RISK PROFILE MANAGER™

BENEFITS

- Product differentiation
- Rapid time-to-market
- Fully integrated with Postilion
- Centrally monitored and controlled

The case for Risk Profile Manager

Despite the introduction of chip cards which provide superior security features, the lowest common denominator for transactions worldwide remains the magnetic stripe. POS and ATM fallback transactions, coupled with transactions that occur in a Card-Not-Present environment (CNP), expose a relatively high surface attack area for fraudsters that exploit the loopholes of technology.

Banks and merchants have responded to fraudulent transactions in a variety of ways. Chip-and-PIN, amount and velocity limits, real-time evaluation of transaction risk are just some of the mechanisms in place than provide transaction security. Others include attempts to predict customer habits based on previous spending habits or disallow the use of cards in certain environments or countries. Issuers that do not want to expose their customers to increased risks tend to lock-down card products and thus restrict their utility.

One problem with these approaches is that legitimate customer behavior that may be regarded as fraudulent activity results in a simple decline of service. The only way around this limitation is to let the cardholder define what transactions should be considered fraudulent, allowing others to be authorized by the issuer.

Risk Profile Manager allows the user to easily become a part of the authorization process through the internet, an IVR or a mobile phone. The cardholder uses an online interface to define the valid profile of transactions. National transactions can be allowed but only from ATM devices, not POS terminals, and only for amounts up to a specified maximum. International transactions originating from a specific country may be allowed only while the cardholder is on a trip. All CNP transactions may be barred from getting an authorization but when that Amazon purchase is declined, the cardholder can temporarily allow the authorization of transactions from that specific merchant and for a specified amount. A time-out facility can lock everything and not allow any transactions after a defined period unless the cardholder explicitly allows it.

FEATURES

- User-configurable control of authorizations
- Accessible through Internet, Mobile phone or IVR
- Authorize specific merchants for CNP transactions
- Immediate reduction of fraudulent transactions

CODIX S.A. | Systems Integration
14, Solonos Str. 10673 Athens Greece
F: +30 210 364 9000, F: +30 210 364 9001
E-mail: info@codix.gr, sales@codix
Web: http://www.codix.gr/

RISK PROFILE MANAGER™

INTEGRATED WITH POSTILION

Risk Profile Manager is completely integrated with Postilion on the server-side. For issuers, the authorization process is implemented as a Postcard plug-in, where Risk Profile Manager takes an active part of the authorization. For acquirers, Risk Profile Manager is implemented as a driver.

To extend its functionality, Risk Profile Manager offers an additional SOA interface which can be utilized by external entities. Customers may choose to define the authorized use of their cards through any external channel, such as the Internet banking site, the Mobile banking facility, an IVR or through an agent.

These channels are integrated with Risk Profile Manager by utilizing the provided SOA facility. The provided interface allows for the detailed configuration of cardholder authorization profiles but it is up to the channel implementation to choose the level of detail that can be provided to cardholders, depending on the capabilities of each channel and the sophistication of the cardholder.

EASY CONFIGURATION

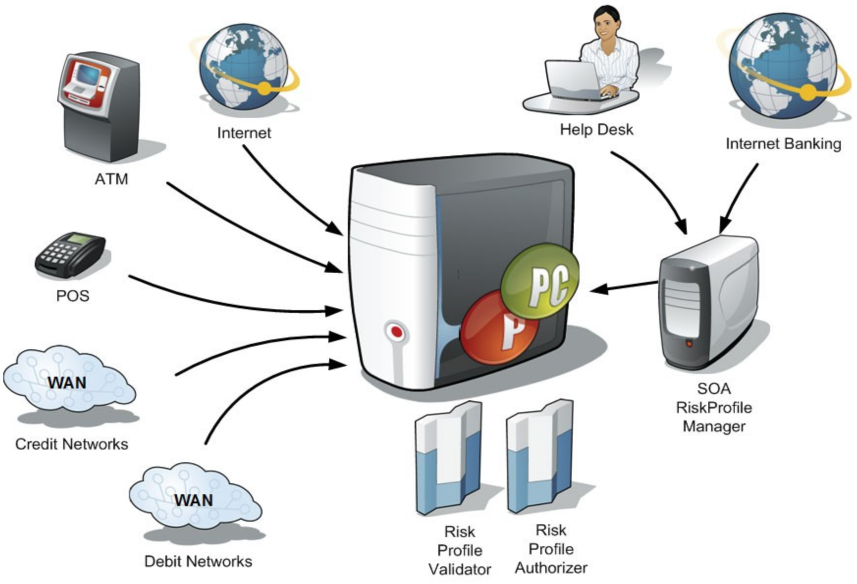
Risk Profile Manager is extensible by nature and can reach any channel to allow cardholders to use the one they're more comfortable with.

Integration with an issuer's internet banking, mobile banking, IVR or helpdesk can be readily implemented using Risk Profile Manager's SOA architecture. Issuers may elect to provide a simple ON/OFF interface to their customers or allow them to fully customize the behavior of transaction authorizations for ATM, POS and CNP environments.

An issuer may also elect to provide their cardholders with a lock-by-default option. When used, Risk Profile Manager does not allow any transactions to be authorized unless the cardholder that uses this option explicitly allows a transaction. After a predefined time period, Risk Profile Manager locks down the card again without any cardholder intervention.

Security Features

- ATM and POS lock-down. The cardholder may choose to allow or decline all transactions originating from ATM or POS terminals. If transactions are allowed, the cardholder may further specify whether to allow national or international transactions, or both. In addition, the cardholder may also define the maximum cash limit that will be allowed. Lastly, the cardholder may specify a date & time period during which transactions may or may not be allowed.
- Card-not-present lock-down. The cardholder has the option to allow or decline all transactions that originate from a CNP environment. If transactions are allowed, the cardholder may specify the maximum amount that can be authorized. Risk Profile Manager allows the definition of invalid authorization profiles that can proceed down to the merchant type level. The cardholder may specify the maximum allowable amount for CNP transactions. Lastly, the cardholder may specify a date & time period during which transactions may or may not be allowed from the CNP environment.



T: +30 210 364 9000
F: +30 210 364 9001
E-mail: info@codix.gr
sales@codix.gr

Address: 14, Solonos str.
Kolonaki, 106 73
Athens, Greece
Web: http://www.codix.gr/