Financial Institution Safety & Security FAQs

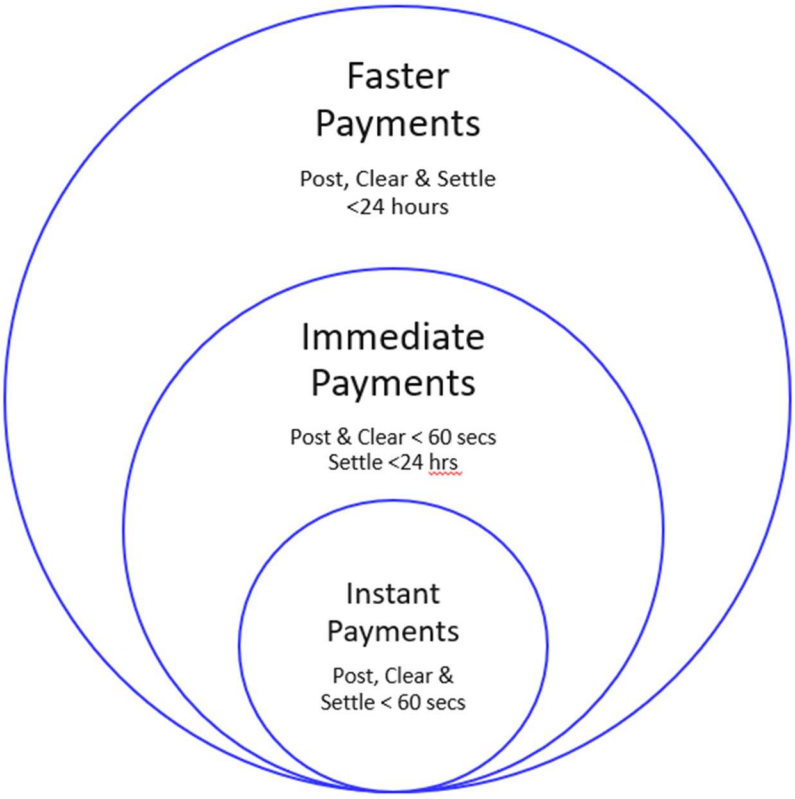
What is a faster, real-time, or instant payment?

To date, the industry has used the terms faster, real-time, and instant payments as if they were interchangeable. The term "faster payments" is broadly used in the payment industry to indicate simply that increased speed, convenience, and accessibility are essential features for the future of the payment settlement system. In addition to the expedited movement and availability of funds, the more efficient and transparent provision of information about the transaction is a key component of the faster payments value proposition. The *Faster Payments Playbook for Financial Institutions* offers 3 definitions that help focus a discussion of "faster payments."

Same Day – a payment for which the effective entry date is the same as the date on which the entry was initiated by the sender.

Immediate - can be sent 24 hours a day, seven days a week (subject to the service offering of the financial institution) and receives a response to the sending bank within 15 seconds, confirming that the receiving bank has accepted or rejected the payment.

Instant – an electronic retail payment solution available 24/7/365, resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payor (within seconds of payment initiation).



*Source – Faster Payments Playbook https://fasterpaymentsplaybook.org/

However, different networks are offering options that differentiate among those terms based on their handling of posting, clearing, and settlement. Javelin Strategy[1] has suggested the following delineations:

- Payments which post, clear, and settle within 24 hours (e.g., Same Day ACH). These payments will be referred to as *faster payments*.
- Payments which message or post in less than 60 seconds, clear, and settle within 24 hours (e.g., Mastercard® Send, Visa® Direct, Zelle®, Venmo, PayPal). These payments will be referred to as *immediate availability payments* in this document. (These might also be called *deferred settlement*, because although funds are available to the receiver right away, settlement between financial institutions may take place later.)
- Payments which post, clear and settle in less than 60 seconds (e.g., The Clearing House RTP®, Mastercard® Vocalink, and the forthcoming FedNow℠ service). These payments will be referred to as *instant payments* in this document.

Based on these definitions, faster payments as a term covers all the payment networks listed above, but a faster payment is not necessarily an immediate availability or an instant payment.

What is the impact of faster payments on my financial institution's safety and security posture?

Faster payments' safety and security will require analysis of existing institution postures. Relevant areas could include:

- **Participation Requirements** - A financial institution's ability to participate in faster payment networks is based on multiple factors including deposit insurance and consideration of its business practices. Networks may also review formal enforcement actions as part of their due diligence process before approving a financial institution as a participant.
- **Risk Management** - Faster payments can help reduce cash flow risk by shortening the length of time between transaction and settlement. Risks should be reviewed in the faster payment context, with the opportunity to add additional controls when appropriate.
- **Security Controls** - Consumer education, vetting user identity and use of a fraud engine are starting points for a layered security posture. Control monitoring, velocity settings and flexibility to change are key elements of success as fraudsters and scams are detected.
- **Settlement Approach** - Settlement occurs at different times for different networks depending on network setup of participant financial institutions. A settlement and reconciliation process that is sensitive to these differences is critical.
- **Resilience** - Institutions should consider how they will monitor uptime and service levels on payments infrastructure that must be available 24/7/365.
- **End-User Data Protection** – Institutions should balance the convenience of storing user data for payments versus privacy regulation compliance.
- **Sender Eligibility -** Financial institutions must evaluate senders for eligibility to access a faster payments platform.

[1] Source: Javelin Strategy & Research, 2019

- **User Authentication** - Verification of the sender's identity during the enrollment and at transaction time is critical to minimizing an institution's risk.
- **Receiver screening** – Establish review processes and consider account validation for payment recipients to better understand payment patterns and mitigate the risk of mule accounts and account takeover.
- **Sender Authorization** – Financial institutions must ensure that eligible users are appropriately authenticated prior to providing payment authorization.
- **Payment Finality** – Some faster payment networks are good funds, credit push only. Payments made through these networks may be considered irrevocable under the network rules. Financial institutions should educate customers when payments may not be able to be recovered in the event of a user error.
- **Fraud Information Sharing** - Information sharing can help keep fraud from spreading. This can take place between departments, institutions, and the payments networks. The institution should review how this takes place today for other payment types and incorporate faster payments into their current strategy.
- **Disputes** – While immediate availability and instant payment transactions are generally irrevocable, support for dispute management may still be a requirement under network rules. Institutions must decide how these good faith dispute processes will be managed. For each new network, financial institutions must understand how inter-participant communication will take place.

What is the impact of faster payments on my institution's operational processes?

Operations teams will need to work closely with their business partners to determine how faster payments will affect volumes across each of their payment methods and even across payment channels (i.e., online, mobile, branch-initiated, etc.). In addition, they will need to review operational models for additional payment settlement windows, and possibly assess the impact of instant settlement. Different customer types may continue to maintain regular business hours for conducting payment transactions, while others will conduct payment activities at times more convenient to them.

Financial institutions should think through customer needs that impact operating and coverage models, including:

- Determine if account edits currently supporting other payment types can be leveraged for faster payment network transactions
- Consider what fraud reviews can be performed prior to transaction initiation to minimize analysis during a faster payment transaction.
- Review dispute resolution processes
- Create a strategy for transaction dollar limits that addresses risk while considering customer goals
- Evaluate call center staffing

Institutions should also consider how faster payments will affect their current reporting and reconciliation processes. With a 24/7 system, the operations team should examine their existing reporting timelines and assess how to best incorporate new reporting based on established windows.

With the addition of each new faster payment product, compliance teams must consider whether disclosures and account agreements need to be updated for consumer and business accounts, and how new payment methods fit into the posting order disclosures.

Finally, if financial institutions outsource operational activities, they should be prepared to assess third parties providing those services as part of their formal vendor assessment process.

What is the impact of faster payments on my financial institution's liquidity?

Some new payment network transactions may affect liquidity immediately and require ongoing funds management, whether by the financial institution or a funding agent, to ensure that the appropriate levels are maintained in addition to reserve requirements. Organizations may find the need to increase or decrease reserves to accommodate deposit outflows or inflows to avoid 1) additional costs of borrowing from other banks or corporations, 2) selling securities, 3) borrowing from the Fed, or 4) calling in or selling off loans.

Historical information and trends are important to predict impacts, as well as potential limits on funds that may be sent from a financial institution.

Should my financial institution perform additional risk management reviews when accounts are upgraded to allow sending of faster payments?

Yes. Institutions will need to make sure that additional risk management reviews occur with the addition of these new payment products. Financial institutions should ensure products, clients, and transactions are approved based on predefined risk-based rules. Enhanced due diligence may be required for certain account holders.

Are the reviews of senders and receivers of faster payments different? If so, how?

Yes, there are different goals when reviewing senders and receivers of payments. While the best way to prevent fraud in environments where payments processing and posting speed increases is to make payment initiation more secure, that only applies to payment senders.

Institutions should also consider the review of payment recipients. For example, a repeated payment between parties poses less risk to the institution than a new one. In the case one party to the transaction is not an account holder at that institution, the institution may have less data to analyze so the rules for review will likely differ.

What should my financial institution do to educate customers on safety for faster payments?

Key categories financial institutions should educate customers on include:

- Considerations before making a faster payment
- Consumer protections in place for their accounts
- How the safety/security of faster payments may or may not differ from more traditional payments
- Actions to take on the loss of a mobile phone
- Steps to follow if a faster payment is made to the wrong person
- Steps to follow if a faster payment that was not authorized appears on their statement

What should my institution know about fraud rules/requirements across networks?

Each network has its own rules framework which addresses fraud rules/requirements. Typically, these requirements cover:

- Authentication requirements
- Fraudulent transaction reporting

- Risk monitoring and transaction review and interdiction
- Use and maintenance of negative lists, restrictions, limits, and velocity settings

Institutions must refer to the fraud and rules for each network and should consider accommodating these requirements within current processes. In general, faster payments do not introduce new fraud prevention requirements that would not already be addressed within an institution for other payment types.

How should my institution think about authentication with respect to faster payments?

FFIEC guidance specifically calls for multi-factor authentication of users engaged in a high-risk or high-value transaction. The need for authentication can also apply to administrative functions: creating and managing user accounts for a commercial banking environment, managing user transfer limits, or in online bill pay scenarios such as entering information for a new online biller.

What should my financial institution consider when reviewing consumers and businesses for risk?

As part of the institution's risk review for new products, it is important to review new products and use cases for suitability for different customer types. For example, does a business have a need for a specific type of faster payment product? Should the product be offered to all customers by default? What is the institution's risk appetite for a product, and which customer segments can use the product appropriately?

How are my KYC requirements impacted by faster payments?

The speed and ease of faster payments gives organizations virtually no time to react to illegal activity, which means that institutions may need to review the timing of KYC activities. Verifying the authenticity of the customer prior to granting access to the system is vital. Financial institutions must balance introducing friction in the onboarding process against the need to manage risk for faster payments, which may introduce delays in making certain payment types available while an institution validates a customer's request for a certain payment type.

How are my BSA requirements impacted by faster payments?

BSA requirements are not altered by the advent of faster payments. However, the speed with which payments can be completed makes it more important than ever for an institution to execute its KYC, transaction monitoring, and suspicious transaction reporting responsibilities crisply.

How are OFAC requirements impacted by faster payments?

Financial institutions offering faster payments must have appropriate customer screening programs in place to comply with the requirements of the Office of Foreign Assets Control (OFAC). Screening is required at account enrollment and periodically thereafter based on the institution's OFAC compliance program.

While OFAC guidance exists for domestic ACH transactions[2] which allows originating and receiving financial institutions to rely on each other for OFAC screening, the guidance is dated from 1997. There is an absence of

[2] Source: Guidance to National Automated Clearing House Association (NACHA) on domestic and cross-border ACH transactions https://www.treasury.gov/resource-center/sanctions/Documents/gn121404.pdf

guidance on screening requirements at the time of transaction where financial institutions exchange faster payments.

What do I have to take into consideration for FFIEC when it comes to faster payments?

FFIEC Guidance calls for financial institutions to perform periodic risk assessments and adjust their customer authentication controls as appropriate in response to new threats to customers' online accounts. These risk assessments should occur as new information becomes available, prior to implementing new financial services, or at least every 12 months. Updated risk assessments should consider, but not be limited to, the following factors:

- Changes in the internal and external threat environment
- Changes in the customer base adopting electronic banking
- Changes in the customer functionality offered through electronic banking
- Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry

In addition to annual risk review, the FFIEC guidance recommends that management and system designers consult with the compliance officer during the development and implementation stages of new products to minimize compliance risk. The compliance officer should ensure that the proper controls are incorporated into the system so that all relevant compliance issues are fully addressed. This level of involvement will help decrease an institution's compliance risk and may prevent the need to delay deployment or redesign programs that do not meet regulatory requirements.

Compliance programs may not need to be revamped, but merely extended to address the new level of technology employed by the institution. Staff should be trained, and a monitoring system implemented to review continually the content and operation of the online programs to prevent inadvertent or unauthorized changes that may affect compliance with the regulations.

What kind of fraud monitoring is required for faster payments and where should it take place?

While each faster payment network may have unique requirements for fraud monitoring, reporting and review, some best practices are emerging. For greatest effectiveness, fraud monitoring should take place early in the transaction initiation process. This means assessing login attempts as well as transactions themselves to determine if they differ from historic activity for the customer initiating the transaction. Several software vendors specialize in detecting anomalies that can indicate fraud. When introducing a new type of payment, an FI should ask its fraud detection vendor if the solution it provides for the legacy payments can detect fraudulent transactions in the faster payment channel as well.

Controls to prevent fraud should be implemented in addition to—and regardless of—controls to detect fraud. If a financial institution offers online initiation of faster payments, it should authenticate initiators of transactions using methods that meet or exceed the expectations of the FFIEC Supplement to Authentication in an Internet Banking Environment (2011).[3] See the question on FFIEC above.

In addition to authenticating the initiator of a payment, a financial institution should encourage customers to implement controls to ensure that payments are properly authorized. Dual control (i.e., one person initiates, and another approves) over payments initiated through online and mobile channels provides an opportunity for a

[3] Source: Supplement to Authentication in an Internet Banking Environment https://www.ffiec.gov/pdf/Auth-ITS-Final%25206-22-11%2520%2528FFIEC%2520Formated%2529.pdffinancial/2011/fil11050.html.

second person to confirm the legitimacy of a transaction before releasing it for processing by the financial institution.

A change approved in November 2018 for the NACHA Operating Rules for ACH included a supplement to the existing rule on fraud screening for WEB debits. For several years, Originators of WEB debits have been required to use a "commercially reasonable fraudulent transaction detection system" to screen WEB debits. The new rule explicitly points to account validation as an inherent part of any commercially reasonable fraudulent transaction detection system. When the rule goes into effect on March 19, 2021, Originators of WEB debits will be required to validate the Receiver's account number for its first use with a WEB debit entry, and for any subsequent changes to the account number. This rule is designed to detect unauthorized debits to the accounts of unsuspecting consumers. However, account validation is equally useful in confirming validity of a receiver's account prior to sending a faster payment credit to the account.

An FI offering faster payments should consider establishing initiation limits (a dollar value per transaction, a cumulative dollar value per day; at the user level, at the customer level) to mitigate the risk of both operational errors and fraud.

Finally, as fraud management and reporting requirements for different faster payments networks may not directly align, institutions should be prepared for ongoing review and evaluation as part of a comprehensive risk management program.

Are faster payments covered under Reg E/UCC4A?

Yes. Reg E applies to funds transfers that involve a consumer account, which means consumers have the same rights to refute a faster payment transaction as they have with other electronic transactions.

UCC 4A applies to funds transfers as defined in 4A-104, except for funds transfers that are in any way governed by the Electronic Funds Transfer Act (Reg E) provisions that apply to electronic funds transfers (EFTs). (4A-102 and 4A-108). The Electronic Funds Transfer Act provisions govern any transfer of funds initiated electronically that instructs a financial institution to debit or credit a consumer's account. (12 CFR 1005.3(b))

UCC 4A will apply to funds transfers that do not involve credits or debits to consumer asset accounts as defined in Regulation E. This means that a faster payment funds transfer must have both a commercial sender and a commercial receiver in order for 4A to apply to the transfer.

What are best practices for handling transactions which have been authorized but result from a scam or fraudulent activity?

When a consumer reports fraud, a financial institution should research and, if warranted, request a return of funds from the receiver's financial institution. In addition, financial institutions should be proactive in recording and reporting fraud incidents, even in cases in which funds are not or cannot be returned to the consumer so that patterns of fraud can be prevented, detected, and potentially remedied.