Transaction Alerts/Controls/Notification Services

1.1 Definition/Description

Transaction alerts are generally an issuer-based control that alerts cardholders of particular activities, which can include both purchase transactions as well as non-monetary actions (such as change of address or activation of a new card). Alerts can also be triggered based on preset thresholds (i.e., alert if the credit limit is utilized > x% or if a payment is due).

1.2 Applicability

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	NA	Customer onboarding	NA	Merchants	NA
Mobile browser	Yes	Authentication (onboarding)	NA	Issuers	Yes: internal
Desktop/laptop computer	Yes	Authentication (transaction)	NA	Issuer processors	Yes: internal
Phone	Yes	Authorization	Yes	Wallet/online payment providers	Yes: internal
		Post-authorization review	Yes	Acquirer processors	NA

1.3 Technical Features/How the Technique Works

A cardholder would receive an alert message based on a particular activity on their account. Alerts can be delivered in a variety of channels, with in-app push notifications, SMS text, and e-mail being the most popular. Outbound calls are generally not used for alerts except in the case of calls to verify suspicious activity. Certain alerts can also be sent by physical mail, but these are generally confirmations related to account information changes.

Alerts can be set up as mandatory, opt out or opt in depending on type of activity involved and the risk tolerance of the bank.

- Mandatory or opt out would generally be used for suspicious activity alerts and payment due notices.
- Opt-in would generally be set up for specific transaction parameters.
  - A further option would be for a cardholder to specify certain transaction types that should be declined.

Types of activity that could generate an alert include:

- Authorization activity
  - Transactions from a certain POS mode (e.g., ecommerce, keyed).
  - Transactions > $x
  - Transaction amount > baseline spending $x
  - All transactions

  - Transactions at a certain merchant category
  - One small CNP transaction followed by a big purchase
- Payments
  - Payment due
  - Payment posted
- Account changes
  - Authorized user added
  - Address change
  - Phone change
- Geolocation
  - New place, first transaction with large amount
  - Two card-present transactions at different locations in short period of time
- Other
  - Card activated
  - Replacement card ordered
  - Card mailed

1.4 Risks Associated with Technique

This technique has few risks since the cardholder opts in to participate.

1.5 Customer Impact/Level of Friction

Friction varies based on the delivery channel and frequency of the alerts. Since most alerts do not require a cardholder action, friction is lower than if the customer was specifically required to respond before completing a transaction.

1.6 Implementation Considerations

Implementation of this technique requires:

- Determining what types of actions will trigger alerts, to identify which authentication and posting processes need to be linked to a communication process.
- Determining delivery channels, which will drive complexity, especially if one or more channels are managed through a vendor service.
- Determining how opt-in selections are made. Selection needs to be made available through self-service channels (e.g., online, mobile) as well as through an internal console which can be accessed by phone agents and back office personnel.
- Implementing security approaches that, at a minimum, need to log any changes made to alert thresholds.

Integration complexity is moderate and depends on the channels, activity types and level of integration that already exists between them.

Implementers will need to balance their desired level of investment in preventative tools and risk appetite. Alerts will provide additional protection above and beyond internal detection tools as cardholders know their activity the best. However, the bank cannot rely on cardholders to police their usage as a control and typically use alerts in conjunction with a robust fraud mitigation strategy. In

addition, the sheer volume of alerts can cause some cardholders to tune out or turn off the functionality.

1.7 Maturity

Electronic alerts have been in use approximately as long as online banking. Alerting functionality is a key service in mobile banking apps.

1.8 Applicable Industry Standards

This technique has no applicable industry standards.

1.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

1.10 Further Reading

https://www.thebalance.com/credit-card-fraud-alert-notifications-4135739

https://usa.visa.com/visa-everywhere/security/transaction-alerts.html