Fraud Risk Mitigation and Best Practices

This guide is meant to serve as a resource for Program Administrators and other company representatives to identify and implement appropriate fraud and risk mitigation controls within all card programs.

Account protection begins with cardholders

The best protection from unauthorised use is prevention. The following are best practices and tips that Elavon shares with organisations:

- Sign the card as soon as it arrives.
- Make sure the card is always in the cardholder's possession; do not leave it in a drawer or out in the open.
- Keep an eye on the card during the transaction and ensure it is returned as quickly as possible.
- Destroy any unneeded receipts and statements.
- Report any questionable charges promptly to customer service.
- Notify customer service in advance of a change in address or phone number.
- Use your chip and Personal Identification Number (PIN) when the option is available. This is the most secure way to complete a transaction.
- Do not lend the card or PIN to anyone.
- Never write account numbers or personal information on unsecured media such as a piece of paper or business card.
- If one receives an email, telephone call, text, or other form of communication asking to confirm an account number or One Time Passcode (OTP), do not provide any information and call the number on the back of your card.
- Do not publish program information on public or unprotected websites. Fraudsters will use this information to take over the account.
- Program administrators should confirm cardholder identity through company instant message or email prior to removing a fraud block or providing account information. Fraudsters may contact you for assistance impersonating a cardholder.

Additional monitoring, communication, and data retention best practices include:

- Suspend or cancel account privileges when appropriate.
- Notify the customer services team in advance of any changes in spending patterns.
- Communicate policies regarding appropriate account use frequently.
- Remind cardholders how to report suspicious activity.
- Keep all records current and be mindful of how card data is stored and destroyed. Card associations have regulations around the storage or account and transaction data.
- Encourage cardholders to keep contact details up to date with Elavon.

Leverage Proven Best Practices

Fraud prevention and detection is everyone's responsibility, Elavon recommends that organisations follow proven best practices when establishing accounts and implementing fraud controls.

(02/21) CAT-19524358

How does Elavon defend against fraud?

Elavon provides automated tools and proprietary systemic monitoring to identify and manage unauthorised account activity. These additional security measures happen behind the scenes and generally do not affect cardholders as they conduct business. This section provides a high-level overview of Elavon fraud defence and case processing processes:

- Develop strategies to decline and/or queue suspicious transactions.
    - Monitor for counterfeit test authorisations.
    - Watch for increased counterfeit activity by location.
- Compare new counterfeit cases against known compromised merchants.
- Assess risk of continued use of compromised card numbers, may suggest a proactive card reissue.
- Analyse transaction history of counterfeit cases daily to find new compromise locations.

Analysing fraud

- As new trends are identified Elavon will adjust or create strategies to detect and stop these trends.
- Strategies are monitored and adjusted daily.
- Two types of fraud rules:
    - Near-time rules
    - Real-time rules
- Combining real-time strategy with near-time strategy provides us with an effective protection against fraud.

Near Time rules

- Fraud system monitors authorisations post-decision and routes highest risk activity including:
    - Authorisations over a risk score threshold
    - Authorisations that meet criteria matching current fraud trends
- Fraud detection analysts review the accounts in queue.
    - Add or remove the Watch Status.
    - Call cardholder to confirm activity, leave block in place if unable to reach cardholder.

Real Time rules

- A real-time rule declines or refers at the point of sale
- Reserved for activity with the highest fraud risk

3-D Secure Authentication

- This strong customer authentication (SCA) occurs prior to the actual authorisation process and helps us to identify and prevent online fraud.
- By inserting this additional authentication step, Elavon can take advantage of more data than ever before to help differentiate good transactions from fraud.
- Allows cardholders to verify online transactions using biometrics.

What happens if fraud is confirmed?

- Fraud claim is initiated.
- Card will be closed as a result of claim initiation.
- Notations added to the account memo.

Fraud Case Process

- Fraud cases should be initiated over the phone. Please do not use mail, fax or online processes to initiate Fraud.
- The Fraud Representative will initiate the case by marking the authorisations and/or transactions that have posted to the account that are believed to be fraudulent.
- Because a third party has gained access to your account information, we will ask you to close your account as we are required to do so. It will be replaced with a new number and all account information transferred.
- If the fraud charges post to your new account, you will receive a credit to your account and sent a statement of fraud to confirm that you did not authorise those transactions.
    - The statement of fraud will be mailed to the system address on the card.
- The statement of fraud will need to be completed by the cardholder and returned to the Fraud Department.
- Once the statement of fraud is received an investigation will be conducted to determine who is responsible for the fraud.

- If it is discovered that the cardholder participated or benefited from the charges the account will be re-billed and the claim denied.
- If the claim is resolved in the cardholder's favor the credit will remain on the account permanently.

Always report unauthorised activity immediately

If one suspects an account has been compromised or notices any unauthorised activity, it should be reported **immediately**. The faster unauthorised activity is reported, the faster it can be stopped.

Other items available for Fraud mitigation

MCC Blocking

High-risk merchant category groups such as casinos or jewellers in which fraud is most prevalent will always be blocked. Clients can apply additional blocking based on individual requirements.

Spending and Transaction Limits

Clients can establish spending and transaction limits to support program needs. Elavon offers a variety of spending controls:

- Limit number of transactions in a day, week, month, cycle, quarter.
- Amounts limits based on transaction, day, month, cycle, quarter.

International Transaction Blocking

If the cardholders within a program will only transact in their home country, they can choose to block all foreign transactions. This block is applied at the corporate account level and would prohibit foreign transactions on all accounts that fall under that company account. Blocking international spend will significantly reduce fraud risk within a card program.

Other important points to note

Please ensure your cardholders have access to the Elavon customer services contact numbers. These are visible on all cards and statements.

We recommend program administrators also make the phone numbers available internally (through internal websites, newsletter, emailing, etc.). They are also available on our website: elavonpayment.com

Country	Customer Service
Ireland	1850 923 486
UK	0345 601 4437
France	0811 64 00 82
Germany	069 380 789 292
Netherlands	0900 040 1424
Italy	02 871 03589
Spain	901 810 958
Poland	022 306 22 49
All Other Countries	+353 1 656 9898