर्नओवर' वाला खाता है, तो फ़्लैग 'चालू' (on) रहेगा; अन्यथा यह 'बंद' (off) रहेगा। प्रत्येक खाते के लिए डिफ़ॉल्ट फ़्लैग 'चालू' ही रहेगा। बैंक, आरबीआई द्वारा नियमों/निर्देशों के माध्यम से दिए गए मार्गदर्शन के आधार पर, अपनी बनाई गई किसी नीति के तहत किसी खाते का फ़्लैग 'बंद' कर सकता है। इसका आधार खाताधारक या उसके माता-पिता आदि की आय, राजस्व, टर्नओवर, संपत्ति, परिसंपत्तियाँ आदि हो सकते हैं; जिसके लिए बैंक द्वारा अतिरिक्त दस्तावेज़ लिए जाएँगे।

क्या 'फ़्लैग'चालू किया जाना चाहिए या नहीं, यह ग्राहक को शामिल करते समय निर्धारित किया जाएगा। हालांकि, बैंक द्वारा प्राप्त अतिरिक्त जानकारी के आधार पर बाद में 'फ़्लैग' चालू या बंद किया जा सकता है। मौजूदा ग्राहकों के लिए, बैंक को विनियमों द्वारा प्रदान किए गए मार्गदर्शन के आधार पर अपनी नीति के अनुसार एक दृष्टिकोण लेना होगा, जैसा कि विनियमों द्वारा निर्धारित किया जाएगा।

एक 'फ़्लैग' चालू वाले बैंक खाते में बैंक द्वारा निर्धारित सीमा तक वार्षिक कुल श्रेय प्राप्त होगा। यदि इस सीमा से अधिक श्रेय प्राप्त होता है, तो बैंक केवल छाया श्रेय की अनुमति देगा। ऐसे धन का उपयोग केवल तभी किया जा सकता है जब बैंक अतिरिक्त जानकारी और / या दस्तावेजों के आधार पर संतुष्ट हो जाए कि लेनदेन वास्तविक है। हालांकि, यदि लाभार्थी 30 कैलेंडर दिनों के भीतर बैंक को संतुष्ट नहीं कर सकता है, तो वह छाया श्रेय वापस ले लिया जाएगा और राशि स्रोत पर भेज दी जाएगी। बैंक उसी के बारे में संतुष्ट होने के बाद 'फ़्लैग' बंद कर सकता है।

यह स्पष्ट किया जाता है कि प्रत्येक बैंक वर्तमान आरबीआईनिर्देशों के अनुसार केवाईसी सहित निरंतर देखरेख का पालन करता रहेगा।

इस दृष्टिकोण का समग्र उद्देश्य वास्तविक ग्राहकों को अत्यधिक असुविधा दिए बिना बैंक खातों के बढ़े हुए जिम्मेदार आचरण को सुनिश्चित करना है।

3.2 फायदे और नुकसान:

फायदे:

- बैंक खातों में धोखाधड़ी गतिविधियों की पहचान और रोकथाम को मजबूत करता है।
- केवल वास्तविक गतिविधि के प्रमाण के बाद ही धन को श्रेय दिया जाता है।

नुकसान:

- निम्न श्रेय टर्नओवर खाते का मूल्यांकन करने में कठिनाई
- अतिरिक्त दस्तावेज के लिए अनुरोध ग्राहक असुविधा का कारण बन सकते हैं।

3.3 संक्षिप्त रूपरेखा:

शामिल किए गए और छूट दिए गए खाते	व्यक्तियों के बैंक खाते (संयुक्त खातों सहित), एकल स्वामित्व खाते, साझेदारी खाते (एलएलपी सहित)। बड़े खाते जैसे कॉर्पोरेट, सूचीबद्ध कंपनियां और सरकार (केंद्र / राज्य) कवर नहीं हैं।

संचयी वार्षिक कुल श्रेय थ्रेशोल्ड	₹25 लाख या उससे कम, जैसा कि बैंक अपने आंतरिक जोखिम मूल्यांकन के आधार पर निर्धारित करता है। बैंक, आवश्यकतानुसार, उचित दस्तावेजों द्वारा समर्थित अतिरिक्त जानकारी के आधार पर इस सीमा को हटा सकता है। मौजूदा ग्राहकों के लिए, बैंक नियमों द्वारा दिए गए दिशानिर्देशों के आधार पर निर्णय लेंगे।
थ्रेशोल्ड के उल्लंघन के मामले में बैंक की अपेक्षित कार्रवाई	'शैडो क्रेडिट' की अनुमति दी जाएगी, और बैंक द्वारा ग्राहक द्वारा साझा की गई अतिरिक्त जानकारी और/या दस्तावेज़ों के आधार पर स्वयं को संतुष्ट कर लेने के बाद ही इन निधियों के उपयोग की अनुमति दी जाएगी; ऐसा न होने पर, 30 दिनों के बाद शैडो क्रेडिट को रद्द कर दिया जाएगा और राशि को वापस स्रोत पर भेज दिया जाएगा।

प्रश्न 12: *इस दृष्टिकोण के बारे में क्या विचार हैं, जिसमें आनुपातिकता के परिप्रेक्ष्य भी शामिल हैं?*

प्रश्न 13: *क्या ₹25 लाख का प्रस्तावित थ्रेशोल्ड उचित माना जाता है?*

प्रश्न 14: *क्या ग्राहक के लिए, कुल क्रेडिट सीमा को पार करने के संबंध में अपने बैंक को संतुष्ट करने हेतु, 30 कैलेंडर दिन पर्याप्त हैं?*

विकल्प 4: ग्राहक-प्रेरित नियंत्रण

वर्तमान में, कार्ड-आधारित भुगतान प्रणालियां ग्राहकों को घरेलू और अंतरराष्ट्रीय उपयोग के लिए एक 'स्विच ऑन/ऑफ' सुविधा प्रदान करती हैं, साथ ही विभिन्न लेनदेन प्रकारों के लिए सीमाएं निर्धारित करने के लिए भी। यह सुविधा ग्राहकों को भुगतान उपकरणों पर अपना नियंत्रण बढ़ाने और धोखाधड़ी के मामलों को कम करने में प्रभावी साबित हुई है। हालांकि, अन्य डिजिटल भुगतान चैनलों में ऐसे उपयोगकर्ता-नियंत्रित तंत्र समान रूप से उपलब्ध नहीं हैं।

4.1 अंतरराष्ट्रीय परिदृश्य:

सिंगापुर:

इसने औपचारिक रूप से एक ग्राहक-नियंत्रित 'किल स्विच' पेश किया है। ग्राहक मोबाइल ऐप या हॉटलाइन के ज़रिए अपने ऑनलाइन बैंकिंग खाते को तुरंत लॉक कर सकते हैं, और इस तरह फंड ट्रांसफर, डिजिटल बैंकिंग एक्सेस और पेमेंट फ़ंक्शन को डिसेबल कर सकते हैं। इस कार्रवाई को केवल बैंक द्वारा पहचान सत्यापन के बाद ही वापस लिया जा सकता है।

ऑस्ट्रेलिया:

कुछ बैंकों ने "डिजिटल पैडलॉक" या "सेफ ब्लॉक" विकल्प लॉन्च किया है, जो ग्राहकों को अपने खातों में अनधिकृत गतिविधि के संदेह में डिजिटल एक्सेस को अक्षम करने की अनुमति देता है।

4.2 संभावित दृष्टिकोण:

4.2.1 लेनदेन स्तर के नियंत्रण

ग्राहकों को डिजिटल भुगतान नियंत्रण प्रदान किए जा सकते हैं जिसमें किसी भी डिजिटल भुगतान मोड के लिए 'स्विच ऑन/ऑफ' सुविधा शामिल हो सकती है, साथ ही खाता स्तर पर विभिन्न लेनदेन प्रकारों के लिए सीमाएं निर्धारित करने के लिए भी।

यह ग्राहकों को खाता स्तर पर किसी भी या सभी डिजिटल भुगतान चैनलों के माध्यम से डेबिट लेनदेन को नियंत्रित करने की अनुमति देगा। इसे ग्राहक द्वारा बैंक शाखा दौरे के माध्यम से या इंटरनेट बैंकिंग, मोबाइल बैंकिंग, फोन बैंकिंग, इंटरएक्टिव वॉयस रिस्पॉन्स या किसी अन्य प्रमाणित बैंक इंटरफ़ेस के माध्यम से पहुंचा जा सकता है।

4.2.2. किल-स्विच

ग्राहकों को एकल सुविधा भी प्रदान की जा सकती है जो खाते('किल स्विच') से सभी डिजिटल भुगतान लेनदेन को एक ही बार में अक्षम कर दे ।

अकाउंट लेवल पर किल-स्विच चालू करने से, अकाउंट होल्डर द्वारा सेट किए गए दूसरे कंट्रोल / कॉन्फ़िगरेशन ओवरराइड हो जाएँगे। एक बार किल-स्विच चालू हो जाने पर, डिजिटल भुगतान को फिर से चालू करने के लिए किल-स्विच को बंद करने की अनुमति या तो डिजिटल तरीकों से (उचित प्रमाणीकरण / सत्यापन उपाय करने के बाद) दी जा सकती है, या फिर खाताधारक के बैंक शाखा में स्वंय जाकर दी जा सकती है। डिजिटल तरीकों से किल-स्विच को बंद करने के लिए, बैंक ग्राहक की असलियत पक्का करने के लिए ज़्यादा सख़्त प्रमाणीकरण / सत्यापन उपाय लागू कर सकता है।

4.2.3 अन्य पहलू

कुछ प्रकार के लेनदेन जैसे भुगतान आदेश, स्थायी निर्देश आदि नियंत्रण और किल-स्विच से छूट दिए जा सकते हैं।

जबकि डिजिटल भुगतान नियंत्रण और किल स्विच को मौजूदा ग्राहकों के लिए एक वैकल्पिक सुविधा के रूप में विस्तारित किया जा सकता है, एक महत्वपूर्ण नीति प्रश्न यह है कि क्या नए ग्राहकों के लिए डिजिटल भुगतान मोड डिफॉल्ट रूप से अक्षम होने चाहिए जब तक कि उन्होंने स्पष्ट रूप से उन्हें सक्षम न कर दिया हो।

एक तरफ, नए खातों के लिए डिजिटल भुगतान मोड को डिफॉल्ट रूप से अक्षम रखने से 'सुरक्षित डिफॉल्ट' सिद्धांत को मजबूत किया जा सकता है। नए खोले गए खाते अक्सर पहचान की चोरी, मूल खाते या ऑनबोर्डिंग धोखाधड़ी के मामले में दुरुपयोग के लिए संवेदनशील होते हैं। हालांकि, डिजिटल भुगतान सुविधाओं को डिफॉल्ट रूप से अक्षम करना ग्राहक सुविधा और डिजिटल भुगतान के अपनाने को प्रभावित कर सकता है। आज कई ग्राहक खाता खोलने के समय यूपीआई, कार्ड और इंटरनेट बैंकिंग जैसे भुगतान चैनलों तक तत्काल पहुंच की अपेक्षा करते हैं।

4.3 फायदे और नुकसान:

फायदे:

· यह उपाय 'ग्राहक-नियंत्रित सुरक्षा' के सिद्धांत को मज़बूत करता है। ग्राहक अपने उपयोग के तरीकों और जोखिम उठाने की क्षमता के अनुसार भुगतान के तरीकों तक पहुँच को कस्टमाइज़ कर सकते हैं।

· धोखाधड़ी की स्थितियों में, समय बहुत महत्वपूर्ण होता है। 'किल स्विच' ग्राहकों को कई सिस्टम्स में जाए बिना या अलग-अलग बैंकों से संपर्क किए बिना, सभी डिजिटल पेमेंट एक्सेस को तुरंत बंद करने की सुविधा देता है।

· यह उपाय भुगतान पारिस्थितिकी तंत्र में एक अधिक समान और मजबूत ग्राहक सुरक्षा ढांचा सुनिश्चित करता है।

नुकसान:

· ग्राहक अनजाने में 'किल स्विच' को सक्रिय कर सकते हैं या कुछ भुगतान माध्यमों को निष्क्रिय कर सकते हैं, जिसके परिणामस्वरूप वैध लेन-देन में बाधा उत्पन्न हो सकती है।

· यूपीआई, कार्ड, नेट बैंकिंग, वॉलेट और अन्य डिजिटल उपकरण जैसे कई भुगतान चैनलों में एक सार्वभौमिक किल स्विच लागू करने के लिए बैंकों के लिए महत्वपूर्ण तकनीकी विकास की आवश्यकता हो सकती है।

· उन मामलों में नियंत्रण अपना उद्देश्य नहीं पूरा कर सकते हैं जहां धोखेबाज ग्राहक के उपकरण तक अस्थायी रूप से पहुंच प्राप्त कर लेते हैं।

4.4 संक्षिप्त रूपरेखा:

क्षेत्र	बैंक ग्राहकों को विभिन्न इंटरफ़ेस के माध्यम से डिजिटल भुगतान चैनलों (एक या सभी) को सक्षम या अक्षम करने की सुविधा प्रदान कर सकते हैं।
छूट	कुछ प्रकार के लेनदेन जैसे भुगतान आदेश और स्थायी निर्देश से छूट दी जा सकती है।
डिजिटल भुगतान पुनर्सक्रिय करने की प्रक्रिया	डिजिटल मोड के माध्यम से या बैंक शाखा में शारीरिक रूप से जाकर।

***प्रश्न 15**: भुगतान आदेश और स्थायी निर्देश के अलावा किन अन्य लेनदेनों को प्रस्तावित डिजिटल भुगतान नियंत्रण और किल-स्विच से छूट दी जानी चाहिए?*

***प्रश्न 16**: क्या नए खातों के लिए सभी डिजिटल भुगतान चैनल "डिफॉल्ट ऑफ" होने चाहिए, या कुछ कम-जोखिम वाले चैनल डिफॉल्ट रूप से सक्षम होने चाहिए? यदि हां, तो ये कौन से होने चाहिए?*

प्रश्न 17*: अगर किल-स्विच लगा दिया गया है, तो क्या डिजिटल पेमेंट को फिर से चालू करने की सुविधा सिर्फ़ बैंक ब्रांच जाकर ही मिलनी चाहिए या डिजिटल चैनल से भी मिलनी चाहिए? अगर बाद वाला तरीका है, तो गलत इस्तेमाल रोकने के लिए क्या सुरक्षा उपाय किए जाने चाहिए?*

v. टिप्पणियों का प्रस्तुतीकरण और आगे की राह

i. इस चर्चा पत्र पर टिप्पणियां / प्रतिक्रियाएं, विशेष रूप से पत्र में उठाए गए मुख्य प्रश्नों और विषय से संबंधित किसी भी अन्य मामले के संदर्भ में, आरबीआई को 'कनेक्ट 2 रेगुलेट' लिंक के माध्यम से आरबीआई वेबसाइट पर प्रस्तुत की जा सकती हैं।

ii. चर्चा पत्र पर प्राप्त टिप्पणियों का विश्लेषण करने के बाद, आरबीआई डिजिटल भुगतान धोखाधड़ी के खिलाफ अतिरिक्त उपाय शामिल करने के लिए अपनी वेबसाइट पर मसौदा दिशानिर्देश जारी करने पर विचार करेगा।

iii. टिप्पणियां प्रस्तुत करने की अंतिम तिथि **8 मई 2026** है।