**MNB identification code: P14**

**Methodological manual**

**Data related to damages incurred, losses written off and abuses in the payment card issuance and acceptance business**

**I. General instructions**

1. This data reporting contains the damages incurred in the payment card business both on the issuer’s and the acceptor’s side and the related losses.

2. The data of cooperative credit institutions using comprehensive services of banks, as reporting entities, are collected from the system, aggregated and submitted to the MNB in an aggregate form by the reporting entity (bank) operating the system. In the case of a sponsoring bank relationship, the data of the sponsored bank are submitted to the MNB either by the sponsored bank or by the sponsoring bank; in the latter case, the data must be separated from its own data and the GIRO code and registration number of the sponsored bank must be indicated.

3. Requirements related to reporting the rendering of cross-border services by non-resident reporting entities:

* Table 01: Issuance business: All frauds affecting payment cards issued by the service provider and the cardholder is resident or headquartered in Hungary shall be reported.
* Table 02: Acceptance business: All abuses shall be reported, which occurred
  + during the card acquiring services provided by the reporting entity to physical acceptance points in the territory of Hungary, and
  + during internet-based (card not present) acquiring services provided by the reporting entity for enterprises registered in Hungary, and
  + during the operation of ATMs, operated in the territory of Hungary, by the reporting entity as acquirer.

4. Reporting entities providing cross-border payment related services in Hungary are required to apply the code “CROSSB” under the “Type of payment service provider” dimension.

5. The codes necessary for filling the form are included in the technical manuals specified in point 4.8 of Annex 3 hereto, published on the MNB’s website.

**II. Definitions related to the data reporting**

1. Damage incurred: Abuse in the reporting entity’s issuance or acceptance business, of which the reporting entity obtained knowledge in the reporting period, which appears in the same reporting period as losses written off at any actor of the card business, or the final settlement thereof runs through to the next reporting period.
2. Loss incurred at an actor of the card business: Write-off of damage incurred in the current or previous reporting period in the reporting entity’s issuance or acceptance business, broken down by the parties bearing the loss.
3. Damage incurred in on-us turnover: Damage incurred in the reporting entity’s own network, connected to the use of its own cards.
4. Damage incurred in domestic interbank turnover: In the issuance business: damage incurred in the network of other domestic banks in connection with the cards of the reporting entity. In the acceptance business: damage linked to cards issued by other domestic banks in the network of the acquiring bank.

The definitions below also include, in brackets, the terms used by the card companies:

1. Damage incurred in cross-border turnover (Cross-border): In the issuance business: damage linked to the use of reporting entity’s cards abroad. In the acceptance business: damage related to the use of cards issued abroad in the network of the acquiring bank.
2. Damage caused by lost / stolen cards (Lost/Stolen): the damage or losses written off, committed by cards lost by or stolen from the rightful cardholder.
3. Damage caused by cards not received (Card not received): cards forwarded by the issuing bank to the cardholder by post, but not received by the rightful holder, but used by an unauthorised person to carry out unauthorised transactions.
4. Damage caused by a card applied for using false data (Fraudulent application): the cardholder applies for and receives from the issuer a card using false data and carries out unauthorised transactions with it.
5. Damage caused by counterfeit cards (Counterfeit): all forms card counterfeiting shall be included here (e.g. abuses committed by duplicated – skimming – cards, changing the personalisation data of real cards).
6. Damage caused by other abuse (Other): all abuses that cannot be allocated to any of the above categories. However, the damage arising from overdrawing the cardholder customer’s account balance and the abuses when the cardholder misuses his or her own card shall not belong here. In the latter case, the amount shall be stated in the damage category to which it may be allocated based on the customer’s notification. However, the item shall not be stated among the losses in any of the cases (irrespective of whether or not the value of the damage can be collected from the customer), since these cases belong to the category of loan losses rather to payment card losses.
7. Acquisition of card data (Card Skimming): unauthorised acquisition of any data necessary for using the payment card (e.g. data of the magnetic stripe or chip, PIN) at the ATM and POS device, and on the internet in order to manufacture, in possession of the data, counterfeit cards and carry out unauthorised transactions with it.
8. Acquisition of the card (Card Trapping): during the execution of an ATM transaction, physical acquisition of the card and the PIN code belonging to it, and using the card for unauthorised cash withdrawal.
9. Unauthorised acquisition of cash (Cash Trapping): during the ATM transaction the cardholder does not receive the cash despite the fact that according to the slip the ATM dispensed it. After that the cardholder, assuming the faulty operation of the equipment, leaves, the fraudster obtains the cash stuck in the ATM “manipulated” by him or her.

**III. Detailed information related to the filling of the tables, method of data compilation**

1. **Table 01: Loss incurred in the payment card issuance and acquiring business in the reporting period and losses written off**

Abuses committed against the owner of the ATM shall be reported by the reporting entity that provides the service on the ATM equipment (acquiring institution ID), irrespective of whether it uses its own ATM network or operated by another organisation.

Data to be reported in the individual columns of the data reporting:

* column “a”: This column shall indicate whether the reporting entity is a payment service provider, an e-money issuer not providing payment services, a cross-border service provider, or a credit institution.
* column “b”: This column shall indicate if the payment account belonging to the issued card is kept not by the reporting entity. This column shall be filled only for the issuer’s data.
  + code “PENZ”: This code shall be used when the abuse is linked to a card that was issued by the reporting entity payment provider, as third party provider, linked to payment accounts kept by other payment providers.
  + code “EGYEB”: This code shall be used when the abuse is connected to a card issued by the reporting entity payment provider linked to an account kept by it.
  + code “TPP”: This code shall be used when the abuse is connected to a card issued by another, third party, payment service provider, for an account kept by the reporting entity payment service provider.
* column “c”: shall indicate whether the reported data refer to abuses (number of incidents and damage incurred), the losses written off due to abuses or to data acquisition and attacks relating to ATM and POS devices.
* column “d”: This column shall indicate whether the reported data refer to issuer abuses or acceptance abuses. In the case of cards with international trademark, the damages incurred on the acceptance side must be filled in accordance with the data received from the card company. The damages incurred in the reporting entity’s acquiring network, which came to the knowledge of the reporting entity in the reporting period, shall be reported (irrespective of whether the abuse occurred in the reporting period or earlier). Those incidents that the issuing bank has already reported as an abuse but later on do not appear as a loss, shall be also reported.
* column “e”: This column shall indicate the card company codes based on the attached code lists.
* column “f”: This column shall contain the function of the cards. For cards with multiple functions (credit, debit, delayed debit), the turnover data shall be clearly separated by function.
* column “g”: This column shall indicate the type of the card turnover in relation to which the respective abuse occurred.
* column “h”: This column shall indicate the equipment on which the reported abuse has been committed. Transactions conducted at POS terminals or ATMs with payment cards digitized into a wallet application are not considered to be “INAPP” transactions, these transactions shall be reported under “POS” or “ATM” codes. Novel, innovative POS solutions are smart devices (e.g. mobile phones, tablets) that are able to process payment card transaction processes related to purchase transactions due to a software update.. There are 3 solutions in this category: using the communication channel and the display of a smart device, but data transmission (e.g. card chip reading) and PIN entry is done on a separate device (MPOS); PIN entry also on the smart device but data transmission (e.g. card chip reading) on a separate device (SPOS); both data transmission (e.g. card chip reading) and PIN entry on the smart device (Tap-on-Phone). Items related to novel, innovative devices shall be reported under the appropriate category and not under the code “POS”.
* column “i”: This column shall indicate if the abuse has been committed in connection with a contactless transaction.
* column “j”: This column shall indicate the direction of the turnover connected to the abuse.
* column “k”: This column shall indicate the registered office of the acquiring payment provider when the reported abuse took place on the issuer side, and the place of card issuance when the abuse took place on the acceptance side.
* column “l”: This column shall indicate the place of the transaction affected by the abuse. Where a foreign service provider renders acquiring services in Hungary directly rather than through a branch office or subsidiary, on the acquirer side the fraud event shall be reported with the code “HU” as a domestic fraud event. Also to be indicated here are the fraud events in the foreign acquiring network of the Hungarian resident reporting entity, with the appropriate code, if it provides services directly, rather than via a subsidiary or branch office.
* column “m”: This column shall indicate, in the case of issuer side abuse, whether the card used for carrying out the transaction is registered in a mobile wallet. Those cards must be indicated as registered in a mobile wallet that have been registered in a mobile phone payment application provided by the card issuer payment provider or by the service provider being in contractual relationship with it, which may be used for payments at physical points of acceptance (by NFC or QR code) and which may be issued in physical form as well.
* column “n”: shall indicate whether the respective turnover qualifies as remote payment transaction based on point 27a of Section 2 of Act LXXXV of 2009 on the Pursuit of the Business of Payment Services (hereinafter: Payment Services Act).
* column “o”: shall indicate whether strong customer authentication (SCA), specified in point 4a of Section 2 of the Payment Services Act has been carried out upon transaction initiation.
* column “p”: if no strong customer authentication has been carried out in the respective turnover, the reason for omitting that shall be indicated here based on Commission Delegated Regulation 2018/389/EU of 27 November 2017 supplementing Directive 2015/2366/EU of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.
* column “q”: shall indicate the data related to the origin of the abuse.
* Payment order initiated by the fraudster: an unauthorised payment transaction where the fraudster initiates a fake payment order having fraudulently obtained the payer’s sensitive payment data or fraudulently obtained access to the cash substitute instrument used by the customer. Also included here are cases when the fraudster accesses the customer’s device or uses remote access software to submit the order from the customer’s device.
* Payment order amended by the fraudster: an unauthorised payment transaction where in the electronic communication between the payer and the payment service provider the fraudster modifies the legitimate payment order (man-in-the-middle attack) or a participant in the processing of the transaction modifies the payment order in the system of some service provider prior to the clearing and settlement thereof.
* Payment order initiated by the payer: an authorised payment transaction, when the payer consciously initiates the transaction as a result of e.g. deception or psychological manipulation.
* Payment order initiated by the relative of the payer: an unauthorised payment order where the order is initiated by a relative of the payer, rather than by a party acting fraudulently, without the approval of the payer.
* column “r”: This column shall indicate the type of payment card abuse.
  + Data phishing / identity theft / theft of card details: acquisition of the payer’s sensitive payment data / identification documents / card details by the fraudster, in possession of which a card payment may be made on behalf of the customer. Complete column “v” in the case of phishing / identity theft, to indicate the method of phishing.
  + Psychological manipulation / deception to initiate or approve payment transaction. This category includes, among others:
    - persuading to make a fictitious purchase: when the payer is persuaded – typically through a fictitious advertisement or webshop – to pay in advance for a product or service which then is never sent or fulfilled;
    - deception related to bogus investment: when the fraudster convinces the payer to invest in a non-existent investment instrument (e.g. investment fund, bullion, real estate or crypto currency), but in fact the investment is never made after transferring the funds to the fraudster;
    - emotion-based deception/manipulation: when the payer is persuaded by citing some problem (e.g. medical treatment related to deteriorating health or covering the costs of organising a personal meeting) to pay to a person with whom she or he has become acquainted earlier (typically in the online space or through social media) and believes to have an emotional relationship with;
    - deception related to making available high-value articles or amounts (e.g. the so-called “Nigerian scam”): when the fraudster convinces the payer to pay a fee alleged to be necessary for releasing a payment of larger amount or goods of particularly high value (e.g. prepayment of administrative costs related to the payment or transfer of a high-amount lottery prize; reimbursement of costs related to the customs clearance of articles sent as gift; reimbursement of costs related to inheritance);
    - deception linked to the payment of invoices: when the payer tries to pay an invoice to a legal beneficiary, but the fraudster intervenes and convinces the payer to make the payment to an account controlled by him or her;
    - deception linked to impersonation: when the fraudster, pretending to be some official person (e.g. employee of public authority, typically the police; state or local government officer), bank employee, high-ranking representative of the payer’s employer, employee of public utility or telecommunication company or representative of a fundraiser civil organisation, convinces the payer to make a payment to an account controlled by him or her.
  + Payer acts fraudulently: self-fraud, when the payer pretends to be a victim of fraud, thereby trying to make the payment service provider refund the sham loss.
  + Direct access to a cash substitute payment instrument: Using the card details stored by the merchant or service provider or a tokenized card for starting a payment in the system of a merchant or service provider without copying the data. This includes executing contactless payments with stolen mobile phones.
* column “s”: This column shall indicate to which party, participating in the payment transactions, the written off losses originating from the acceptance and issuer abuses has been charged. If the incurred loss is shared by more than one party, it shall be divided between the rows of the relevant code values. If the abuse is recovered in any form or the amount of the loss involved in the abuse is partly or fully recovered, report the recovered part under the “MEGTER” code. In this case reduce the loss charged to the customer or the merchant, and borne by the service provider with this amount. If the recovery took place in a period other than when the loss was actually written off, carry out a retrospective amendment based on the available new information. On the other hand, report the written-off loss only when the respective case has been closed and the accounting settlement has also been performed; accordingly retrospective adjustment is necessary only if any change occurred as a result of new information in an already closed, and thus reported case.
* column “t”: This column shall indicate the type of data acquisitions and attacks:
  + Incidents aimed at acquiring the card: Report the number of payment cards, and corresponding loss, where the card was stolen from the cardholder.
  + Incidents resulting in the reversal of unauthorised transactions: The number of those incidents shall be reported that affect the operation of the ATM in such a way that it declares the transaction failed despite dispensing the cash.
  + Cash trapping incidents: the number of those incidents and corresponding loss shall be reported where the cash is dispensed but not to the rightful cardholder (e.g. sticking).
  + Physical and electronic attacks against ATMs (except explosion): the number of incidents and the amount of cash effectively stolen or becoming worthless, where the ATM equipment or the network serving it is affected by a physical or electronic attack. (excluding explosions). Those incidents shall be also reported when only the equipment is damaged as well as those when the cash stored in the ATM is stolen or destroyed. (e.g. ripping the ATM from the wall or drilling into it to get the safe cassette).
  + Attacks against ATMs involving explosion: the number of incidents and the amount of cash effectively stolen or becoming worthless, where the ATM is exploded.
  + Attacks against the ATM service staff: the number of incidents (occasions) and the amount of cash effectively stolen or becoming worthless where the ATM service staff was attacked. Incidents when the stealing of cash did not succeed shall be also reported.
  + Incidents aimed at acquiring card data: Report the number of incidents where the purpose was to obtain the card data.
* column “u”: shall indicate whether the attempted abuse succeeded. Failed attempted abuses, when the amount intended to be stolen cannot be established, shall be reported with 0 amount.
  + All cases: It shall also qualify as a payment abuse when a relative of the payer initiates a transaction without the payer’s authorisation or the payer submits a payment order to the benefit of a party acting fraudulently as a result of a deception or psychological manipulation. However, only those cases shall be reported that the reporting entity also classifies as an abuse and its appropriate of organisational unit (e.g. bank security, internal audit) treats it as such.
  + Failed case: All cases where the payment order is not executed shall qualify as failed attempted abuse. This category includes cases when the payer’s payment service provider – usually as a result of the applied fraud detection mechanisms – intervenes before the authorisation of the payment order, irrespective of the origin or motive of the abuse. The failure of the authorisation of persons disposing over the cash substitute payment instrument shall not qualify as an unsuccessful attempted abuse, e.g. providing wrong password several times in the mobile wallet application. On the other hand, it also qualifies as a failed abuse when the party acting fraudulently obtains the payer’s sensitive payment data or access to the cash substitute instrument, but does not get as far as commencing the submission of the payment order (e.g. the payment service provider’s fraud detection mechanism detects the intervention of a malicious software, providing remote access, when applicable, and thus it restricts the submission of payment orders). In such cases enter HUF 0 as the amount of the failed abuse. When reporting failed abuses, notifications by the customer shall be also taken into consideration, but it is subject to reporting only if the competent organisational unit of the reporting entity also classifies these incidents as an abuse.
  + Successful case: All cases when the reporting entity executes the order, even if the stolen amount is later recovered by the reporting entity, shall qualify as successful abuse.
* column “v”: indicate here the exact method of committing the abuse indicated in column “r”, related to phishing / identity theft / theft of card data.
  + Harvesting of data by malware: Accessing personal or card data with the help of software installed on the customer’s device. The definition also includes the malicious use of legal software (e.g. software facilitating remote access).
  + Unlawful access to data by hacking an IT system: Accessing data by hacking the system of a party other than the customer. This may be any participant in the payment chain, or even third parties storing the personal data of the customer for some other purpose.
  + If the method of accessing the data is not known, the “Egyéb” (“Other”) code should be used for reporting.
* column “w”: indicate here the exact method of access in the case of indirect access to the cash substitute instrument indicated in column “r”. If fraudsters access user account details for their fraudulent purpose without hacking any software or IT system installed by the payer, the “Egyéb” (“Other”) code should be used for reporting (e.g. obtaining data from customers by psychological manipulation)
* column “x”: name the source from which the data provider learned of the fraud. If a data provider has learned about a fraud from more than one source, it should be classified into the category of the source from which the data provider first learned about the fraud.
  + UGYFEL: Fraud that has been reported by a client of the data provider. This does not include fraud which the data provider had already learned of from another source and was subsequently reported by the client.
  + VALOSIDO: Fraud detected by the data provider’s real-time automated fraud filtering mechanism, before the transaction has taken place. This includes corresponding systems provided by financial infrastructures integrated into banking processes.
  + SZURES: Fraud detected by the data provider’s other fraud filtering mechanism. This includes corresponding systems provided by financial infrastructures integrated into banking processes.
  + PSZOLG: Fraud that has been reported to the data provider by another payment service provider or financial infrastructure in a separate message or a complaint handling process. This does not include frauds identified by fraud filtering systems provided by financial infrastructures. (e.g. Visa, MasterCard)
  + HATOSAG: Fraud of which the data provider has been informed by Hungarian or foreign authorities. (e.g. police, court)
* column “y”: In this column, indicate whether the fraud was committed with a retail or a corporate card. Business or corporate cards are cards issued to employees of companies and other organisations. Retail cards are cards issued to private individual clients. For SZÉP cards, only the retail card code may be used.
* column “z”: shall indicate the number of abuses and data acquisitions.
* column “a1”: shall indicate the amount of loss incurred and written off in connection with the abuses, stated in units of forint. The forint equivalent of the data arising in foreign currency shall be calculated using the reporting entity’s own exchange rate prevailing on the day of the transaction or the average MNB exchange rate for the reporting period.

**Table 02 Fraud rate statistics in the payment card issuance business in the reporting period**

Data to be reported in the individual columns of the data reporting:

* column “a”: This column shall indicate whether the reporting entity is a payment service provider, an e-money issuer not providing payment services, a cross-border service provider, or a credit institution.
* column “b”: This column shall indicate if the payment account belonging to the issued card is kept not by the reporting entity.
* column “c”: This column shall indicate the fraud rate related to the amount reported in column “f” and the deviation from the reference fraud rate under the SCA Regulation, i.e. when the calculated fraud rate differs from the reference fraud rate under the SCA Regulation. Furthermore, the termination of the application of exemption from strong customer authentication based on transaction risk analysis shall be reported here, i.e. the case when for any of transaction types the calculated fraud rate in two consecutive quarters (180 days) exceeded the reference fraud rate under the SCA Regulation, and based on this the reporting entity terminated the application of the exemption based on transaction risk analysis.
* column “d”: This column shall indicate the transaction type, i.e. the respective abuse occurred in connection with card turnover.
* column “e”: When the fraud rate differs from the fraud rate under the SCA Regulation connected to the transaction type, the threshold value shall be reported here.
* column “f”: This shall indicate the percentage value of the calculated fraud rate, as well as the deviation from the reference fraud rate under the SCA Regulation. The deviation from the reference fraud rate under the SCA Regulation shall be calculated by deducting the reference fraud rate under the SCA Regulation from the calculated fraud rate. The values shall be specified in values for one unit, with an accuracy of 3 decimal points. In the case of deviation from the reference fraud rate under the SCA Regulation negative values may be also reported, while upon the termination of the application of exemption from strong customer authentication based on transaction risk analysis only positive values may be reported.