Rethinking the future of payments

Steve Ledford

Received (in revised form): 23rd March, 2015

The Clearing House, 115 Business Park Drive, Winston, Salem, NC, 271076536, USA
Tel: +1 336 769 5308; mobile: +1 336 486 3635,
e-mail: steve.ledford@theclearinghouse.org

Steve Ledford

Steve Ledford *is Senior Vice President for Product and Strategy at The Clearing House, the US payment system operator and advocacy organisation. Prior to joining The Clearing House, Mr Ledford was a partner with Novantas, a financial services consulting firm. Before that he was a leader in McKinsey's global payments practice, and was President of Global Concepts, a consulting and research firm specialising in payments and cash management. Mr Ledford is a graduate of Wofford College with a BA in Economics.*

ABSTRACT

As more nations implement immediate payment systems, the industry has an opportunity to make payments not only faster, but safer and more useful. Tokenisation of payment credentials, credit-only transactions, imposition of robust access security, real-time anti-fraud/anti-money laundering/sanctions screening and network activity monitoring are ways to make any payment system safer. There is a continuum of choices that balance settlement risk with cost and complexity. Internet and mobile connectivity support rich, timely, flexible messaging. Combined, these factors provide an opportunity to build an unprecedented platform for payments innovation.

Keywords: payments improvement, immediate payments, safer payments, settlement, real-time messaging, payments innovation

Journal of Payments Strategy & Systems
Vol. 9, No. 2 2015, pp. 164–171

THE IMMEDIATE PAYMENT OPPORTUNITY

There is much excitement in the world of payments as, one after another, countries embark on ambitious plans to implement immediate payment systems. According to Lipis Advisors (see Table 1), a research firm, at least 16 countries had payment systems supporting immediate low-value account to account transfers at the end of 2014; other sources cite even higher numbers. Work is well under way in Australia and Colombia. In the USA, the Federal Reserve has called for the implementation of 'a safe, ubiquitous, faster payments capability',[1] and The Clearing House has announced that it will create a national real-time payment system. Similarly, the European Retail Payments Board agreed on 'the need for at least one pan-European instant payment solution'.[2]

This is clearly a time of tremendous change, but the focus on speed of payment can overshadow an equally important objective for payment system improvement — making payments safer. National payment systems and financial institutions have the opportunity to greatly increase security and customer protection as they implement faster payments. Failure to do so could undermine consumer and business confidence in new payment systems, impeding adoption.

Table 1: Retail immediate payment systems

Countries with retail immediate payment systems	*Retail immediate payment systems under development or announced*
Chile	Australia
Columbia	Colombia
Denmark	USA
India	Eurozone
Japan	
Mexico	
Nigeria	
Norway	
Poland	
Singapore	
South Africa	
South Korea	
Sweden	
Taiwan	
Turkey	
UK	

Source: Lipis Advisors

Focusing solely on speed also draws attention away from other aspects of a modern payment system that make it attractive for users. Payments are not made for their own sake; they are usually part of a commercial or social transaction. People pay bills, buy goods and services, send money to friends and family. Companies pay employees and suppliers. Smartphones, internet connectivity, web services architectures and other technological advances make it possible to integrate payments directly into these transactions in a way that yields benefits for payers and payees alike. Using existing card networks and electronic payment systems, innovators are already doing this to great effect including 'one-click' Amazon ordering and the seamless Uber process for booking and paying for a car ride. A payment system designed as a platform for integration into complex transaction flows can provide value well beyond simply moving money.

SAFETY FIRST

Cyberattacks have compromised hundreds of millions of accounts over the past few years, focusing attention on the safety of payments. Although losses due to fraudulent payments typically amount to only a fraction of a per cent of overall payments volume, system-wide averages hide the full picture. Card numbers stolen by cybercriminals can be used online, where defences are weaker than at a physical point of sale. According to the most recent reported data from the Federal Reserve, US 'card not present' fraud rates for credit and signature debit card transactions (0.118 per cent and 0.095 per cent respectively) in 2012 were more than three times higher than for 'card present' transactions (0.037 per cent and 0.028 per cent).[3] In 2013, 'card not present' fraud losses in the UK totalled £301m, or 67 per cent of total card fraud losses, much higher than would be expected based on the relatively low share of remote card transactions.[4] The use of mobile payments also creates new exposures and opportunities for fraud.

Fast payments are not inherently more risky than conventional alternatives, but the speed of payment makes them a target for fraud. Criminals target fast payment systems because, if they are successful, they can abscond with funds immediately, reducing the likelihood of getting caught. The launch of an immediate payment system can expose weaknesses in online and mobile banking security. When the UK introduced its Faster Payment Service in 2008, online banking fraud losses increased by 132 per cent, according to Financial Fraud Action UK.[5]

Tokenisation of mobile, e-commerce and other payments over card networks is a response to this threat. Tokenisation replaces the account number associated with a credit or debit card with a 'token' that can only be used for the intended

payment, and is useless to anyone other than the intended payee. Tokenisation protects payments against cyberattack by making stolen payments data useless to criminals.

Tokenisation is being added to existing payment systems, but can be built into new payment systems from the start. In a credit transfer system, using aliases instead of current account numbers avoids the need for payees to provide account data to be paid, while also simplifying the process of sending a payment (a credit transfer can use an unchanging alias instead of single payment token because the alias can only be used to put money into an account). Examples of alias addressing include Swish in Sweden and Paym in the UK, which allow users to send payments to registered payees by providing a telephone number. A more comprehensive approach would require the use of an alias for all credit transfers, and single-use tokens for debits.

Another way to make payments safer is to avoid third-party debits altogether. A credit transfer system is inherently safer than a payment system that allows the payee to debit the payer. All payments start with the payer instructing their financial institution to send funds. The onus is on the sender's financial institution to verify the identity of the sender, and they are in the best position to do so because of the existing relationship and 'know your customer' obligations. The sending financial institution can also verify and secure good funds, eliminating the risk to the payee of transactions reversed due to insufficient funds.

A credit transfer system also has structural advantages in defending against cybercrime. A hacker can create thousands of fraudulent debits using stolen account numbers through a single compromised online account, and then quickly abscond with the funds before transactions are returned unpaid. A credit transfer system, however, requires the hacker to compromise every account from which it steals funds, and is limited to the funds in each account. Cybercriminals have to work much harder in a credit transfer system to carry out large-scale fraud.

A credit transfer system can also, in effect, provide a safer type of debit transaction. For example, the soon to be launched Zapp scheme in the UK allows prospective payees to initiate a request for payment. The recipient of a request for payment can respond by initiating a credit transfer. This is safer than a conventional debit payment, because the payer must specifically authorise each payment. A well-designed process can also reduce the risk of misrouted payments by automatically embedding the payee's account number or alias into the request and associated transfer. With effective identity verification by the requester's financial institution, a request for payment process built into the payment system is also a protection against phishing (soliciting sensitive information through misleading e-mail) or smishing (the same activity using SMS mobile phone messages). The recipient knows that the requestor's identity has been verified and the communication channel is secure, unlike solicitations by e-mail or text message, which can be easily spoofed.

The first line of defence for an electronic payment system is access control — ensuring that only those authorised to initiate a payment can do so. Multi-factor, multi-layered security is good practice for any type of online or mobile payment application, and is essential for immediate payments. Choices regarding access security methods are often left to individual financial institutions. The rationale is that, in a credit transfer system, the sending financial institution bears the liability for unauthorised transactions and therefore

has an incentive to employ effective online and mobile banking security. But if some financial institutions fail to implement adequate access security, they become the weakest link in the payments chain. When these institutions attract the attention of cybercriminals, they may react by imposing drastic restrictions on their customers' payment activity, such as low limits on transaction value. This impairs the utility of the payment system for payees at other institutions, and can have the general effect of undermining confidence in the system as a whole. Preventing unauthorised access and fraudulent payments is a concern for the entire payments community.

Immediate payments create challenges for conventional fraud detection, anti-money laundering (AML) and sanctions compliance methods used for electronic funds transfers. Non-immediate payment systems can employ processes that rely on automated screening coupled with manual review of suspicious transactions. This approach is possible because conventional electronic payment processes are sequential, beginning with initiation by the customer, followed by a series of operational and screening steps by the financial institution before submission to the payments network. There is time for exceptions such as fraud or AML suspects to be reviewed by experienced staff before release.

The immediate payment process, however, is essentially synchronous. Processing and qualification of the payment by the sending financial institution is done while the sender is initiating the payment. There is not enough time for a manual review, even of a small percentage of exceptions. To be truly effective, anti-fraud, AML and sanctions screening must be automated and integrated into the real-time payment initiation process. This is already common practice for card payment networks, where fraud detection is embedded into online transaction authorisation.

Detection of suspicious activity can extend beyond individual financial institutions to the payments network. Some criminal activities are more readily detected by observing activity across multiple institutions to detect patterns. An example is money muleing, the money-laundering technique of transferring funds among a large number of different accounts held by individuals recruited, often unwittingly, for the task. Transfers that seem innocent when viewed by a single financial institution can be identified as part of a complex web of transactions at the network level. Inter-bank payment systems are increasingly taking steps to monitor network traffic to identify potentially criminal activity.

Tokenisation of payment credentials, avoiding third-party debits, imposition of robust access security, real-time anti-fraud/AML/sanctions screening and network activity monitoring are ways to make any payment system safe. As nations seek to modernise their payment systems, they have the opportunity to implement safety measures that are built-in from the beginning instead of bolted on afterwards.

Settlement is another element of safety. Financial institutions cannot accept a material risk of settlement failure if they are expected to provide their customers fast access to funds.

Shortening the length of time between clearing and settlement limits the risk of settlement failure. Immediate settlement reduces the length of time between clearing and settlement to zero. To effect immediate settlement, financial institutions are required to hold sufficient funds in a central bank account or other cash facility to cover peak payment activity over any given period. Immediate settlement is also more complex and operationally demanding than deferred net settlement. For this reason, RTGS and continuous net settlement, two methods of immediate settle-

Table 2: Settlement methods

Least settlement risk/ Higher cost and complexity ⟵ ⟶ *Higher settlement risk/ Lower cost and complexity*	*Real-time gross settlement*	*Continuous netting*	*Seconds/ minutes*	*Multiple time*	*Late eventing*	*Next day*
Descriptions	*Immediate settlement of the gross amount*	*Immediate netting of offsetting positions*	*Close-to-immediate net settlement*	*Frequent net settlement*	*Settlement after normal business hours*	*Next day settlement of net amount*
Problems addressed						
Single-payment default	×	×				
Short-term settlement risk	×	×	×			
Large unfunded positions	×	×	×	×		
Overnight settlement risk	×	×	×	×	×	
Liquidity efficiency		×	×	×	×	×
Cost of settlement				×	×	×

ment, are typically associated with high-value, low-volume payment systems where the need to eliminate the possibility of settlement failure warrants the additional cost and complexity. Some existing and planned retail immediate payment systems, however, do employ immediate settlement.

Deferred net settlement reduces overall funding requirements by offsetting debits and credits for payments sent and received over the settlement period, typically requiring less liquidity to be held in central accounts for settlement. Net settlement is also less operationally demanding than immediate settlement, because there is no need to synchronise transaction clearing and settlement with the central bank. Net settlement does, however, introduce the risk that a financial institution in a net debit position will not settle its obligation.

Payment systems that employ deferred net settlement use a variety of techniques to mitigate or eliminate settlement risk, including prepaid settlement funds, pledged collateral pools and debit caps on positions held by individual financial institutions. Increasing the frequency of net settlement is another way to reduce the risk of settlement failure by discharging obligations before large unsettled positions can build up. It is not uncommon for low-value bulk payment systems to settle the day after clearing, while many retail immediate payment systems settle multiple times a day, sometimes every few minutes or seconds.

A third option that combines features of Real-Time Gross Settlement (RTGS) and deferred net settlement is continuous net settlement or real-time final settlement. Under this approach, offsetting positions are netted in real time, with the net amount charged immediately against a settlement account.

Variations in settlement methods create a continuum ranging from RTGS and continuous net settlement to next-day net settlement, with corresponding trade-offs between settlement risk and cost or complexity.

Table 3: Settlement risk mitigation methods

Prefunding	Financial institution must deposit full settlement obligation amount in cash prior to clearing, clearing is suspended when gross or net position reaches prefunded balance
Collateralisation	Financial institution must deposit full or partial settlement obligation amount in collateral (typically high-quality securities) to be liquidated in case of settlement failure
Pre-funded Common Backup Fund	Participants contribute to a pool from which to draw in event of settlement default
Loss-sharing Agreement	Remaining participants cover losses in event of settlement default
Gross Debit Cap	Limit on the total amount of payments initiated by a participating financial institution
Bilateral Net Debit Cap	Limits on net settlement positions for a participant set by and for each counterparty
Multilateral Net Debit Cap	Limit on net settlement position for a participant across all counterparties

ADDING VALUE

The essential function of a payment system is moving money. A modern payment system, however, can do much more. Every payment is made for a reason. Understanding the reasons, or use cases, behind payments allows financial institutions to create products and services that facilitate extended commercial or social transactions.

Immediate payment systems are particularly well suited to provide value beyond the inherent benefit of fast money movement. A fundamental feature of immediate payment is real-time communication among senders, receivers and their financial institutions. The use cases for immediate payment are those that benefit from both immediate funds transfer and immediate messaging, such as notification, confirmation and request for payment.

Bill payment provides examples that distinguish between use cases for immediate payment and conventional alternatives. In most cases, bill payments can be scheduled ahead of due date, using low-cost batch automated clearing house (ACH). Some customers, however, choose to pay bills on the due date, either because of procrastination or because they do not have sufficient funds before then. These 'just in time' bill payments require fast movement of funds from the bill payer to the biller. They also require immediate notification to the biller that payment has been made, and confirmation to the bill payer that the payment has been received. The biller can avoid taking action for collection or service cut-off, and the bill payers know that they have fulfilled their obligation. The immediate exchange of notification and confirmation messages is an essential part of the transaction.

Similarly, a single business-to-business (B2B) transaction illustrates the value of extensive immediate messaging. Consider a restaurant that orders produce for immediate delivery from a supplier that does not extend trade credit. The restaurant needs the produce for tonight's dinner service, and the supplier needs to be paid before shipping the goods. Using the immediate messaging capabilities of a fully featured immediate payment system:

(i) The supplier sends a 'request for payment' through the network to the restaurant. Sending the request through a secure, trusted channel reduces the risk of fraud associated with an e-mail invoice, which can be spoofed by criminals.
(ii) The restaurant receives the request for payment and immediately sends a payment to the supplier.
(iii) The supplier receives notification from its financial institution and loads produce for delivery to the restaurant, confident that payment has been made.
(iv) The supplier sends acknowledgment of payment receipt to the restaurant, confirming that the produce is on the way. Because confirmation is sent through a reliable, trusted channel, the restaurant is assured that diners will enjoy salads, fruit and vegetable dishes made with fresh ingredients that evening.

In this example, the restaurant and supplier exchanged four messages through a secure, reliable channel, only one of which was the actual payment. Each message fulfilled a specific need for the buyer or seller in the transaction.

Note that the exchange of information between buyer and seller goes beyond the remittance detail that typically accompanies B2B electronic payments. Remittance data are essential, allowing the supplier to apply payment to the correct invoice and account, and reconcile any differences. In this immediate payment example, the payment request, notification and confirmation messages provide additional value for a time-sensitive transaction.

A relatively recent innovation is the use of external references within payment messages to provide value-added information or services. An example is the approach used to link medical payments to payment detail in the US ACH network. Instead of embedding sensitive medical payment details in the ACH transaction, the payment includes a 're-association trace number', which corresponds to the same element in the electronic remittance advice (ERA) provided by the health-care plan.

This approach can be extended by embedding live links to external data or processes, a process that is often compared to the use of the Universal Resource Locator (URL) on the internet to reference websites within text. For example, instead of including remittance data in the payment record or an addendum, an embedded link might point to a server with richly detailed invoice data, including a full explanation of returns, exceptions and discounts taken. An external link could even invoke an application instead of simply pointing to data.

External links have several advantages. The data referenced by the link do not need to fit within the constraints of the payment message format. External data can be customised for the unique requirements of specific use cases, industries or even individual counterparties, a level of variability that would be difficult for a single payment system to accommodate in its standard formats. Perhaps most importantly, external links provide opportunities for innovation beyond those that can be envisioned by the planners of a centralised payment scheme.

Ultimately, this should be the goal of modern payment systems. Moving money rapidly is the baseline capability. Doing so safely is essential, and achievable. A payment system that is flexible and adaptable, however, can be a platform for innovation. No one could have envisioned the explosion of applications built on the internet and mobile telephony. Payment systems should aspire to be adaptable enough to

support the ever evolving needs of the future.

References and Notes

(1) United States Federal Reserve System (2015) 'Strategies for Improving the U.S. Payment System', United States Federal Reserve, January, 56 pp.
(2) European Central Bank European Retail Payments Board (2014) 'Statement following the second meeting of the Euro Retail Payments Board', 1st December.
(3) United States Federal Reserve System (2013) 'The 2013 Federal Reserve Payments Study — Recent and Long-Term Payment Trends in the United States: 2003–2012 — Summary Report and Initial Data Release', December, 43 pp.
(4) Financial Fraud Action UK (2014) 'Fraud the Facts 2014', May, 100 pp.
(5) *Ibid*.