

SecurLOCK™ Fraud Management Suite

The Advantage Network has the lowest fraud rates among all Visa debit issuers. Two factors contribute significantly to this accomplishment:

- The Advantage Network processes all disputes for all members in our network and receives all fraud notices. Because of this we are able to see fraud trends and common points of compromise before an individual institution would be able to spot them.
- SecurLOCK Fraud Management. This FIS Global product provides industry-leading fraud mitigation tools layered across all FIS payment card platforms.

SecurLOCK gathers acquirer and issuer transactions, strips identifying information, and feeds the data to a continuously updated neural network for scoring. This process improves fraud mitigation and results in fewer false positives for cardholders.

SecurLOCK develops a profile for each cardholder; spending habits are considered each time a transaction is scored. A specific transaction could be scored high or low depending on several additional factors such as merchant, whether the card was present or not, and the amount of the purchase.

There are two foundational products in the SecurLOCK suite of products in which all Advantage member institutions participate:

1. SecurLOCK BLOCK fraud rules are included in the scoring process and are also applied independently to each transaction. Rules are a fraud protection system which declines high-fraud-risk transaction authorizations, dynamically responding to emerging fraud schemes.
2. SecurLOCK Communicate
When fraud is suspected, the card is automatically blocked and a text, email or telephone call is generated to the cardholder. The automated calling system attempts to reach the cardholder at all available telephone numbers and can handle validating information from the cardholder, removing warm blocks on cards and verifying “unrecognized” transactions. In some cases, the card may be transferred to a fraud analyst for assistance.

A Fraud Alert Detail Report is sent via email to the issuer to advise of the actions taken after the system has attempted to reach the cardholder; this includes the case number, information on any card status change, whether the cardholder responded, and whether fraud was confirmed or not.

Daily and monthly reports are available and data is reported by BIN (card type) so the financial institution can isolate, interpret and react to specific fraud events. These reports are in addition to email notifications.

SecurLOCK monitoring is applied to all Advantage card products and all card activity including ATM, PIN Debit and signature transactions.

SecurLOCK Optional Services

❖ SecurLOCK Demand Custom Rules

Financial institution can order customized transaction rules to respond to their unique fraud experience. Rules are evaluated by the Risk Analytics Team and tested against live transaction data to ensure greatest fraud mitigation and minimize negative cardholder impact.

Rules will not transfer to the next year if they are not used.

❖ SecurLOCK Predict

A dedicated fraud analyst will perform ongoing fraud trend analysis to help the institution create a customized fraud strategy to address specific fraud activity. Monthly reports and fraud metrics reviews are provided.

❖ SecurLOCK Profile Debit

A profiling period will be provided to build accurate profiles. Profile Debit has two components:

- Predictive Merchant Profiling develops fraud scores specific to merchants based on global data including worldwide fraud trends and is updated weekly. High scoring transactions are reviewed by a Fraud Analyst.
- Predictive ATM Profiling includes global data to build ATM and cardholder profiles which improves fraud scores for PIN transactions. (includes PIN POS transactions)

❖ SecurLOCK Warranty

FIS provides a warranty to financial institutions against unrecoverable fraud losses of over \$50 per occurrence incurred through debit card fraud. SecurLOCK Warranty uses leveraged analytics in finding and detecting fraudulent card use; Fraud Analysts are able to identify and react to fraud faster, reducing card losses for the institution. Approximate implementation period: 15-30 days.

Per case and annual limits apply. Custom warranty limits can be requested; pricing will be adjusted accordingly by quote.

Program Exceptions: Employee theft or negligence, cardholder attempts to defraud the institution, friendly fraud, VIP card fraud and cards not reissued after a compromise.

❖ SecurLOCK Intelligence

SecurLOCK Intelligence is machine learning automation that takes the results of fraud investigations made by the FIS fraud analytics team and adjusts the scoring models daily. Updating models with greater frequency allows for new fraud trends to be incorporated as they are identified from around the globe. This is an added layer to the SecurLOCK Profile solution, which is a prerequisite to SecurLOCK Intelligence.

❖ SecurLOCK ATM Real Time Rules

FIS-defined rules are applied to on-us and foreign ATM transactions prior to being processed to mitigate the risk of fraudulent transactions and suspicious activity at the ATM. Email alerts will be sent to the institution when abnormal behavior is detected. Custom rules can also be created.

❖ SecurLOCK Equip

Cardholders can use a single mobile application to manage all aspects of their Advantage Checkcards, including taking an active role in fraud mitigation and detection. The mobile application is a “stand alone” product and is not integrated with an institution’s core or mobile banking product.

The financial institution benefits from reduced fraud losses, reduced call center costs, increased Checkcard usage and spend, as well as improved customer retention.

Cardholders can customize each card using the features and preferences below.

- **Switch card on/off** – Cardholders can lock or unlock cards with a single touch. Auto-lock turns on a card for a specified time or for a certain number of purchases, locking it afterward.
- **Control by location** – Cardholders can limit card activity by location, either by limiting card-present transactions to the location of the card or by limiting card usage to a region on a map. They can also turn on cards for international usage or deny international charges. This way, absence of a cardholder at a merchant location strongly indicates fraud, while the presence of a cardholder is proof positive of a legit transaction.
- **Control preferences** – Cardholders can limit merchant categories (grocery, retail, gas, travel, etc.), and transaction types (ATM transactions, online transactions, recurring charges, etc.) as well as set spend limits per transaction. They can personalize preferences according to their unique spending behavior.
- **Instant transaction alerts** – Cardholders can act instantly on real-time in-app transaction alerts. Higher cardholder engagement drives loyalty and increases card usage. (These transaction alerts are not related to SecurLOCK Communicate alerts which are generated if fraud is suspected.)
- **Self-service** – Cardholders can view available balances [if the FI sends Positive Balance Files to Advantage], analyze spending and manage transactions. Self-service increases cardholder satisfaction while lowering support costs.

Cardholders can register multiple Checkcards and multiple users can register a single card.

Cardholder choices do not override institution settings in Cardbase which means that daily spending limits and other settings (including status) in Cardbase cannot be changed by the cardholder. Information from Cardbase and SecurLOCK Equip or the core and SecurLOCK Equip is not shared.

Cardholders cannot set Lost/Stolen card notifications nor travel notification to the FI within SecurLOCK Equip; cardholders must still contact their institution to notify them directly.

The financial institution will have access to “mConsole,” an administrative tool to assist the cardholder with SecurLOCK Equip settings.

Approximate implementation is 12 – 14 weeks. There are two opportunities for customization in addition to the standard program. Pricing is available by quote.