FedNow 24/7 INSTANT PAYMENTS

THE FEDERAL RESERVE Financial Services

PROTECTING AGAINST INSTANT PAYMENT FRAUD

FedNow® Service risk management capabilities

As with any type of payment, the potential for fraud exists with instant payments. It's important for financial institutions and others in the FedNow Service ecosystem to work together to combat fraud.

Financial institutions are the first line of defense against instant payments-related fraud. As they prepare for the FedNow Service, participating institutions will want to evaluate their own fraud management approach and consider taking steps to help protect themselves and their customers.

To support and complement financial institutions' own fraud mitigation efforts, the FedNow Service offers fraud management capabilities and enable features to help protect against threats. Future releases of the service will add even more capabilities.

TRANSACTION LIMITS AND NEGATIVE LISTS

The following capabilities are available to participating financial institutions at the launch of the FedNow Service.

Network-level transaction limits
The maximum amount per transaction a financial institution can send over the FedNow Service – amount set by the Federal Reserve.

Participant-level transaction limit
Participants can set a lower transaction limit for credit transfers they initiate based on their organization's risk policies.

Participant-defined negative lists
Financial institutions may specify suspicious accounts their organizations can't send to or receive from.

PARTICIPANT REPORTING AND NOTIFICATION OF FRAUD

When FedNow participants confirm a transaction is fraudulent through their own investigation, they are required to report it to the FedNow Service. This information is used to strengthen the FedNow network and support counterparty fraud mitigation processes.

RISK MANAGEMENT AND ERROR RESOLUTION

FedNow participants can configure preferences and use ISO® 20022 messages to help with their efforts to mitigate fraud and to resolve errors.

Participation type

The FedNow Service offers different ways to participate in the service so that participants can enable the options that best match their needs and risk profile. For example, financial institutions may choose to support customer credit transfers, but elect not to support liquidity management transfers.

Accept without posting

Participants may submit an "accept without posting" status back to the originating financial institution indicating that further information is required with respect to compliance considerations before accepting the payment.

Request for information

Financial institutions may request another FedNow participant provide additional information on a transaction or request for payment message – for example, if the receiver financial institution would like to request further details about a sender.

Return request

Financial institutions may submit a "return request" message to request another FedNow participant return the amount of a transaction identified as fraudulent.

INFORMATION SECURITY

Security is foundational to the FedNow Service and the Federal Reserve Banks have designed the service to protect data at each step, aligning with industry best practices. The following are a few key security measures in place.

Digital signatures

- The FedNow Service requires messages exchanged with participants to be cryptographically signed to verify the integrity and authenticity of messages.

Data encryption and tokenization

- Data in the FedNow Service environment is encrypted in transit and at rest.
- Certain sensitive data is tokenized.

Authentication and authorization

- All connectivity into the FedNow Service is mutually authenticated.
- User interface via FedLine® Solutions access is protected by multi-factor authentication.
- Throughout the system, role-based access controls and separation of duties enforce least privilege principles.

YOUR ORGANIZATION IS THE FIRST LINE OF DEFENSE

Ultimately, the best defense includes multiple layers of safeguards to *prevent* fraud from occurring in the first place, *detect* it when it happens, and *mitigate* the financial and reputational impacts of fraud. In addition to understanding and considering the FedNow Service capabilities, your organization can take the following steps to strengthen your overall fraud management strategy.

UNDERSTAND the basics of instant payments and fraud

The speed, finality and always-on nature of instant payments can pose unique challenges when it comes to fraud prevention and detection. Learn more in our Fraud and instant payments: The basics article.

ACTIVATE your fraud management team

- Get your fraud management experts – whether in house or outsourced – involved in plans early. They'll need to become familiar with the implications of instant payments so they can evaluate your current processes, procedures and systems, and advise on an approach for enhancing your defenses.
- In this dynamic environment, it's useful to stay informed of industry best practices and Federal Reserve Bank expectations to help ensure your programs evolve as threats and approaches change.
- Consider how to monitor transactions 24x7x365 to help mitigate risk.

REVIEW and upgrade your systems as needed

- Look at your systems to ensure that robust account opening procedures, strong user authentication practices at login and continual verification of user contact information (email, mobile numbers, etc.) are in place.
- Take steps to prevent and mitigate synthetic identity fraud using detection and prevention approaches and technologies.
- Add suspicious accounts and aliases to a watch list to block potentially fraudulent transactions before the funds leave your institution.
- Determine what systems upgrades are needed to analyze incoming transactional data in real time, 24x7x365, to help prevent fraudulent transactions from completing.
- Systems designed to combat fraud involving payments that are cleared and settled in batches on predictable cycles may need updates to address fraud involving payments that clear and settle immediately.

ENLIST your customers in prevention

Educate your customers on how to identify fraud attempts and protect their personal data. Examples include:

- Tell customers you will never ask for their login information over phone, email or text.
- Encourage strong authentication mechanisms for different accounts.
- Guide customers to enable alerts related to transactions in their accounts and educate them on potential scams.

TALK with your vendors about tools to improve detection

- Talk with your vendors and technology partners about new approaches such as applying real-time fraud detection capabilities and achieving a comprehensive view of transaction patterns across all payment types.

CLASSIFY fraud to strengthen mitigation efforts

Explore the FraudClassifier℠ model, which enables organizations to systematically classify fraud involving payments.

- Enables organizations to classify fraud involving payments.
- Allows those in the payments industry to speak the same language on fraud.
- Leads to holistic view of fraudulent events, which can help with a more strategic approach to fraud management.

READ our Get ready for instant payments: Fraud edition article for more information.

Visit FedNowExplorer.org for more resources to help you prepare for the FedNow Service.