

**SPOTLIGHT ON:
ADVANCING SAFE PAYMENTS**

Managing Fraud Risk

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 payment-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 enables features to help protect against threats. Future releases of the service will add even more capabilities.

RISK MANAGEMENT CAPABILITIES

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

**Network-level transaction limits**

The maximum amount per transaction a financial institution can send over the FedNow network. (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.

Correspondent net send limits

A correspondent with an active FedNow participant profile can establish a net send limit for each of its respondents at the financial institution level to help manage liquidity risks.

Participant-defined negative lists

Financial institutions may specify suspicious accounts their organizations can't send to or receive from.

Account activity threshold functionality

Participants can define value and velocity thresholds by customer segment to fit their unique business needs and risk tolerance.

**CURRENTLY
IN PILOT**

Network Intelligence API

Sending financial institutions will be able to request information (data insights) about a receiver account prior to submitting a transaction to the FedNow Service.

PARTICIPANT REPORTING AND NOTIFICATION OF FRAUD



When FedNow participants have reason to suspect a transaction is fraudulent through their own investigation, they are required to report it to the FedNow Service. The fraud reporting capabilities provided by the FedNow Service enable financial institutions to report fraud as soon as they have reason to suspect a payment is fraudulent, even if there are fewer details available initially, to help contain and prevent the spread of threat actors. By working together to combat common threats, all parties can benefit from safe and secure instant payments. [Learn more in our fraud reporting article.](#)

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 that 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 that another FedNow participant return the amount of a transaction identified as fraudulent.

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 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 system 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 [FraudClassifierSM model](#), which enables organizations to systematically classify fraud involving payments, and the [ScamClassifierSM model](#), which supports improvements to scam reporting, detection and mitigation. [Explore how the two models can be leveraged together.](#)

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



CHAMPION fraud and scam prevention measures internally

- Measure changes in fraud and scam rates, as well as fraud and scam types, to see which categories represent the most serious threats to your institution and your customers.
- Leverage these insights to inform and evolve your fraud and scam prevention strategies and procedures.
- Document and evangelize what you are doing, to raise awareness and align the organization.
- Revisit these plans each time there is a meaningful change in the rates or types of fraud and scams being perpetrated against your organization and customer base.



DEVELOP and implement a mule-prevention strategy

Mule accounts are major enablers of fraud and unfortunately criminals have many ways to obtain mule accounts, whether buying accounts, coercing victims to use theirs, or opening accounts using stolen and synthetic IDs.

- Protect your institution's reputation and help to root out fraud in payment rails by developing and documenting a strategy to monitor for mule activity on your accounts.
- Collaborate across BSA/AML, Account Opening and Fraud functions to share information and develop a holistic view, which will help identify, investigate and close these accounts most rapidly.



UNDERSTAND the fraud reporting requirements for the FedNow Service

- Review the fraud reporting capabilities provided by the FedNow Service.
- Establish an internal process to report fraud as soon as there is a reason to suspect a payment is fraudulent.



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.

This guide may and is likely to change from time to time, including as the Federal Reserve Banks obtain feedback from various stakeholders. The Readiness Guide is not an agreement with the Federal Reserve Banks and is not necessarily reflective of the final terms, operating procedures or other documentation for the FedNow Service.

The Federal Reserve Financial Services logo, "FedNow," "Fedwire" and "FedLine" are service marks of the Federal Reserve Banks. A list of marks related to financial services offered by the Federal Reserve Banks is available at FRBServices.org. Marks of any third parties identified in this document are owned by their respective holders.