Good Security Practices in the Area of Card Transactions

These "Good Practices" should be applied as part of the Company's ongoing operations, and in particular card payments, their monitoring and transaction reconciliation.

Card Payments:

1. The processes of each card program should be based on the appropriate contract and terms & conditions, as well as principles such as:
    a. a transaction where card details are used to directly initiate a payment should only be ordered by the holder of that card (Cardholder);
    b. if a transaction standard requires the transfer of card details via an open channel, such as e-mail or telephone (i.e. MOTO transactions), the card details should be sent directly to the Merchant, without any third party's having access to these details.
2. A refund should be made in the same manner in which the original payment was executed (i.e. to the instrument that was used to make the payment).
3. In the case that a large volume of transactions are executed on a single card, we suggest that at least 1 additional card be issued for each Cardholder and that they be replaced alternately at short intervals, e.g. every 6 months.
4. In addition, the set of places where card payments can be made should be limited (by specifying permitted or excluded MCCs (merchant category codes), i.e. four-digit codes assigned to payment-accepting entities to specify the type of business run by the entity – the payment recipient) to typical or expected expenses, if the cards used have high limits or are dedicated to specific payments/recipients.

    Example: In the case of companies from the tourism industry, cards should be configured so that they can only be used at sellers from that industry, or even for the purposes of specific activities of individual teams, for instance cards of the air travel department should only enable payments for airline tickets or services.
5. Systems/portals/online transaction sites used by the Company – cards should be used with their details masked or with a low limit if the card details may be visible to a third party.
6. Card limits should correspond to the most common transaction value. For higher and less frequent amounts, the limit can be changed online via the OLM module in the CitiManager system. Such a change should be temporary and the card/transaction limit should be restored to its original level after the payment is made.
7. Card and transaction limits should include a possibility of submitting chargebacks, the number of which may be limited (the rules and limits for chargebacks are determined by the card organization, e.g. Visa, and the Bank has no influence on how these rules and limits are set by card organizations).
8. MOTO (mail order, telephone order) transactions are only allowed where there is no other way to make a payment.
9. Limits should be tailored to various departments of the Company and payment types, for example in the case of a company in the travel industry cards of, for instance, the hotel booking department, should have different total limits and individual transaction limits than cards used by the airline ticket purchase department.

Card transaction monitoring:

1. Transactions pending authorization which are visible in CitiManager (status visible before the card is charged online) should be analysed on an ongoing basis. Such transaction analysis during authorization makes it possible to detect a fraudulent transaction before it is charged to the card.
2. Transactions recorded on the card that are visible in CitiManager should be analysed on an ongoing basis.
3. Notifications of each high-value transaction and each instance when the card limit utilisation rate is high should be analysed on an ongoing basis. CitiManager makes it possible to send online notifications to 5 different recipients, in many variants, such as notification of each transaction, of each transaction above the defined amount limit, or of each instance where the card limit utilisation rate has reached X%.
4. Monitoring should be carried out whether a given seller (merchant) is on the list of sellers dealing with the Company. Such control should not be limited to verifying whether the seller type is specific for a given department.
5. A card should be blocked each time an attempt is made to charge it or the card is charged with an unknown transaction.
6. Once a fraudulent transaction is identified, the merchant should be contacted immediately to cancel or block the service and payment refund.

Reconciliation process:

1. Data from transactions recorded in the CitiManager or CitiManager Reporting system with reservations/orders should be reconciled on a daily basis, immediately after they are made available in the Bank's system.
2. Processes should be automated based on system integration between the Bank and the Company.

The Bank reserves the right to cancel, limit or change the terms & conditions of current cooperation at any time based on further transaction processes. This material is not intended for confidential use and the guidelines contained herein may be forwarded to other recipients in order to improve the security of transactions made with payment instruments offered by the Bank, and they are not an exhaustive set. For this reason, we also recommend using other good market practices and systems.

In order to secure processes and complete an audit, we recommend hiring a specialized company that provides security/cybersecurity services in your industry.