Ödəniş kartları ilə fırıldaqçılıq əməliyyatlarının qarşısının alınması üzrə
TÖVSİYƏLƏR

Azərbaycan Respublikasının Mərkəzi Bankı öz mandatına uyğun olaraq, bankların istifadə etdikləri ödəniş sistemlərinin etibarlılığının və təhlükəsizliyinin, habelə bank informasiyasının mühafizəsinin təmin edilməsi və eyni zamanda ödəniş kartları ilə fırıldaqçılıq mübarizə tədbirlərinin gücləndirilməsi məqsədilə aşağıdakı istiqamətlərdə tədbilərin görülməsini zəruri hesab edir:

1. Təşkilati tədbirlər

1.1. Ödəniş kartlarının itirilməsi, oğurlanması və səlahiyyəti olmayan şəxslər tərəfindən qanunsuz istifadəsi ilə aparılan əməliyyatlar aşkar edildikdə və əməliyyatların qaydalar çərçivəsində həyata keçirilməsinə şübhə yarandıqda operativ qərarların qəbul edilməsi üçün ödəniş kartları ilə aparılan əməliyyatların sutka ərzində monitorinqini həyata keçirən xidmətin yaradılması;

1.2. Ödəniş kartları ilə fırıldaqçılıq əməliyyatlarının qarşısının alınması sahəsində digər banklarla, kart prosessinq mərkəzləri və hüquq-mühafizə orqanları ilə qarşılıqlı əməkdaşlığın təmin edilməsi;

1.3. Ödəniş kartları ilə bankomat, POS-terminal vasitəsilə, həmçinin internet üzərindən fırıldaqçılıq və saxtakarlıq hallarının hər bir konkret halda baş vermə mexanizminin hərtərəfli araşdırılması və gələcəkdə belə halların baş verməməsi üçün zəruri tədbirlərin görülməsi;

1.4. Ödəniş terminallarının və ödəniş kartlarının EMV (çip) texnologiyalarına tam keçidinin sürətləndirilməsi və maqnit zolaqlı kartların istifadəsinin tədricən məhdudlaşdırılması;

1.5. Kart infrastrukturunun təhlükəsizliyinin tədricən "PCI DSS" standartının tələblərinə uyğunlaşdırılması;

1.6. İnternet üzərindən həyata keçirilən ödənişlərdə "3D secure" təhlükəsizlik texnologiyasının ("Verified by Visa" və "MC SecureCode") tətbiqinə keçidin sürətləndirilməsi.

2. Ödəniş terminalların quraşdırılması, dəstəklənməsi və onlar vasitəsilə əməliyyatların aparılması

2.1. Bankomatlarda xüsusi sensorların (titrəyiş, istilik və s.) quraşdırılması, həmçinin kənar xarici qurğuların yerləşdirilməsini aşkarlayan və ya sıradan çıxaran, o cümlədən bankın təhlükəsizlik xidmətinə xəbərdarlıq siqnalı göndərən "anti-skimming" qurğularının quraşdırılması;

2.2. Açıq havada yerləşən bankomatların yaxşı görünən ərazilərdə quraşdırılması və sutkanın qaranlıq saatlarında həmin ərazilərin kifayət dərəcədə işıqlandırılması;
2.3. Bankomatlarda antivirus proqram təminatının quraşdırılması və virus bazasının müntəzəm olaraq yenilənməsi;
2.4. Bankomat vasitəsilə əməliyyatın aparılması zamanı kart istifadəçisinin eyniləşdirilməsi üçün biometrik məlumatlardan istifadənin mümkünlüyünün nəzərdən keçirilməsi;
2.5. Hər bir bankomatda və ya onun ətrafında ən azı bir müşahidə kamerasının quraşdırılması;
2.6. Quraşdırılmış gizli kameraların və ətrafdakı şəxslərin kart sahibi tərəfindən daxil edilən PIN kodu görə bilməməsi üçün "PIN pad"ın üzərində xüsusi maneələrin (məs., düymələri yalnız istifadəçinin görə bilməsinə imkan verən tor) quraşdırılması;
2.7. Açıq havada yerləşən bankomatların dələduzlar tərəfindən demontaj edilməsini çətinləşdirmək üçün onların yerə bərkidilməsi;
2.8. Müştərilər tərəfindən elektron bankçılıq və ya elektron ticarətdə kart sahibinin eyniləşdirilməsinin dinamik metodlarından (çip autentifikasiya proqramından (CAP) və müxtəlif birdəfəlik parol (OTP) metodlarından) istifadəyə üstünlüyün verilməsi mexanizmlərinin yaradılması.

3. Əməkdaşlarla işin təşkili

3.1. Ödəniş kartlarının xüsusiyyətlərinin və kart texnologiyalarının mənimsənilməsini, habelə ödəniş kartları ilə fırıldaqçılıq əməliyyatlarına qarşı mübarizənin aparılması yollarını mükəmməl bilən mütəxəssislərin hazırlanmasının prioritet vəzifələrdən biri kimi daima nəzarətdə saxlanılması;
3.2. Ödəniş kartları vasitəsilə hesablaşmaların aparılmasında təhlükəsizliyin təmin edilməsi və ödəniş kartları ilə fırıldaqçılığın qarşısının alınması üzrə Mərkəzi Bank və beynəlxalq kart təşkilatları tərəfindən keçirilən tədbirlərdə ödəniş kartları üzrə risklərin idarə olunmasına məsul əməkdaşların aktiv iştirakının təmin edilməsi;
3.3. Bankomatların işinə monitorinqi həyata keçirən və onlara xidmət göstərən əməkdaşlara nəzarətin həyata keçirilməsi;
3.4. Bank əməkdaşının və həmçinin dəstəkləyici (*outsource*) şirkətlərin nümayəndəsinin bankomatların idarə olunması sisteminin resurslarına icazəsiz girişinin qarşısının alınması, həmçinin proqram təminatına sanksiyalaşdırılmamış müdaxilələrin edilməsinə qarşı mühafizənin təmin edilməsi;
3.5. Ekvayer banklar tərəfindən təsərrüfat subyektlərində POS-terminalla işləyən kassirlər üçün mütəmadi treninqlərin keçirilməsi, onların ödəniş kartlarından istifadə üzrə biliklərinin artırılması məqsədilə zəruri materiallarla təmin edilməsi;
3.6. Ödəniş kartları ilə fırıldaqçılıq halı baş verdikdə bank əməkdaşının zərərçəkmiş kart sahibinin müraciətinə operativ reaksiya verməsi üçün daxili prosedur

qaydalarının müəyyənləşdirilməsi və məsul əməkdaşların bu haqda təlimatlandırılması.

4. Kart istifadəçiləri ilə işin təşkili

4.1. Kart istifadəçilərinin ödəniş kartlarından təhlükəsiz istifadə qaydaları haqqında təlimatlandırılması məqsədilə xüsusi "yaddaş kitabçaları"nın hazırlanaraq kart istifadəçilərinə ödəniş kartını alarkən təqdim edilməsi;

4.2. Bankomat və POS-terminaldan istifadə zamanı, həmçinin internet üzərindən kartla ödəniş aparılan zaman təhlükəsizlik qaydalarının kart istifadəçilərinin rahatlıqla görə biləcəyi yerlərdə və bankın internet saytında yerləşdirilməsi;

4.3. Kart istifadəçilərinin bankomatlar üzərində yerləşdirilmiş əlaqə telefon nömrələri, ünvanlar və s. elanlarla təmin olunması;

4.4. Kart sahibləri tərəfindən banka müraciət edilməyənə qədər, onların ödəniş kartları vasitəsilə risk kategoriyası yüksək olan ölkələrdə əməliyyatların (nağd pul vəsaitlərinin çıxarılması, əməliyyatların həcmi və sayı üzrə məhdudiyyətlər) aparılmasının məhdudlaşdırılması;

4.5. Müştərilərin ödəniş kartları vasitəsilə həyata keçirilən əməliyyatları barədə əlverişli şərtlərlə SMS vasitəsilə məlumatlandırılması;

4.6. Kart istifadəçilərinin qarşılaşdığı problemlər və şübhəli hallar barədə sutka ərzində məlumat verə bilməsi imkanının yaradılması;

4.7. İnternet üzərindən ödəniş aparmaq üçün risklərin azaldılması məqsədilə kart istifadəçilərinə ayrıca kartların təqdim olunması;

4.8. Müştərilərə ödəniş kartı təqdim edildiyi zaman kart üzərində imza bölməsində kart istifadəçisi tərəfindən imzanın qoyulmasının təmin edilməsi;

4.9. Kart sahibinin beynəlxalq kart təşkilatlarının "məsuliyyətin ötürülməsi qaydası"nın (*liability shift rule)* qüvvəyə minmədiyi ölkələrdə aparılan əməliyyatlarda ehtiyatlı olmaları barədə hərtərəfli təlimatlandırılması.