चित्र नं. १
सामान्य अवस्थाको कारोबार

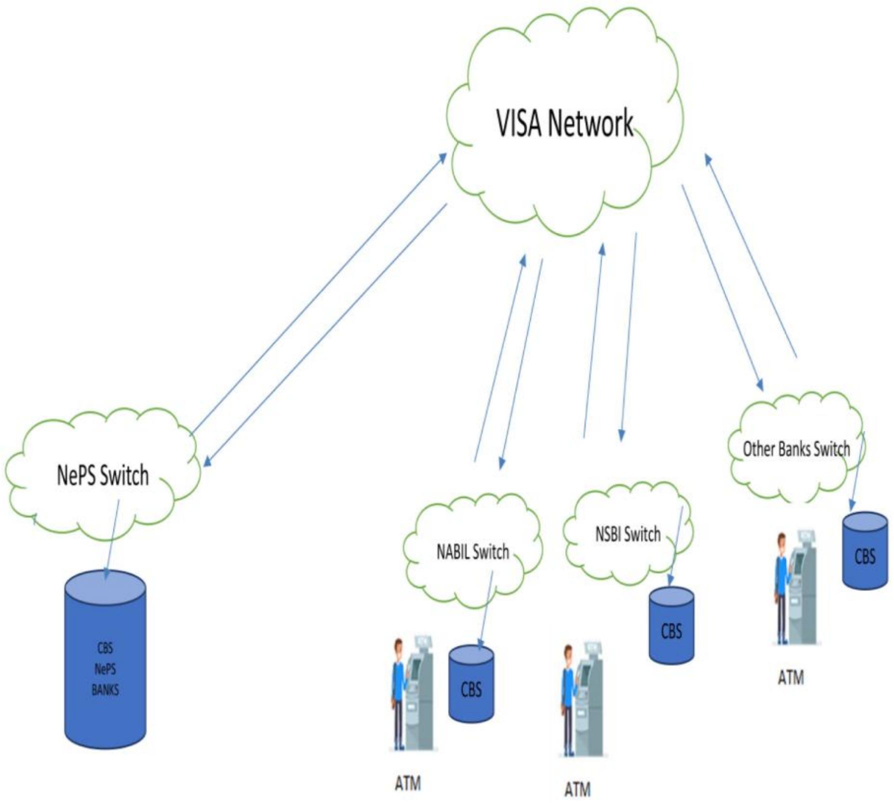


**Figure -1: Normal Scenario of NepS Transaction Processing**

Clickmandu.com

**चित्र नं. २**
**असामान्य अवस्थाको कारोबार**

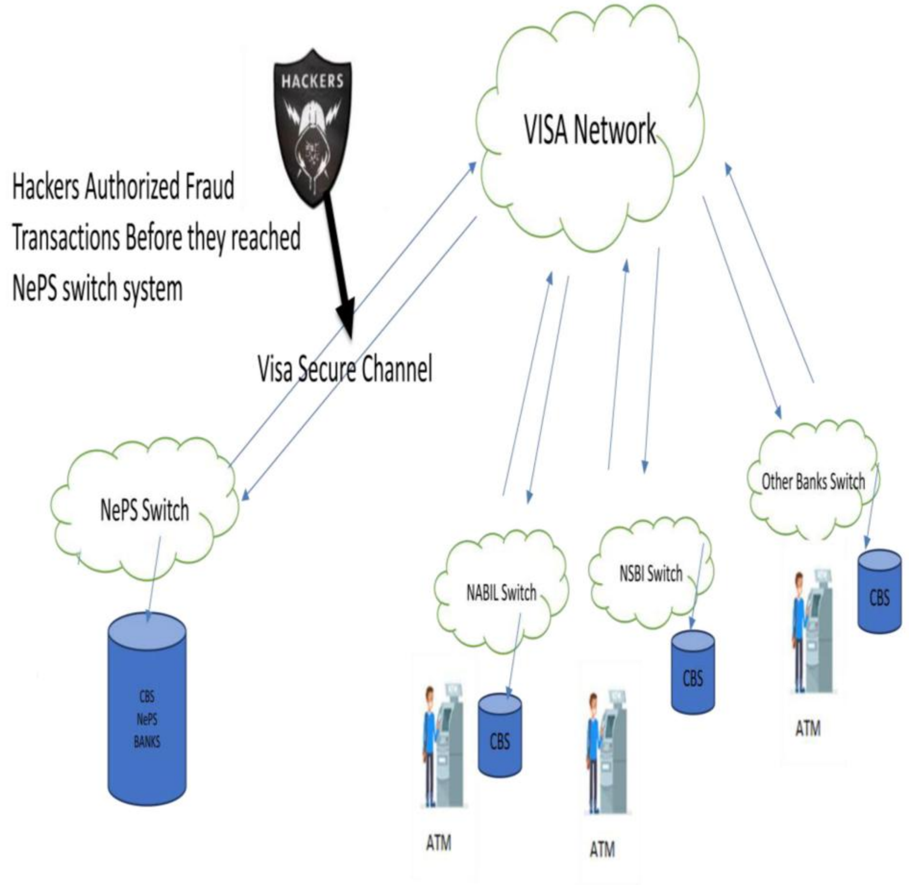


**Figure -2: Suspected Scenario of NepS Compromise**

Clickmandu.com

**निष्कर्ष :**

मिति २०७६/०५/१४ मा नेपाल तथा भारतका विभिन्न बैंकका **ATM** बाट भएका शंकास्पद कारोबारहरुको प्रारम्भिक

- प्रारम्भिक अनुसन्धानबाट भिजा इन्टरनेशनलसँग आबद्ध **NEPS** का सदस्य बैंकहरुको **Clone Debit/Credit Cards** प्रयोग गरी २०७६/०५/१४ गते शनिबार विहान ११:०० बजे देखि साँझ ४:३५ सम्ममा नेपालबाट ७ वटा बैंकका विभिन्न कार्डहरु प्रयोग गरी १७ वटा बैंकका विभिन्न स्थानका ६८ वटा **ATM** बाट रु. १,८९,४४,५००।-, भारतभित्रबाट ६ वटा नेपालका वाणिज्य बैंकहरुको विभिन्न कार्डहरु प्रयोग गरी भारतका विभिन्न स्थानका २४ बैंकका १३२ **ATM** बाट भा.रु. १,०५,८७,२००।- गरी कुल नेपाली रुपैयाँ ३,५८,८४,०२०।- बराबरको रकम झिकिएको पाइएको । यद्यपि उक्त समय भएको कारोबारहरुमध्ये केही कारोबार वास्तविक रहेको पाइएको र थप अन्य कारोबारहरुको **Verification** गर्ने कार्य भई रहेकोले क्षति भएको रकम सो भन्दा केही कम हुन सक्ने ।

- **VISA Network** वा **NEPS Switch** वा दुई प्रणालीको बीच कही कतै कसैले अनधिकृत रुपमा नियन्त्रणमा लिई उल्लेखित **Fradulant** कारोबार हुन गएको अनुमान रहेको । यस सम्बन्धमा **Forensic Expert** बाट प्रतिवेदन प्राप्त गर्नु पर्ने ।

**२) सुझाव :**

यस समितिबाट अध्ययन भएको उल्लेखित घटना तथा नेपालमा कार्डको प्रयोग गरी हुने भुक्तानी प्रणालीमा देखिएको कमी कमजोरीहरुलाई मध्यनजर गरी सम्भावित जोखिम न्यूनीकरणका लागि देहाय बमोजिम सुझावहरु दिइएको छ ।

***(क) अल्पकालीन :***

- हाल घटेको घटनाहरुको **Forensic Experts** द्वारा सुक्ष्म अध्ययन तथा विश्लेषण गरी प्राप्त सुझावहरु कार्यान्वयन गर्नु पर्ने ।

- इजाजतपत्रप्राप्त बैंक तथा वित्तीय संस्थाहरु, **PSP** र **PSO** लाई आ-आफ्नो सूचना प्रविधि तथा इलेक्ट्रोनिक माध्यमबाट हुने भुक्तानी प्रणालीको जोखिम मूल्यांकन गरी जोखिम न्यूनीकरणका आवश्यक उपायहरु अवलम्बन गर्न निर्देशन दिनु पर्ने ।

Clickmandu.com

- कार्ड प्रणाली लगायत **Visa, Master Card** को हिसाब मिलान कारोबार भएको अर्को दिन ( **T+1**) भित्र गर्ने व्यवस्था मिलाउनु पर्ने ।

- नेपालका बैंक तथा वित्तीय संस्थाहरुबाट जारी भएका नेपाली मुद्राका डेबिट तथा क्रेडिट कार्डहरु अब उप्रान्त अनिवार्य रुपमा **Acquirer** र **Issuer** दुवै तर्फ **Chip** र **PIN** को माध्यमबाट मात्र कारोबार हुने व्यवस्था मिलाउने । नेपाल बाहिर यस्तो कार्ड प्रयोग हुँदा नेपालका **Issuer** ले **Fallback Transaction** स्वीकार नगर्ने व्यवस्था मिलाउनु पर्ने ।

- नेपाली बैंक तथा वित्तीय संस्थाहरुले जारी गरेका **Dollar cards** को हकमा विदेशी **Terminals** मा **Acquire** हुँदा **Magnetic Strip** को **Fallback Transaction** नहुने व्यवस्था मिलाउनु पर्ने (**Magnetic Strip बाट घटना घटेकों.**) ।

- बैंक तथा वित्तीय संस्थाहरुबाट यसअघि जारी भएका **Magnetic Strip Card (Non-Chip)** कार्डहरु ३ महिनाभित्र **Chip-based Cards** द्वारा विस्थापन गर्ने व्यवस्था मिलाउनु पर्ने ।

- नेपालमा सञ्चालनमा रहेका सम्पूर्ण **Terminal Devices (POS/ATM)** लाई ३ महिनाभित्र **Chip** र **PIN** लाई स्वीकार गर्न सक्ने गरी सक्षम बनाउन आवश्यक व्यवस्था मिलाउनु पर्ने ।

- बैंक तथा वित्तीय संस्था र **PSO/PSP** ले **24*7 Security Operation Centre (SOC)** सञ्चालन गरी सूचना प्रविधिको क्षेत्रमा उत्पन्न हुन सक्ने जोखिमहरुलाई नियमित रुपले अनुगमन गर्ने व्यवस्था मिलाउनु पर्ने ।

***(ख) दीर्घकालीन :***

- कार्डसँग सम्बन्धित नेटवर्क र सिस्टमको सुपरिवेक्षण नियमित रुपमा गर्नु पर्ने ।

- कार्डसँग सम्बन्धित सूचना प्रणालीको वार्षिक रुपमा अडिट गर्ने व्यवस्था मिलाउनु पर्ने ।

- कार्डसँग सम्बन्धित प्रणालीको **Vulnerability Assessment and Penetration Testing (VAPT)** अर्धबार्षिक रुपमा गर्ने व्यवस्था मिलाउनु पर्ने ।

- कार्डसँग सम्बन्धित प्रणालीको जोखिम मूल्यांकन त्रैमासिक रुपमा गरी सम्बन्धित बैंकको जोखिम व्यवस्थापन समितिमा छलफल गर्ने व्यवस्था मिलाउनु पर्ने ।

- **ATM** कक्षमा जडित **CCTV** को नियमित रुपमा केन्द्रीकृत रुपले अनुगमन गर्ने व्यवस्था मिलाउनु पर्ने । साथै, यस्तो अनुगमन शनिबार लगायत अन्य विदाको दिनमा समेत नियमित रुपले गर्ने व्यवस्था मिलाउनु पर्ने ।

Clickmandu.com

- इजाजतपत्रप्राप्त वित्तीय सेवा प्रदायक संस्थाहरुले साईबर सेक्युरिटीको जोखिमबाट हुन सक्ने सम्भावित नोक्सानी न्यूनीकरण गर्न साइबर सेक्युरिटी बीमा गर्नु पर्ने व्यवस्था मिलाउनु पर्ने ।

- कार्डबाट हुने कारोबारको सीमा नियन्त्रणका लागि भिसा, मास्टरकार्ड लगायत अन्य भुक्तानी प्रणाली सञ्चालक **(PSO)** हरुबाट सबै बैंक तथा वित्तीय संस्थाहरुले कारोबारको सीमा निर्धारण गर्ने सेवा लिनुपर्ने व्यवस्था मिलाउनु पर्ने ।

- बैंक तथा वित्तीय संस्था र **PSO/PSP** ले **Privilege Access Management (PAM)** प्रयोग गरी सूचना प्रविधि प्रणालीको महत्वपूर्ण पूर्वाधार सुरक्षित राख्ने व्यवस्था मिलाउनु पर्ने ।

- **Payment Card Industry and Data Security Standards (PCI-DSS)** पालना गर्ने र **ATM Switch** सञ्चालन गर्ने बैंकहरुले बार्षिक रुपले **PCI-DSS Audit** गर्ने व्यवस्था मिलाउनु पर्ने ।

Clickmandu.com