Cyber Security

Risk & Fraud Services

In today's landscape, attempts at fraud are rampant, and you have legitimate concerns when it comes to your duty to protect customer accounts. Threats of identity theft, phishing, viruses and a whole host of other undesirable encroachments are always lurking. Our suite of Risk and Fraud Services offers you 11 detection and protection solutions to help ensure security and customer confidence.

FOR YOU:

Umpire/PAC Blocker

Prevent fraudulent account access by locking accounts with suspicious login attempts.

- Lock accounts after three failed login attempts until the following calendar day
- Protect yourself from brute force attacks - if more than 50 failed logins with the same PAC occur in a 24-hour period, the Umpire will lock any accounts with that same PAC until the following calendar day.

Increased Authentication with Risk Engine & Case Manager

The Risk Engine uses an advanced Bayesian algorithm to evaluate customer patterns, and it notifies you by using the Case Manager if it detects any suspicious online activity during login and other transactions.

- Delivers an additional layer of security by asking members to step-up authentication via 2-Step Verification or by answering challenge questions. In addition to their unique online banking password, in case their login is seen as risky.
- Enables you to proactively identify fraudulent transactions.

reCAPTCHA

Protect your site from spam and abuse by verifying that your login activity is not being generated by automated software.

- Advanced risk analysis engine and adaptive challenges that prevent abusive activities while letting valid users pass through with ease.

Botnet

Block malicious login attempts by automated software and human-driven "sweat shop" attacks using the latest machine learning and next-generation bot detection technology.

- Control bot traffic, regulating site access for both good and bad bots
- Get the full picture and proactively protect customer accounts, with deeper reporting into blocked login attempts and their source
- Ensure valid users always have access to their accounts – even during an attack
- Improve user experience by eliminating the need for customers to complete verifications, like challenge images, to access their accounts
- Never fall behind the attackers with cutting edge AI that learns from each malicious login attempt

Enhanced PAC

Strong PAC

With the implementation of Strong PAC, opt to move from numeric to alphanumeric PAC configurations.

Extended PAC

Allows you to create PACs up to 30 characters long, instead of the standard maximum 8.

Weak PAC Detection

Allows you to display the strength of a new PAC in real-time to prevent the creation of weak PACs.

- Forces existing customers with a weak PAC to update to a strong PAC at their next login.
- Protects weak PAC customers by not allowing login during times of increased threat.

RSA® FraudAction

Protect your customers and your organization against phishing, Trojan attacks, social media threats and rogue mobile apps using the all-inclusive RSA FraudAction threat management service. RSA FraudAction:

- Identifies a new phishing attack every 30 seconds
- Blocks 96 percent of malicious sites in 30 minutes or less
- Has shut down more than two million cyber attacks globally

FOR YOUR CUSTOMERS:

ID Verification

Secure identity verification is triggered when a user wants to enrol in digital banking, or has forgotten their PAC or the answers to their challenge questions. Fast & convenient way to send messages to your customers.

- Allows users to self-serve, reducing staff time requirements.

Lock'N'Block™

Customers can take control of their own security by locking their debit card and blocking transactions anytime they feel their debit card has been compromised, through their online banking account or mobile device.

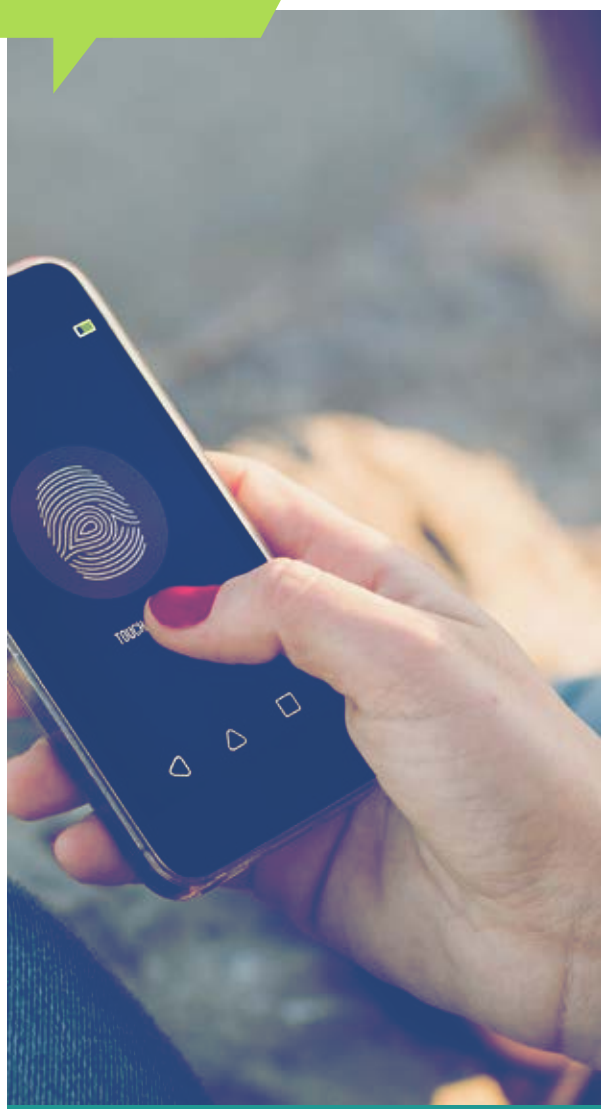
- Allows customers to independently lock their debit card and block transactions
- Eliminates the need to contact the credit union call centre or go into a branch in the event of a compromised card

Alerts

Automatically send a text message (SMS) or email to immediately notify your customers of insufficient funds, scheduled payments, potential compromises, and other types of account conditions.

- Fast & convenient way to send messages to your customers
- Enables your customers to stay on top of their finances from wherever they are
- Provides an added level of security by informing customers of suspicious or fraudulent transactions

Our suite of Risk and Fraud Services offers you 11 detection and protection solutions to help ensure security and customer confidence



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

Support@central1.com
T 1 888 889 7878

central 1
central1.com