Risk Engine & Case Manager

An additional layer of security within your online banking to reduce the risk of fraudulent activities and increase customer advocacy. The Risk Engine & Case Manager is an Increased Authentication solution that uses an advanced Bayesian algorithm to actively detect and prevent suspicious online activity.

HOW DOES IT WORK?

By creating usage profiles for each customer that includes device, location and other behavioral patterns, the Risk Engine evaluates and scores each customer transaction against their individual usage profile. As it logs transactions, the Risk Engine scores each from zero to one thousand. A score of zero is the least suspicious, and one thousand is the most.

Suspicious transactions can trigger additional authentication steps to verify the user's identity, or be forwarded to the Case Manager for review by your fraud prevention team, or be blocked all together.

The Risk Engine & Case Manager offers three different models to detect and prevent fraud

1 **Fraud-Reactive**

2 **Fraud-Fighter**

3 **Fraud-Conqueror**

Fraud-Reactive

A good analogy for the Fraud-Reactive model is a surveillance camera setup for your online banking; it is always recording activities and when a fraud event happens you can go back and review the tape. Or you may watch the camera from time to time, and if you see something suspicious you can take preemptive measures to prevent fraud from occurring.

By having your customers activity tracked in a convenient format, you can investigate suspicious online banking behavior in their accounts using the Lookup User tab. You may also look at all activities the Risk Engine deems suspicious by using filters in the Research Activities tab.

By default, clients are set up with the Fraud-Reactive model. With the Fraud-Reactive Model, the Risk Engine and Case Manager does not put transactions on hold, nor does it create cases for analysts to review.

For more robust fraud prevention capabilities, we recommend...

Fraud-Fighter

Continuing with our surveillance camera analogy, the Fraud-Fighter model is like a security guard watching your camera footage 24/7. When it sees something suspicious, it takes note of it for you to look at.

With the Fraud-Fighter model, you can add policies to automatically create cases whenever pre-set conditions are met. These cases are reviewed by your organization's analysts, who can then take appropriate actions to prevent or reduce fraud losses. In order to have a meaningful impact on fraud losses, this model requires your staff to actively use the Case Manager daily.

Example policies

Login: Aggregator Bypass - an aggregator like mint.com is being used to log into the users account: Allow.

Login: Critical Risk - user has logged in with a risk score greater than 900: Ask challenge questions, and create a case.

Login: High Risk - user has logged in with a risk score greater than 800: Challenge, and create a case if challenge unsuccessful.

Login: Medium Risk - user has logged in with a risk score greater than 500: Challenge.

Login: Low Risk - user has logged in with a risk score of less than 500: Allow.

Electronic Bill Payment: Payment Sent - user has sent a bill payment: Allow.

Electronic Bill Payment: Add Payee - user has added a new bill payment payee with a risk score less than 700: Allow.

Electronic Bill Payment: Add Payee High Risk - user has added a new bill payment payee with a risk score greater than 700: Allow, and create a case.

e-Transfer: Payment Sent - user has sent an Interac e-Transfer®: Allow.

e-Transfer: Recipient Added - user has added a new Interac e-Transfer recipient with a risk score less than 700: Allow.

e-Transfer: Recipient Added High Risk - user has added a new Interac e-Transfer recipient with a risk score greater than 700: Allow, and create a case.

Inter-member Transfer: Low Risk - user has sent an inter-member transfer with a risk score of less than 700: Allow.

Inter-member Transfer: High Risk - user has sent an intermember transfer with a risk score of greater than 700: Allow, and create a case.

User Enroll: - user has enrolled in Increased Authentication: Allow.

Profile Activity: Profile Update Low Risk - user has made a profile change with a risk score of less than 700: Allow.

Profile Activity: Profile Update High Risk - user has made a profile change with a risk score greater than 700: Allow.

Profile Activity: Password Change - user has changed their password: Allow.

Profile Activity: Challenge Questions Changed - user has changed one or more of their challenge questions: Allow.

Fraud-Conqueror

The final analogy would be if the security guard received automatic notifications before someone leaves the premises. The video camera would automatically send a notification the moment it detects a fraudulent pattern.

This model is not yet available to clients. The Risk Engine calculates risk scores based on statistical analysis, constantly improving the accuracy of these scores each time it calculates. Once the risk scores are accurate enough (measured by looking at the correlation between risk score and actual fraud) then the Case Manager will be able to put transactions on hold without human intervention, stopping fraud as it happens. When clients actively mark cases as fraud in the Risk Engine & Case Manager, it helps improve the accuracy of the analysis.

For an improved customer experience & superior fraud prevention, we recommend...

Risk-Based Authentication

The Risk-Based Authentication improves the customer's login experience and their online banking security, and it makes the Fraud-Reactive, Fraud-Fighter and Fraud-Conqueror models even more effective.

Improved Customer Experience

Historically, a device-based authentication policy required customers to answer challenge questions when they log in with a device or browser that they haven't used before. This policy results in a challenge to 30% of your customer logins. With the upgrade to Risk-Based Authentication, challenge questions are only asked for logins with a highrisk score. As a result, the challenge rate can drop to 3 to 5%, while maintaining or even reducing fraud levels.

The experience of your customers is improved due to the reduction in frequency of challenge questions and fewer account lockouts. Your customers will spend less time on the phone to your staff, which results in reduced wait-times for them and/or reduced call center costs for you.

Enhanced Security

Less complex malware will only steal the data that a customer enters into their browser. By reducing the frequency of challenges, we also reduce the opportunities for fraudsters to get the answers to the challenge questions.

What impacts are there to your customers?

- They may notice that the "remember my computer" option has disappeared from the online banking login screen.
- They may find that challenge questions are asked less frequently.
- This may generate some queries from customers after the upgrade, but the volume should be lower than it is currently experienced today with lockouts.

Easy to Implement

The Risk Engine & Case Manager does not require additional hardware or software, and is designed to work with all banking systems. There is no impact to your customers during deployment.

More Information

Contact your Central 1 Relationship Manager at: relationshipmanagement@central1.com

Order Today

To get started today, place your request with Service Now.

Support

MemberDirect_support@central1.com
T 1 888 889 7878

central 1
central1.com