How does Real-time Falcon differ from Online Falcon?

The difference between Real-time Falcon and Online Falcon is that Real-time Falcon can deny a transaction at the point of authorization before the fraudster completes the transaction. This proactive denial occurs as part of the authorization request response, and potentially reduces overall monetary loss due to fraud prior to the case being presented and worked by a Card Member Security Call Analyst.

With Online Falcon, transactions are scored after responding to an authorization request, a reactive approach. If the activity meets the criteria of Falcon Case Management rules, a case is created to follow up with the member only after completion of the purchase transaction(s).

What is a Real-time Falcon filter?

In order for a transaction to be eligible for real-time review, it must meet one of the following real-time filter criteria:

- Non-U.S. transactions — All dollar amounts for transactions originating outside of the U.S. (not equal to U.S. currency code 840)
- U.S. Transactions (must be U.S. currency code 840)
  - $100.00 - $199.99 from domestic merchants for six specific merchant category codes (MCC) which have a high frequency of fraud:
    - 5310 – Discount Stores (e.g.: WalMart, Target)
    - 5311 – Department Stores
    - 5411 – Grocery Stores, Supermarkets
    - 5541 – Service Stations
    - 5912 – Drug Stores & Pharmacies
    - 6011 – ATM Withdrawals
  - $200.00 or greater from a domestic merchant for all merchant category codes.

How much of the credit union's transaction volume will be impacted by Real-time Falcon?

On average, less than 1% of transaction volume is denied as a result of real-time review in Falcon.

How does Real-time Falcon functionality fit into a Risk Management Program for debit/credit cards?

As with existing neural network transaction scoring services, the real-time transaction analysis functionality should be viewed as complementary to other CO-OP Financial Services best practice risk avoidance techniques, such as: requiring card activation prior to first use, address verification, CV1 and CV2 verification, expiration date matching for authorization requests, as well as use of Verified by VISA and MasterCard Secure Code. Additionally, credit unions should establish daily limits on dollar and transaction velocity, monitor Falcon reports as well as the Cardholder Suspect Report and the Cardholder International Usage Report.

Does real-time Scoring that triggers a declined authorization also block the cardholder account from all further authorizations?

No. Unless a temporary block has been placed on the account, Real-time Scoring reviews each authorization separately. Therefore, subsequent authorizations could be approved or declined based on the criteria associated with each transaction. This allows high-risk transactions to be potentially prevented, but also allows subsequent non-high-risk transactions to continue to be approved until the case is reviewed by a Fraud Analyst.

If a member has received a real-time denial for a legitimate purchase, does Card Member Security need to be contacted so that the member can resume using their card?

If a transaction has been denied by Real-time Falcon and subsequently a case created, Card Member Security must be contacted either by the credit union or the member so that the transaction in question can be tagged as legitimate and the case closed to prevent additional real-time denials. Contact by phone is preferred so that the case can be updated immediately, allowing the member to use their card right away. However, Card Member Security can also be contacted to resolve cases by email at falcon.supervisor@co-opfs.org.
If a transaction meets Real-time Falcon filter criteria, will Falcon deny it?

A transaction must meet the Real-time filter criteria and meet the criteria of a Real-time rule in order to be denied at the point of authorization by Falcon. Falling within one of the filter categories does not automatically deny a transaction.

After a Real-time Falcon case has been resolved and confirmed legitimate, how long is it before a member can use their card again?

After tagging the questioned transaction(s) as “legitimate,” closing the Falcon case and removing any temporary blocks, the member’s card should be available for use again. Time elapsed is usually no more than 5 minutes. Removal of a temporary block only will not return the card to “available-to-use” and transactions could still be denied by Real-time Falcon. To make the card available again, the case must also be closed as “No Fraud.”

If there is a Real-time Falcon case created that is closed as “Confirmed Legitimate,” can a member be denied by Real-time again? What happens if one or more subsequent transactions meet one of the filter criteria and a Real-time Falcon rule?

Once a Real-time Falcon case is closed as “Confirmed Legitimate,” the impacted card is exempt from another real-time denial for 14 calendar days. This helps ensure a member is not excessively impacted by real-time denials. While a transaction cannot be denied by Real-time Falcon for 14 days, a card is only exempt from Case Creation for 7 calendar days. Therefore, a case could be created for review a week after a previous case if there were further suspicious activity, but the member would not experience another real-time denial within the 14-day period. This procedure protects members from being denied so frequently as to minimize their ability to use a card at the Point of Sale.

Will a credit union have more Falcon cases when it moves to Real-time Falcon?

No. Cases that qualify for Real-time Falcon are of the highest risk so they already qualify for review through Case Management whether they (a) fall within a high score range or (b) meet criteria for a Flash Fraud rule for a known trend. No additional case volume is created as a result.

How much of the credit union’s transaction volume will qualify for real-time review?

On average, 10% of transaction volume meets the filter criteria and qualifies for real-time review in Falcon.

When going on Real-time Falcon, should a credit union delete current Authorization Blocks?

There are a couple scenarios where a credit union should retain use of Authorization Blocks.

1. If the Authorization Block is working successfully and not negatively impacting members, a credit union should consider leaving it in place. Keep in mind that Real-time Falcon only denies transactions with high scores, but this may not be the case for all transactions that fall under the criteria of an Authorization Block.

2. If a credit union discovers multiple members disputing items from one or more merchants, but they did participate in transacting business with them, this is not fraud, so Real-time Falcon is not the place to block these transactions. If a credit union wants to prevent transactions for a specific merchant, they should continue to use Authorization Block.

When a credit union goes on Real-time Falcon, does it require use of AP (CO-OP Authorization/Cooperative Authorization) for authorization decisioning, and eliminate use of a credit union Host Processor?

CO-OP Authorization or Cooperative Authorization is not required for use of Real-time Falcon. A credit union can continue using Host Authorization and still take advantage of Real-time Falcon. The authorization level for Real-time Falcon is the same as Online Falcon, Host Authorization with a cardholder file.

Are any transactions excluded from Real-time Falcon review?

The following scenarios could prevent activity from being reviewed in real-time:

- A card has an active VIP Authorization Block Bypass Record in CO-OP Concierge, or
- A case that was created due to a Real-time Falcon denial and recently closed as confirmed “Legitimate” is not eligible for another real-time denial for 14 days. This timing aims to prevent excessive impact to members.
When does a record in CO-OP Concierge for a Falcon Travel Notification or VIP have impact on Real-time Falcon review?

CO-OP’s staff does not review or see VIP Authorization Block Bypass records. However, to prevent member inconvenience, any member with an active VIP Authorization Block Bypass record in CO-OP Concierge is exempt from Real-time denial rules as well as any active Authorization Blocks placed by the credit union.

An Active VIP Bypass record in CO-OP Concierge will only prevent a transaction in Real-time from being denied. If a bypass record is Pending Active, Cancelled or Closed, a transaction can still be denied in Real-time Falcon if it meets both the Real-time filters and a Real-time rule.

If there is an active travel record for a card within the Falcon Travel Notification and the credit union uses Real-time Falcon, transactions on that card will still be scored using the Real-time rules, but they will NEVER be denied by Real-time Falcon. Transactions on that card will be treated as if scored by Online Falcon, and the appropriate case creation will take place. A Travel Record becomes “active” on the first day travel was scheduled to begin within the record. The Record stops being active 7 days after travel was scheduled to end within the record. So if a member has a travel record that says he/she will be gone from May 1 through May 7, the record will be considered “active” and Real-time denials will be suspended from May 1 through May 14.

NOTE: Travel notes are updated by batch to FIS once a day. In the example above, if a credit union were to enter the travel note prior to 5/1, all should work as described above. However if the credit union entered the travel note on 5/1 (the same date the travel begins), it would not update and forward the information to Falcon until later that evening (approximately 7 pm PT). Therefore, the Travel Record would not necessarily prevent a real-time denial until the batch file is accepted by FIS.

Is there a location where a credit union can see all its daily transactions denied by Real-time Falcon?

The Suspect Fraud Transaction Report includes a section for Real-time denials. They are identified in the group named “VJ – Denied by Real-time Scoring.” This is a daily report.

Are Real-time rules and Case Management rules within Falcon the same thing?

Separate rule bases are maintained to support case creation (for Case Management) and authorization denial (for Real-time). There is some overlap because all transactions denied by Real-time Falcon will also create a Falcon case to be worked by Card Member Security.

Note: CO-OP Risk Analysts constantly monitor fraud patterns and trends and work with various partners such as FICO to analyze fraud trends. Because of shifting trends and emerging fraud patterns, both Real-time rules and Case Management rules may be adjusted to meet current fraud detection needs.

Should a credit union use marketing materials to educate members about fraud monitoring and let them know that transactions could be denied by Real-time Falcon?

While member service and convenience to cardholders is a critical factor that must be balanced against fraud prevention, experience has shown cardholder inconvenience to be minimal. Communicating with cardholders and emphasizing the protection of their accounts goes a long way toward minimizing cardholder complaints. Credit unions are encouraged to consider proactive marketing measures to help educate cardholders about the additional security features in place to protect them. This could include statement messages, branch brochures, and website updates to name a few.

To assist credit unions, marketing communication materials are available for members to download at no fee from CO-OP. Visit the following link—all that is needed is your User ID and password for the CO-OP Extranet to gain access.

http://co-opfs.org/public/company/marketing/marketingConsumerEducation.cfm

How can a credit union identify when a transaction is denied by Real-time Falcon?

Credit unions are able to review cardholder authorizations in Data Navigator and will see an Action Code value of “A37” when a transaction was declined due to Real-time Scoring.
The easiest way to contact our credit union members is via their cell phone, however the CO-OP Cardholder File only contains segments for home and work phone. With Real-Time Falcon how can the credit union ensure members will be contacted via their cell phone?

The CO-OP Cardholder file only contains fields for a home or work phone number, however the phone numbers provided can be any number including the member’s cell phone number. CO-OP recommends that the most likely number to help ensure contact is submitted in the phone number segments.

Why is CO-OP moving our credit union to Real-time Falcon?

Today's fraud environment is exponentially worse and CO-OP has researched the best ways to beat it. With the increasing sophistication of fraudsters, this is truly a Fraud 2.0 world and previous solutions are not the best tool for catching today’s fraud. At this time, Real-time, with its proactive approach to deny transactions before they happen, is the recommended solution for credit unions.

When will the credit union gain access to Real-time Falcon?

CO-OP will turn Real-time Falcon on for credit unions on July 25, 2011. If the credit union wants it turned on sooner than that, they can submit a work order through the extranet.

Only transactions that meet the filter criteria will go through Real-time Falcon, and the rest go through Online Falcon score review.

Do credit unions pay the Real-time Falcon Scoring cost for all transactions?

Once on Real-time Falcon, all transactions are screened according to Real-time filter criteria before they are sent for review within the Real-time Falcon Denial rules. Therefore, the Real-time Scoring cost applies to all transactions. Typically credit unions experience a return on investment with fraud savings in the first three months of running Real-time Falcon.

For example, almost one third, or almost $1,000,000, in fraudulent transactions were denied in May due to real-time monitoring. The average credit union saves $4 in fraud losses for every incremental $1 in Real-time Falcon costs, a huge return on investment.

When a Real-time Falcon transaction scores 950 or greater, a case is created. Is the card also blocked?

A card is not automatically blocked. A case must be presented to a Fraud Analyst so that a card can be blocked if necessary. In the example provided, if an attempt to contact a member was not successful, the card would be statused with a temporary block since the case included a transaction that scored over 900.