ACI UNIVERSAL PAYMENTS℠

INDUSTRY PERSPECTIVE

IMMEDIATE NEED FOR FRAUD PREVENTION

BEST PRACTICES FOR PREVENTING FRAUD IN A REAL-TIME WORLD

As countries speed along the path towards immediate payments, the historical model of crossing that bridge when we get to it is no longer a viable option when managing the threats of fraud and money laundering. Global rollouts of any new payments scheme have proven that any vulnerability for financial exploitation will realize some form of abuse until tighter controls for authentication and prevention solutions are put in place. So naturally, as fraud finds its way by the path of least resistance, immediate payments present an attractive new pathway to abuse. The residual for any payments provider who seeks to offer these real-time services is that financial losses and compliance issues are inevitable, especially when transactions times shorten to as little as three seconds. To mitigate fraud in such a short time window requires investment in new processes, technology and training staff, and educating customers.

With the goal of a successful immediate payments launch, careful consideration should be given to the balance of a friction-free user experience against the protection and security for customers. Payment providers that take an enterprise, layered, customer-centric approach to addressing fraud in real time will position themselves to be trusted providers, generating new revenue from differentiated, value-added services. This paper outlines best practices for payment providers to adopt when considering how to protect their customers in a real-time payments world.

BACKGROUND

An immediate (sometimes referred to as a real-time, instant or faster) payment is an interbank account-to-account transaction that is posted to the receiver and confirmed to the sender within seconds. Numerous immediate payments schemes are in operation today and there are several planning to enable real-time payments in the coming years, including the two largest payments markets in the world: the United States and Europe.

Immediate payments present significant benefits for the economies who adopt it, allowing for a dramatic increase in the execution speed of digital payments and, in turn, accelerating working capital. While this payments evolution will inevitably have a tremendous reach both domestically and in the future, cross-border, it provides a significant opportunity for fraud in a high-velocity environment. The characteristics of faster payments make them highly attractive for fraudsters.

Irrevocability, immediacy and liquidity make this payments channel incredibly attractive and preferential to the traditional online banking fraudster. This was evidenced when the U.K. Faster Payments initiative launched in 2008. Online banking fraud losses increased from £22.6m in 2007 to £52.5m in 2008 and then to £59.7m in 2009, before security measures implemented forced the fraud rates to start dropping again.

Taking a holistic approach prepares the payments provider to remain resilient to threats to immediate payments across the entire processing workflow. Methodologies used and suggested by industry thought leaders and recognized bodies illustrate that a multi-point, consolidated solution that can integrate the right tools with the appropriate actionable outputs is best positioned to address the new threats that will emerge.

FASTER PAYMENTS FRAUD: A U.K. CASE STUDY

All of the dozen countries currently in the development stages of their immediate payments schemes could learn valuable lessons from the introduction of the U.K.'s Faster Payments scheme in 2008. Often considered the standard of the "modern" immediate payments schemes, the U.K. experienced a sudden and significant jump in fraud cases as soon as it was launched, and it took the banks and building societies about 18 months to pinpoint and adequately address its issues. As the volume of immediate payments has skyrocketed over the past eight years, the industry has managed to keep fraud levels at a slightly higher rate than checks and considerably lower than cards. How they did so provides valuable insights for new schemes.

BACKGROUND

The U.K.'s immediate payments scheme, named Faster Payments Service (or FPS), launched in May 2008, and over the past several years has successfully achieved an enviable level of ubiquity in the market: we estimate over 5.6 billion payments have been made since launch, with all U.K. banks and building societies having access to the service. In less than a decade, Faster Payments became the second largest payment type by transaction volumes, exceeding 1.1 billion transactions in 2014, second only to cards. Exhibit 1 illustrates the strong and continued growth of Faster Payments in the U.K. as measured by transaction volume and value.

U.K. Faster Payments launched with an initial transaction limit of £1,000. The limit quickly grew to £10,000 and in 2010 it was raised to £100,000. In November 2015, the maximum transaction value rose yet again, this time to £250,000 (the current equivalent of $360,000). This steady lifting of the transaction ceiling provides a clear indicator of the scheme's growing comfort with managing the related fraud from faster payments.

GROWTH IN U.K. FASTER PAYMENTS VOLUMES

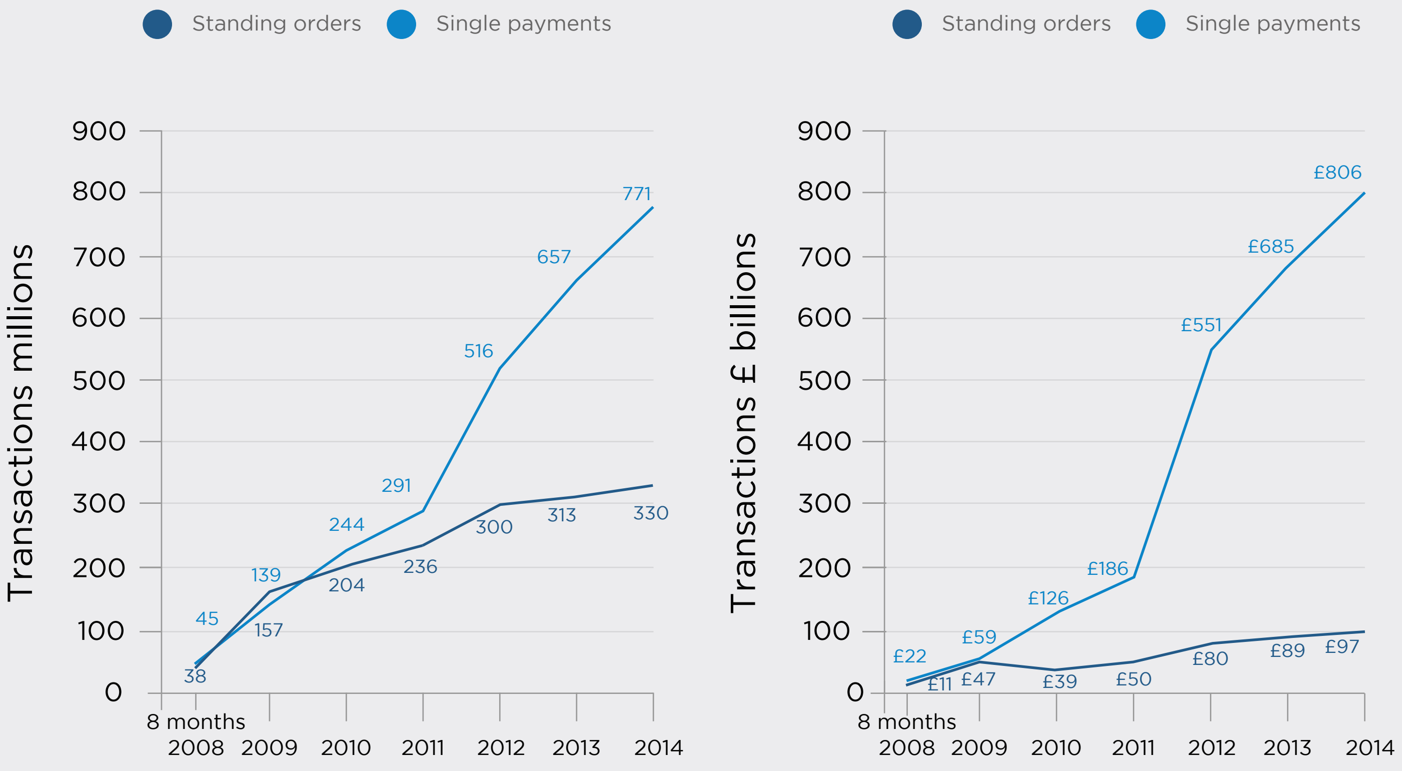


Exhibit 1

Source: Payments Council

COMBATING SHARPLY RISING FASTER PAYMENTS FRAUD CASES

The banking and payments industries in the U.K. were caught off guard with the sudden spike in online banking and telephone banking fraud cases as the result of the faster payments launch. While it was later determined that the inherent infrastructure of the faster payments was sound, the entry points to transaction initiation were weak, and this weakness was exposed by fraudsters.

The annual value of fraud losses from online banking nearly tripled in the 18 months after faster payments were launched. It wasn't until 2010, the schemes third full year, that banks began to update their internal fraud processes, as well as collaborate with other banks against the attacks.

With each successive year, fraud loss rates have dropped as a percentage of the total value of faster payments transactions. Exhibit 2 indicates the quick growth and subsequent tapering off of faster payments-related fraud losses.

While the annual losses now appear to be relatively consistent (ranging from £35m to £41m for online banking and £12m to £13m for telephone banking), the decreasing red line shows a continued lowering of the fraud percentage per value transacted. It is a startling recovery. Consider this: in 2009 (Faster Payments' first full year of operation), there were £106bn in transaction value, but by 2013, that number had increased seven-fold, reaching £770bn. And in 2014, transaction value exceeded £900bn.

In 2013 the Payments Council released data indicating that Faster Payments fraud per £1,000 of spending was 7 pence per thousand (0.007), slightly higher than checks, but considerably lower than cards (see Exhibit 3). It has been a significant victory, and was the result of the considerable efforts undertaken by the banks and building societies, as well as by the scheme operator.

U.K. FASTER PAYMENTS FRAUD LOSSES

Fraud has declined from £1.6 per £1,000 in 2008 to just 7p per £1,000 in 2013

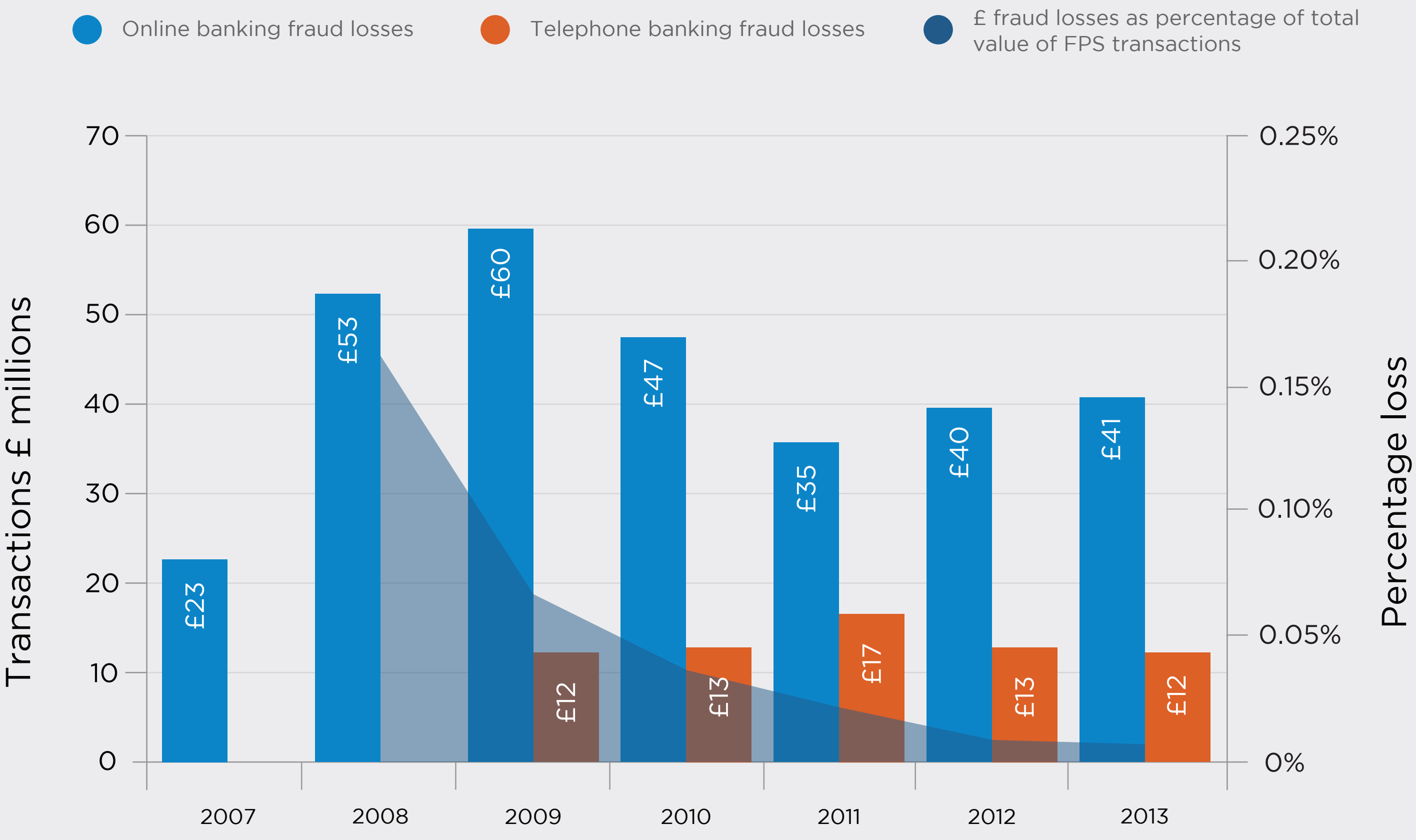


Exhibit 2

Source: Payments Council and FFA UK

CONSIDERATIONS FOR OTHER COUNTRIES

Based on the experiences of the U.K. participants, three key points are suggested for organizations preparing to support immediate payments in their own countries:

1. **Get involved**
   It is essential for bankers, PSPs, merchants and other participants to read the work being produced by governments, scheme operators, industry analysts and vendors which have participated in schemes in other countries. Ask questions. Join industry councils, such as the Federal Reserve Bank's Secure Payments Task Force in the United States.

   Many banks are now forming cross-bank strategy teams, linking retail, commercial and corporate banking groups with technology and fraud teams to develop enterprise-level strategies around immediate payments. Determine if your organization has started such a group, and if so, join it. Work across the company to determine where your own faster payments vulnerabilities might reside.

2. **Speak with each other**
   Find your peers at other banks, PSPs, merchants and other likely participants in an immediate payments scheme. Attend industry conferences and share those learnings internally. Collaborate with other institutions and share insights. Choose to work with vendors that demonstrate credible experience, that have worked successfully in other regions and that have shown active participation in the development of the local faster payments schemes.

3. **Talk to your customers**
   Start a dialogue with your customers. Let them know you're already engaged internally and externally regarding faster payments and fraud, and that you'll be a trusted resource for them. It's not too early to start those conversations.

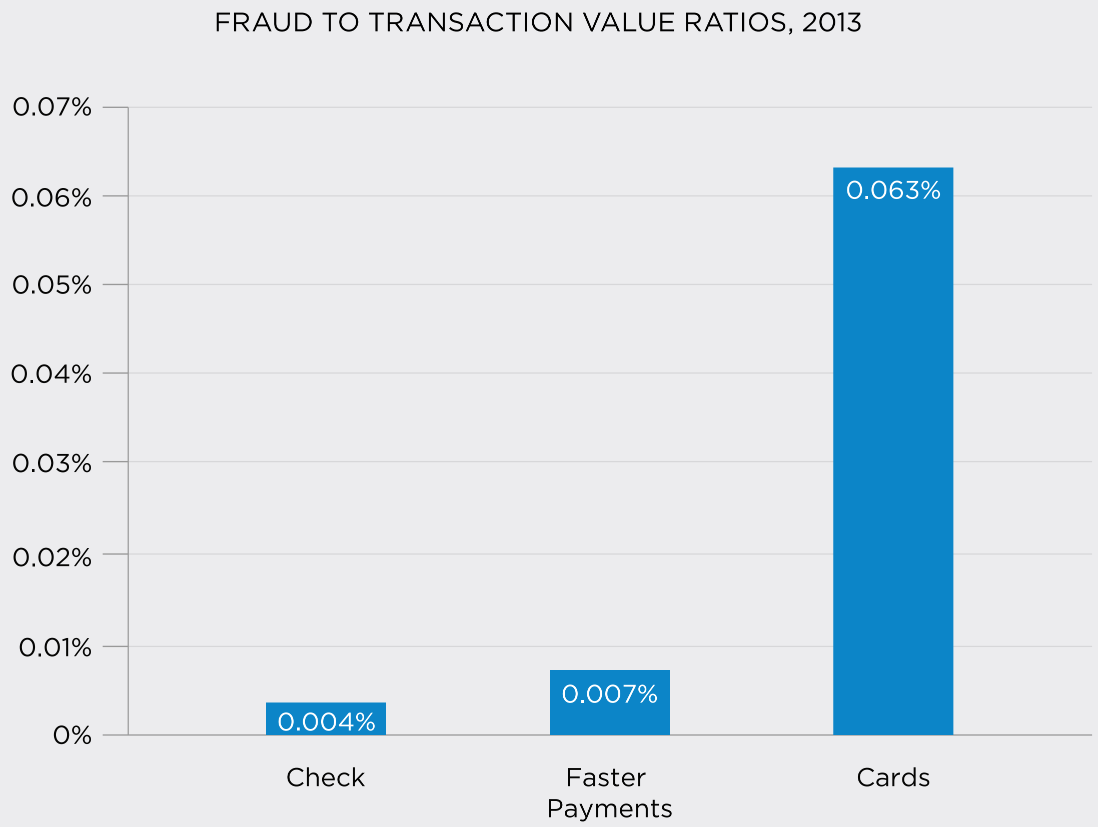


Exhibit 3

Source: Payments Council and FFA UK

RISK SEGMENTATION

In developing the risk management framework including immediate payments, one of the core functions is understanding channel (online, mobile, employee/terminal and even network) risk, and developing a segmentation strategy that is based on an operational risk assessment methodology (e.g., the COSO model). Vulnerabilities exist in all channels, subsequently it is critical to develop a layered control environment that follows the transaction lifecycle, which will prove resilient against evolving attempts by attackers to identify weaknesses.

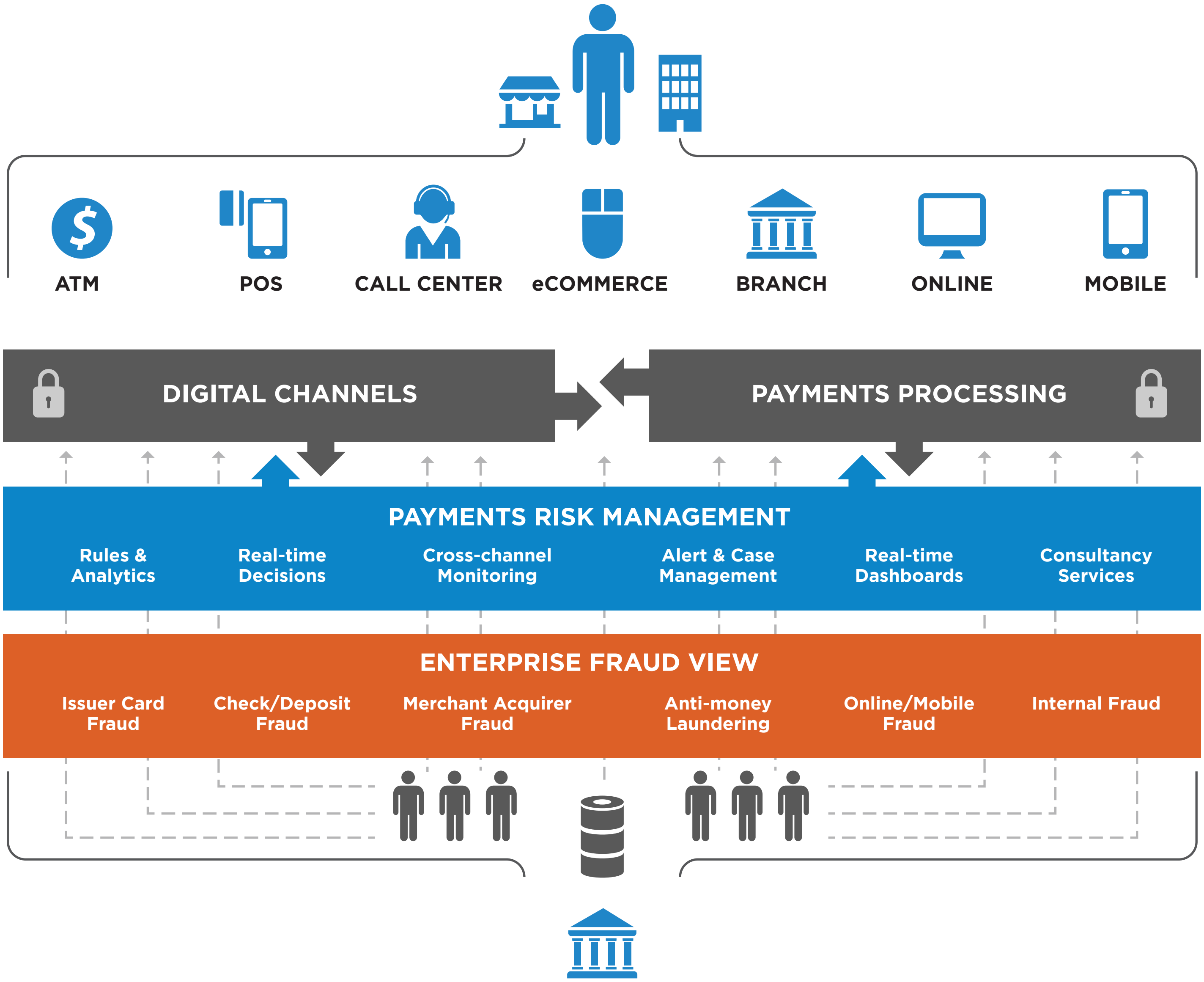
The layering of this environment should include dynamic authentication, navigation and device analysis systems, as well as the capacity to integrate these various data feeds with real-time rules in the enterprise fraud detection solution.

The layering of this environment should include dynamic authentication, navigation and device analysis systems, as well as the capacity to integrate these various data feeds with real-time rules in the enterprise fraud detection solution. These controls will need to be dynamic, beginning at the point of entry, with risk-weighted controls at various parts of the user's interaction with the channel gateway as the customer's session runs its course. A robust fraud prevention strategy should also have the capacity planning that allows for an agile integration of any additional third-party tools to monitor any point in a user's session, should a gap be later recognized. Furthermore, it is critical to have a solution that scales in real time to handle the adoption of faster payments in concert with any of the layered third-party elements.

Segmentation opportunities exist in the session interactions where the customer makes contact with the payments provider, and detection controls must be placed at all touch points with the customer following their path from login through to the monetary transaction. The following (integrated) layers can be applied to the session phases (such as logging in, then form filling, preparing a payment, etc.) and solutions exist in the marketplace to act as key risk indicators (KRIs) relative to the phase:

1. **Authentication** — Assessment at the initial login. Evaluation of the relative risk of the login, access point and the overall risk potential of the initiation of the session. Monitoring the front end against attackers can be aided by device, navigation and behavioral monitoring solutions.
2. **Device analysis** — Applied to look for areas of abuse and manipulation of the end users and their access point. The devices tend to be able to be recognized for the user, applied a score, and identified as safe, secure and ultimately reliable.
3. **Session navigation** — Identify path of the session and whether it represents a customer's usual access. Were the session transactions, click stream and online interactions of the user aligned with what would be typical of how this customer interacts with the site or gateway?
4. **Behavioral profile** — Verify the profile of the customer is aligned with the monetary transaction(s) that were attempted. Assess for anomalous elements or parameters relative to how the customer typically transacts.
5. **Review of cross-channel or multi-channel activity** — Review account activity in relation to the most recent activity, to identify additional elements that may be related to this activity both inside the account and between seemingly unrelated accounts. Non-monetary transactions and/or a review of the demographic elements associated with the transactions can be a risk indicator.
6. **Real-time and/or transaction alerting rules** — Integrate transaction controls of the above elements into a holistic solution. At the point of initiating a monetary transaction, the comprehensive intelligence of the session is gathered and logic is applied to make the approval, decline or hold decision. Although the focus is on "immediate" payments, many implementations have service levels (SLAs) that allow for a small percentage of transactions to be held before release. For example, the Australian implementation of immediate payments (New Payments Platform) will have an SLA of 95% of transactions responded to within 15 seconds. Transactions that are deemed high-risk, but not high enough to decline, can be held, reviewed, then released/declined. In many cases, an approval can be given and any low-risk suspicious activity flagged for follow-up by an analyst.

Utilizing a suite of analytical options, such as behavioral profiling, enterprise data points (including cross-channel and non-monetary transactions) and the capacity for the agile integration of multiple and disparate sources of rich data elements, will provide sufficient data points for developing fraud detection strategies. These strategies will allow for the application of rules that are specific and precise enough to create a volume of alerts that are both high-quality and low-quantity and therefore manageable in a high-volume, high-velocity environment. Lastly, capacity for not only alerting, but also a real-time decline or hold capability for any immediate payment, is a must for any solution.



To this end, where immediate payments are accessible to end users through digital channels, these risks must be mitigated through an advanced enterprise-grade fraud detection solution, such as the diagram on the next page illustrates.

FINDING THE BALANCE: FRAUD AND CUSTOMER EXPERIENCE

Certainly there is a strong relationship between a friction-free customer experience and the effective mitigation of fraud. In a recent Aite and ACI survey, more than half of customers suggested they wanted to be a part of the fight against fraud (https://www.aciworldwide.com/fraud-survey). The customer experience, both in terms of preventing impact from false positives and in resolution handling, requires a steady balance. This is the critical takeaway of the survey, that customer confidence and follow through is a competitive advantage for the institutions who efficiently manage the overall process.

As previously noted, there may be SLA thresholds for throughput rates, and this extends to the processing of alerts by the investigative analysts assigned to the portfolio. However, there is a limit to the customer's patience for transaction disruption, so the minimization of false positive alerts and real-time declines is a critical component of this solution. Combining the previous session phase recommendations, such as device analysis and other integration layers, sophisticated behavioral profiling will keep false positives minimized and at acceptable thresholds.

Finally, it's important to include services that allow for end user engagement, from SMS transaction alerting mechanisms, which may include in-app customer-generated transaction thresholding, to authentication strategies which provide a reduced or friction-free user experience as much as possible. During creation of end user engagement strategies, consideration must also be given to the type of customer transaction; immediate payments could be a P2P, P2B, B2P or B2B transfer.

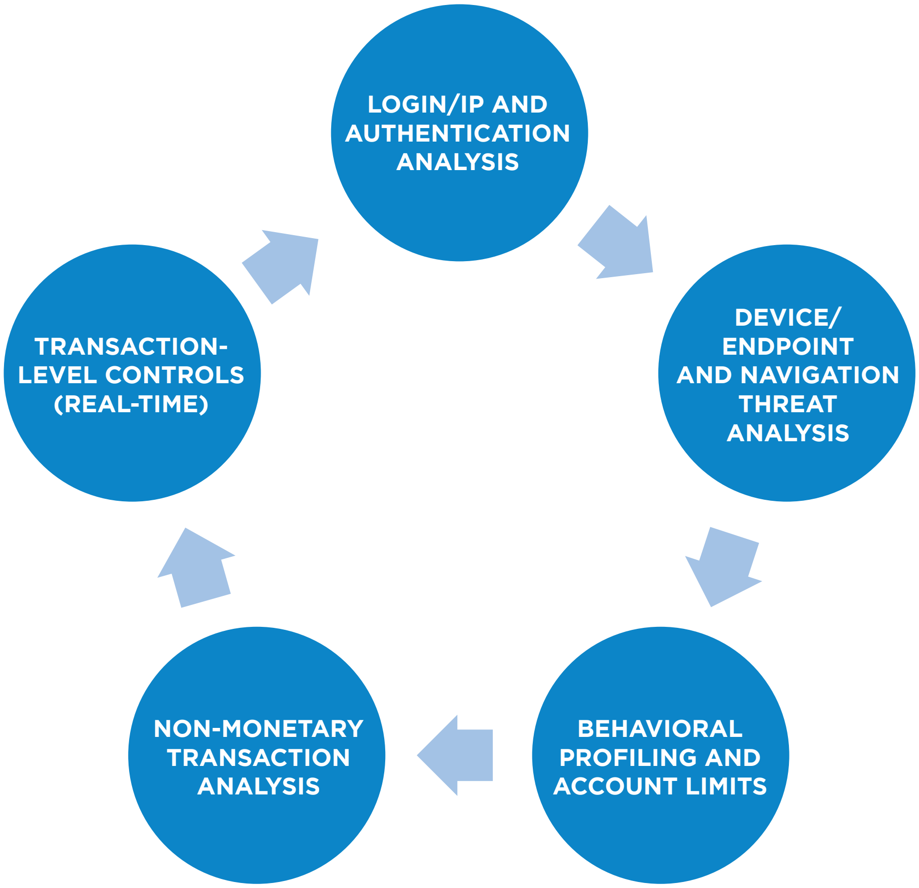
Controls must be appropriate to the risk the transaction represents, for instance controls placed on a low-value consumer payment (settling a restaurant bill with friends) should be very different to those with commercial purpose, likely to be much higher in value. Although many use cases for immediate payments tend to focus on consumers, with scheme limits increasing, such as in the U.K. where it was increased to £250,000 in 2016 with views to increase further in the future, or Australia which is set to have no limit at all; it should be expected that high-value transactions will be processed in high velocity. Combining end user mechanisms into the fraud detection strategy with scalable customer contact mechanisms ensures that the customer has a balanced experience and maintains the expectation that the payments provider has a sound security policy. Controls should be deployed and tested well ahead of the actual launch to maintain security and help ensure adoption and growth by avoiding preventable fraud. Properly executed, the customer contact strategy and fraud control strategy can be aligned, offering a positive customer experience.

APPLICATION OF THE COMPONENTS

Once the selection of third-party key risk indicators and/or authentication elements are identified, the solution should be stood up against the risk assessment methodology. Using a control environment assessment relative to the channels which may be monitored, real-time and alert rule logic can be applied. Deployment of such a solution requires distribution of the findings from the completed risk assessment, definition of appropriate metric targets, for example, alert rates and false positive rates, and agreement on acceptable thresholds.

Rule layering, the application of multiple rules for a single channel segment, has become best practice for implementing an effective defensive position and must consist of multiple safety nets to be effective. Developing these multi-part strategies, which begin gathering information at login, to include authentication strategies as well as user endpoint analysis, starts the process of integrating multiple data points to properly understand the legitimacy of the device accessing the services.

The right technologies from trusted partners, integrated into a true multi-channel enterprise fraud management


LOGIN/IP AND AUTHENTICATION ANALYSIS
DEVICE/ ENDPOINT AND NAVIGATION THREAT ANALYSIS
BEHAVIORAL PROFILING AND ACCOUNT LIMITS
NON-MONETARY TRANSACTION ANALYSIS
TRANSACTION-LEVEL CONTROLS (REAL-TIME)

A layered strategy offers the most holistic approach to fraud prevention.

solution, will create a secure environment with payments delivered reliably, rapidly and securely. While we are in a period of significant disruption in the industry and immediate payments is a driver of this, the lessons learned up to this point support a holistic fraud approach — as the cliché goes "an ounce of prevention is worth a pound of cure".

NETWORK FRAUD MANAGEMENT

Payments operate in open networks with many parties and layers of relationships between these parties. The central infrastructure/network connecting the parties can play a critical role in risk management beyond credit worthiness and solvency. As more real-time solutions are implemented globally within domestic schemes or extending across borders, the role of the network in protecting against fraud could be extremely valuable.

As a provider to both banks and non-bank members, the central infrastructure is in a unique position to provide enhanced fraud prevention because it touches all of the transactions in the network. In this capacity, the central infrastructure has access to the most data on the network. Used appropriately, this data could be used to further protect the entire community. This is not to say that it is the sole responsibility of the operator; it is the responsibility of the entire community participating in the scheme. The aggregation of as much data as possible (i.e., customer and endpoint information) would allow for comprehensive efforts to mitigate threats.

> This key characteristic of an effective fraud detection solution also allows the tools to easily digest actionable intelligence and new, reconfigured or third-party data elements without significant technical support.

To this end, numerous approaches and technologies used for modelling could be chosen for enhanced fraud prevention and analytics. This function could be centralized as an activity performed by the central infrastructure. Or the central infrastructure could provide the capability as a service to its members, using the intelligence it has as a result of its central processing role. In either case, addressing fraud prevention at the start, with a proactive approach based on profiling information available via historical analysis of other payment types, can only help to protect in the environment of faster, irrevocable payments.

ACI PROACTIVE RISK MANAGER™ AND IMMEDIATE PAYMENTS

In ACI's experience, reductions in false positives by over 40% can be achieved by upgrading fraud management tools over prior systems, while simultaneously tripling detection performance on a transaction basis. The long-term success of a fraud detection solution typically requires one element to retain confidence and relevance during a fraud event — agility. Agile solutions can be rapidly configured to meet a new threat head on, without significant resource investment or technical support. This is critically important when considering a new payment type that is irrevocable such as an immediate payment. Fraud events act like business disruptors when an unexpected significant event in both size and scope and without immediate visibility to causative factors occurs. Having an open solution and flexible configuration is key to the successful remediation of the risk. An extendable fraud detection solution should provide its users with the flexibility and independence to fully utilize the tools, where necessary under appropriate oversight, and not block access to a critical element in a time of need. This key characteristic of an effective fraud detection solution also allows the tools to easily digest actionable intelligence and new, reconfigured or third-party data elements without significant technical support. Empowering business users through tools that feature extendable and agile architecture can transform a high-risk fraud event into a residual loss avoidance situation, instilling confidence in the team's ability to mitigate the risk of a fraud event via a creative and persistent approach.

UNIVERSAL
PAYMENTS℠

ABOUT ACI WORLDWIDE

ACI Worldwide, the Universal Payments (UP) company, powers electronic payments for more than 5,100 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software and SaaS-based solutions, we deliver real-time, any-to-any payments capabilities and enable the industry's most complete omni-channel payments experience. To learn more about ACI, please visit www.aciworldwide.com. You can also find us on Twitter @ACI_Worldwide.

www.aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ATL6002 07-16