Додаток 1

Рекомендації з питань упередження шахрайства з платіжними картками

Для запобігання та протидії злочинам із платіжними картками банкам потрібно скеровувати зусилля на максимальне інформування клієнтів – держателів платіжних карток.

Особливої уваги потребує застереження держателів платіжних карток не повідомляти третім особам власні персональні дані та/або реквізити платіжної картки (номер платіжної картки, ПІН-код, CVV2, термін дії картки, а також код (пароль), який надходить на мобільний телефон для підтвердження переказу/платежу) та інші персональні дані, які необхідні для здійснення переказів та платежів.

Під час здійснення операцій із використанням платіжних карток (у тому числі мобільних платежів), держателям необхідно дотримуватися правил безпеки, які встановлені банком-емітентом, здійснювати постійний контроль за рухом коштів, оновлювати антивірусне програмне забезпечення на персональному комп'ютері, здійснювати своєчасне інформування банку щодо втрати платіжної картки або її реквізитів чи несанкціоновані списання за рахунком, а також дотримуватись рекомендацій, розроблених Національним банком України та розміщених на сторінці офіційного Інтернет-представництва в мережі Інтернет: http://bank.gov.ua/doccatalog/document?id=70904.

Враховуючи активний розвиток такого напряму, як електронна комерція, банку необхідно наголошувати клієнтам про доцільність збереження (а у разі втрати – негайного блокування шляхом подання відповідної заявки до оператора стільникового зв'язку) свого номеру «фінансового телефону», який може бути використаний шахраями для викрадення коштів злочинним шляхом.

Підрозділам банків, які відповідають за банківську та інформаційну безпеку, потрібно забезпечити найвищий рівень безпеки платежів та розрахунків, а також здійснювати моніторинг операцій з використанням електронних платіжних засобів (та/або їх реквізитів) в режимі 24/7. Моніторинг доцільно здійснювати за допомогою системи моніторингу, яка дозволяє виявляти сумнівні операції та вживати заходи для зменшення потенційних ризиків.

Банкам слід сформувати та постійно супроводжувати базу даних інцидентів з електронними платіжними засобами на підставі даних системи моніторингу.

Моніторинг доцільно здійснювати на підставі інформації з власного процесингового центру (у разі його наявності) та/або з незалежного процесингового центру, з урахуванням внутрішньобанківських правил, розроблених відповідно до вимог законодавства України, нормативно-правових актів Національного банку, правил платіжних систем та з урахуванням вимог цих рекомендацій.

У внутрішньобанківських правилах та договору з клієнтом банкам необхідно враховувати можливість врегулювання нестандартних ситуацій у процесі здійснення операцій із використанням платіжних карток та розглядати звернення/скарги клієнта відповідно до умов договору.