Fraud in the World of Real-Time Payments
Executive Summary ..................................................................................................................1
Introduction ............................................................................................................................2
Section 1: What exactly are “real-time payments”? ............................................................4
  How is it defined in the UK? ...............................................................................................4
  How are real-time payments beneficial for the digital economy? ................................6
  How have real-time payments been rolled out around the globe? ................................9
Section 2: What impact do real-time payments have on fraud? ........................................14
  What type of fraud keeps financial crime experts up at night? ......................................14
  What is being done to understand and combat payments fraud in a real-time environment? .................................................................14
Section 3: A look at the Which? Super Complaint — Is there a fine line between responsibility and liability? .................................................................21
Section 4: Strategies around technology and innovation ..................................................28
  How can AI, distributed ledger technology or tokenization aid in supporting fraud prevention strategies? .................................................................28
Section 5: How FICO helps prevent fraud in a world of real-time payments ..........32
Executive Summary

The past few months have seen the launch of new real-time payment schemes in significant geographies. In November 2017, SEPA Credit Transfer Instant was launched in the eurozone, while in the USA The Clearing House Faster Payments scheme also went live. In February 2018, the newest real-time payments scheme was launched in Australia with their New Payments Platform. Meanwhile, Canada is on track to launch their real-time payments scheme by the end of 2019. These schemes are all intended for mass adoption. They will fundamentally alter how payments are made in the geographies concerned. This will have a significant impact on the types and volumes of fraud they experience.

In this whitepaper, we look at the history and experience of countries such as the UK that have had mass adoption of real-time payment schemes for some time. We will consider the effect that real-time payments has on fraud and the response of the public and the industry. We will ask what can be done to help manage fraud in the world of real-time payments and uncover the strategies that will help new adopters avoid the pitfalls experienced by the real-time payments pioneers.
Fraud Prevention and Real-Time Payments — Introduction

On July 11, 2017, a little over nine years since its launch in the UK, the Faster Payments service successfully tested a payment. A rather large payment. With 16 financial firms receiving, and quite a few sending, a “live proving” exercise saw a payment processed by the scheme valued at tens of millions of pounds. This, according to people close to the live proving, was done in anticipation of raising the Faster Payments limit from its current £250,000 to £20 million. This made the possibility of using the platform to purchase high-value items, such as a house, via Faster Payments in the UK much more likely—if banks’ collective risk appetite raises to that level.

Nine years after Faster Payments restructured the payments landscape, taking on the 1960s era BACS (Bankers’ Automated Clearing Service) for everyday direct debits and credits, the UK platform is gearing itself to make a dent into CHAPS (Clearing House Automated Payments System). Used since the 1980s, CHAPS supports high-value payments that tend not to be an everyday occurrence for most people living in Britain today.

While the UK is entering a decade’s worth of experience dealing with Faster Payments, the availability of “on demand” payments is only now spreading around the world. These payments services tend to be known by a variety of names and descriptions — from the hotly debated use of the term “real time,” to immediate payments, to variations on the initial UK description of fast or faster for new payments processing and settlement.

Whatever the description, these new payments schemes adhere to a common theme: They replace older, legacy, batch-based clearing systems, which often take days to clear, with an on-demand service that is ready to transfer and confirm payments 24 hours a day, 365 days a year, within minutes or seconds.

Singapore launched FAST (the Fast and Secure Transfers service) in March 2014 and several countries in Europe have been developing their own approach to on-demand payments over the past few years. In November 2017, the European Payments Council went live with the SEPA Credit Transfer Instant covering credit transfers in the eurozone. In conjunction with SEPA Credit Transfer Instant, EBA Clearing launched RT1, its pan-European solution for instant payments in euro. In the US, The Clearing House launched a real-time payments service with its member banks in November 2017. This after years of cajoling from the Federal Reserve and many hours spent debating and discussing such a service by its Faster Payments Task Force. And Australia launched its New Payments Platform (NPP) in February 2018, aimed at supporting the need for real-time payments in a digital economy.

All of these changes in structure, protocols and platforms bring many things to a market. Their proponents hope that creating an environment that supports payments, at any time and on request, will promote innovation within the industry as well as answer many growing needs put forth by the digital economy.
However, the lure of the new not only attracts progress, it also attracts fraud. Criminals and fraud have been around almost as long as people have started accruing wealth. Separating a fool from his or her money — or simply stealing — is truly one of humanity's oldest practices. So while fraud, scams and good old-fashioned stealing isn’t new, major overhauls of infrastructure and protocols do present casual and professional criminals with an opportunity to employ new tactics and strategies to ensure successful nefarious activities.

Legacy prevention tactics that sought to protect consumers and businesses from fraud in the past often had time on their side. Paper checks — perhaps written for a charming, soon-to-be-unveiled con artist — could be stopped days before money left your account. Older electronic systems, such as BACS, would give a bank three days to monitor and analyze current accounts for unusual activity, giving both the bank and its customer a chance to query and identify out-of-the-ordinary payments, such as a newly created standing order or direct debit that does not match personal history.

With real-time payments, the time between a payments request and final settlement is often, at most, 10 or 12 seconds. Much like realizing you lost £10 to a street hustler playing three-card Monte, when a payment is completed within a system such as the UK’s Faster Payments, that money is gone.

Fraud analysis and prevention procedures need to be much quicker in today’s 24/7, on-demand, digital world.

The paper will seek to outline the changes in risk management, fraud prevention strategies, and operational techniques needed by banks and financial firms in order to manage a real-time, on-demand payments environment.
Section 1: What exactly are “real-time payments”?

How is it defined in the UK?............................................................................................................................4
How are real-time payments beneficial for the digital economy?.........................................................................6
How have real-time payments been rolled out around the globe?.........................................................................9

The dawn of real-time payments

As one of the first real-time payment schemes and arguably the scheme that has the most mass adoption, the UK Faster Payments Scheme (FPS) is a valuable case study. For banks and industry bodies in those geographies that have just started on their path to ubiquitous real-time payments there is much to be learned from what has happened in the UK.

FPS is a payments-clearing scheme for electronic sterling payments in the UK. Most electronic payments sent through FPS will arrive at the recipient bank on the same day — as long as both the sending and the recipient banks are participating in the scheme and the payment amount falls within the scheme limit.

FPS was initially launched in 2008 with a limit of £10,000, rising to £100,000 in 2010 and to a further £250,000 in 2015. Despite those overall limits, individual risk appetites still determine what is allowed to be sent and received, via FPS, by each participating bank. A smaller building society in the UK, such as Nationwide, may set its FPS limit at £10,000, while a larger global bank such as HSBC would allow the full £250,000. Faster Payments can be made via online banking, mobile banking, telephone banking, in branch or self-service kiosks. It can also be used as the rails on which other payment mechanisms run, such as person-to-person payments and ewallets.

At launch, nine banks and one building society, accounting for about 95% of payments traffic, initially committed to use the service. As of 2018, Faster Payments lists 19 directly connected participants in the scheme. Those banks are:

<table>
<thead>
<tr>
<th>Barclays Bank</th>
<th>BFC Bank</th>
<th>Citibank</th>
<th>Clearbank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clydesdale Bank</td>
<td>The Co-Operative Bank</td>
<td>HSBC</td>
<td>HSBC UK</td>
</tr>
<tr>
<td>Lloyds Bank</td>
<td>Metro Bank</td>
<td>Monzo</td>
<td>Nationwide</td>
</tr>
<tr>
<td>NatWest</td>
<td>Northern Bank</td>
<td>Raphael Bank</td>
<td>Royal Bank of Scotland</td>
</tr>
<tr>
<td>Santander</td>
<td>Starling Bank</td>
<td>Turkish Bank UK</td>
<td></td>
</tr>
</tbody>
</table>

As of early 2018, both Barclays International and Atom Bank, the mobile-only offshoot of Metro Bank, are in a testing phase to directly connect to FPS.

For a retail customer, the Faster Payments organization (known as the Faster Payments Scheme Limited (FPSL) in the UK describes a payment between two friends, “Simon” and “Mike.”

Simon owes his friend £50. He instructs his bank, via mobile, online or the telephone, to send £50 from his bank account to his friend Mike’s account at a different institution. Simon’s bank carries out its normal checks to verify that he is the genuine customer. For example, they may ask Simon to provide a password or other security information.
Simon also provides Mike's sort code and account number — this is the information used to address the payment. The FPSL offers an online sort code checker, accessed via its website, to ensure that the corresponding bank is set up to receive Faster Payments. Mike's name also appears on the payment, acting as a reference for the friends.

Before Simon's bank allows the payment to be made, it will check that Simon's account has sufficient funds and that the request to make a payment is genuine. In certain cases, the bank may need to hold the payment to undertake further checks to protect Simon. This stage of the transaction is crucial to any fraud management, as once the payment is made, reversing or stopping the payment is impossible. Once Simon's bank sends the transaction through FPS, he is committed to making that payment.

Once the payment reaches Mike's bank, it checks that the account number is valid, but does not check that the name on the account and the account number match. The onus on that information being correct lies with the sender. The receiving bank then sends a message back to the sending bank on whether the payment has been accepted or rejected. If accepted, Mike is paid the £50 he is owed and Simon's bank receives a message confirming successful payment.

If both Simon's and Mike's banks are participants in the Faster Payments scheme in the UK then all of the above should take a few seconds to complete. Prior to 2008, with the older BACS payment system, this process took three days.

BACS is still used in the UK for some payments, and between parties where not every firm is a participating member of FPS. Despite tests to increase the limit on Faster Payments to millions of pounds, CHAPS is currently used to support high value payments. CHAPS is most often used when people are buying a house, for example. BACS payments are protected by The Direct Debit Guarantee, which is offered by all UK banks that accept direct debits. This guarantee is used in case there is an error in a payment, and not to mitigate contract disputes between payees and creditors. As for CHAPS, if a customer is found to be a victim of fraud, they are entitled to a refund of their payment. For errors, a bank must make “reasonable” efforts to correct the transaction, but does not guarantee a refund. Faster Payments holds no such guarantees.

**Staying with the UK system, these are the following payments that are allowed:**

- **Single immediate payments** made by customers in a bank branch, via mobile, online or on the telephone, 24 hours a day, seven days a week.

- **Forward-dated payments** are one-off payments sent and received on a pre-arranged date, set up by the customer in advance. These are typically used to pay bills, rent, etc.

- **Standing orders** are a regular payment that pays a fixed amount to the same recipient on regular dates, such as the first of the month. Payments can be sent Monday through Friday, excluding bank holidays. If the pre-arranged date falls on a weekend or bank holiday, the payment is made on the next working day. It is not possible to guarantee the exact time the payment will reach the recipient’s account, although at least 90% of standing order payments are sent by 6:00 am.

- **Direct corporate access payments** is a service for business customers that enables bulk files of payment messages to be sent directly to the Faster Payments Service. Not all Faster Payments Participants offer Direct Corporate Access, but they offer alternatives for their business customers.
Geographies that are newly adopting real-time payment schemes are aiming to make them ubiquitous and the UK example shows how achievable this is. In December 2017, Faster Payments processed 150 million payments, which is a 20% increase on the amount processed in the same month in 2016. In total, the amount processed in 2017 rose by £210.7 billion compared to 2016, making the total amount transferred in 2017 over £1.4 trillion. Since its launch in 2008 in the UK, Faster Payments has served as the rails for the launch of Paym, a person-to-person payments system used by participating banks, to enable payments using consumers’ mobile phone numbers.

According to global bank HSBC, which was one of the founding participants for Faster Payments, its statistics (along with those of UK trade association Payments UK, now part of Finance UK) show that while corporate usage is growing, consumers still initiate more FPS transactions than businesses. Reasons why business usage has not grown to a greater extent may include the cost of the service and the use of the ISO 8583 format, rather than ISO 20022 XML. The UK scheme was developed before widespread global use of ISO 20022 became prominent. However, it means that limited information is provided for reconciliation, with no return transaction codes, and these are so important in the B2B workflow.

Geographies that have recently launched real-time payments schemes are using the ISO 2022XML standard — this means that it is more likely that B2B usage will gain traction.

Speaking to financial technology newswire, Finextra, Carina Olsson, Director of Payments, Bankgirot, a clearing house in Sweden, lays out the benefits of rolling out a real-time payments infrastructure.

Olsson says that Bankgirot has been working on establishing a real-time payments infrastructure (called Payments in Real Time in the region) together with their member banks and the central bank in Sweden, since 2012. One of the main benefits of the new payments infrastructure is the opportunity to replace cash, not just reduce cash use, as well as compete with card transactions, says Olsson. “Sweden will probably be the first cashless society in the world; we will demand real-time services,” she adds.

The opportunities of payments in real time present the opportunity for the financial system in Sweden to be open, instant and irrevocable, and enable settlement 24 hours a day, seven days a week, says Olsson. All of this should be available in an environment that allows for settlement without risk between the participating banks, she adds.

*An open infrastructure that a payments provider or banks can participate in, if they fulfill requirements, is the best way to do it. We can also see that an open infrastructure means that the banks, or payments service providers, can make new offers and make new services that are overlaid on top of the payments infrastructure,* says Olsson.

Much like the Paym consumer person-to-person payments service using mobile phone numbers was built on top of the existing Faster Payments rails in the UK, Sweden is also rolling out new applications as a result of this new payments environment.
One recent application, built on top of the real-time payments infrastructure in Sweden, has already been downloaded by six million people, says Olsson. With a population of 10 million in Sweden, that means almost every "adult between the ages of 13 and 65" has downloaded the new payments app. "Real-time payments are here to stay and will be the new normal," she says.

The experience in Sweden is echoed even by banks with a global reach, such as HSBC. Writing in their Insights blog early last year, HSBC describes the buzz around instant payments.

"The digital economy and the rise of mobile banking for consumers and corporates have provided a strong platform for faster payments, with an expectation that decision-making should be able to be done on the go. Professional life is now expected to echo consumer experiences. The exponential growth of mobile has further nurtured this expectation.

This is not the only driver behind the rise of instant payments. Regulators are also pushing for these schemes to reduce the use of cash, as we have seen in India, and to help tackle financial crime and fraud. Equally, regulators are looking to provide greater access to payment services for under-banked or unbanked consumers, as a means of social inclusion.

Over time, the features of these schemes have matured and become increasingly connected to the digital economy."

Recently, HSBC built a mobile collections service, specifically for recurring B2C payments, on top of the Unified Payments Interface (UPI), the instant real-time payment system in India. The UPI was developed by the National Payments Corporation of India enabling inter-bank transactions. The interface is regulated by the Reserve Bank of India and works by instantly transferring funds between two bank accounts on a mobile platform. India has an 80% mobile phone penetration, with over 1.05 billion mobile phones and 220 million smartphones in use.

In India the UPI enables the transfer of funds instantly between person-to-person and person-to-merchant using a smartphone. UPI can be used to send and receive funds. This platform allows both payer and payee initiated payments. The platform offers users access to different bank accounts, by way of a virtual payment address (VPA). The user can avoid disclosing actual account details and it operates 24/7/365. The current transaction limits are 20 transactions per day with a maximum value of INR 100,000 per day.
While real-time payments services continue to be developed around the world, not every payment is suited, or even requires, a new payments infrastructure. In 2015, Swift, the bank-owned global financial messaging provider, provided the results of a survey that looks at the types of payments suited to real time.

Swift concluded that some, but not all, payment types may benefit from, or be suitable for, real-time availability and confirmation of funds transfer. In broad terms, the study findings showed a strong or a very strong case for:

- The immediate funds availability and immediate confirmation for large-value purchases, across P2B (e.g., houses and cars) and B2B segments (e.g., one-off invoices).
- The immediate funds availability and immediate confirmation for urgent P2P money (remittance) transfers between individuals, and for B2B urgent invoice payments in order to optimize working capital.
- The immediate notification for P2B e/m-commerce, with a medium case for immediate funds availability for both physical purchases (e.g., books) and digital goods (e.g., online newspapers, documents, games, music).
- The immediate notification at P2B point of sale (POS), but a weaker case for immediate funds availability.

The case is weaker for immediate funds availability and confirmation for P2B bill payment, including direct debits, and for B2P salaries and pensions. This is not surprising as these payments are typically scheduled in advance, on a defined date or with a defined frequency, and the incremental value of having the payments transacted on the predetermined date in real time is, arguably, marginal.

For merchants, the survey also revealed that the desire for real time is supplemented by the need for convenience (introduction of new mobile POS and new applications; for example, Apple Pay), for cost effectiveness (drive towards credit transfers as alternatives to credit and debit card payments), and for increased understanding of consumers’ purchasing habits, to develop loyalty programs and maximize cross-selling opportunities. The results of the survey reflect the potential use cases for real-time payments globally. The use cases may be different in specific markets; for example, POS payments are not candidates for immediate funds availability in the US, where the existing payment instruments represent a convenient and well entrenched alternative.

The emergence of digital payments, value-added services and the push for immediacy are having a knock-on effect on underlying Payment Market Infrastructures, which were originally designed to process relatively simple payment information in bulk files, either at the end of the day or overnight, according to Swift. To satisfy “immediacy,” the underlying payment systems would have to provide:

- Instant and irrevocable debiting of payers’ accounts and crediting of payees’ accounts.
- Immediate confirmation to both parties that the funds have been transferred, and can be reused immediately.
- Service availability on a 24/7/365 basis.

Although real-time payment services may differ in some aspects (for example, the type of instrument, or the authorization mechanism), they aim to offer the same thing: a real-time funds transfer service to end consumers and businesses, so that the beneficiaries can reuse the funds immediately.
In addition to the UK, Sweden and India, there are more than 30 existing instant payment schemes around the globe — and more being implemented, according to professional services company Accenture. The majority of these schemes are based on 24/7/365 availability and are real or near-real time.

**Most of these real-time payment schemes adhere to several characteristics:**

- Instant and irrevocable debits and credits to customer accounts
- Service availability 24/7/365
- ISO20022 XML format used in many schemes supports additional remittance information
- Immediate confirmation to both payer and payee
- Participation in overlay or value-added services

One of the first major financial centres to launch an immediate payments system, after the UK, was Singapore in March 2014. **FAST (Fast And Secure Transfers)** is an electronic funds transfer service that allows a secure and almost immediate transfer of Singapore dollar (SGD) funds between accounts held in the 20 participating banks. Much like the UK, prior to the rollout of FAST, interbank funds transfer could take up to three working days.

According to the Association of Banks in Singapore (ABS), FAST was introduced in response to the increasing demand from consumers and businesses for funds transfer that is faster and more efficient.

Customers in Singapore can make interbank funds transfers, on a 24/7 basis, of up to $50,000 per transaction, subject to their daily or monthly withdrawal limits. Security for FAST is equal to the security standards established by the banking industry in Singapore for funds transfers.

FAST is accessible via a bank’s internet banking service using electronic devices such as tablets, smartphones or personal computers. The accountholder’s name and bank account number will be needed to transfer funds, but only between the 20 participating banks in Singapore. The older Interbank GIRO is still used in Singapore to transfer funds between a participating bank and a non-participating bank.

The 20 participating banks are:

<table>
<thead>
<tr>
<th>Sumitomo Mitsui Banking Corporation</th>
<th>Royal Bank of Scotland</th>
<th>BNP Paribas</th>
<th>CIMB Bank</th>
<th>Citibank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank of Tokyo-Mitsubishi UFJ</td>
<td>Deutsche Bank</td>
<td>Far Eastern Bank</td>
<td>HL Bank</td>
<td>Mizuho Bank</td>
</tr>
<tr>
<td>HSBC Bank (Singapore) Limited</td>
<td>United Overseas Bank</td>
<td>Bank of China</td>
<td>Maybank</td>
<td>OCBC Bank</td>
</tr>
<tr>
<td>Standard Chartered Bank</td>
<td>DBS Bank/POSB</td>
<td>ANZ Bank</td>
<td>HSBC</td>
<td>RHB Bank</td>
</tr>
</tbody>
</table>

As with other immediate payments schemes, consumers need to be careful they key in the correct amount and bank account number as funds transferred via FAST will be credited to the recipient’s bank account almost immediately.
In terms of security and fraud prevention, the ABS advises consumers that as with other electronic funds transfer services such as via ATM or internet banking, customers should confirm with the recipient on his/her bank account number, and exercise due care in keying in the recipient’s bank account number when using FAST services. Funds transferred via FAST will be credited to the recipient’s bank account almost instantly. If customers have transferred funds to a wrong bank account, the ABS recommends that they should inform the bank immediately. The participating bank will investigate and follow up with the recipient/recipient’s bank to return the funds. The bank may also advise its customers to lodge a police report, if theft is suspected, to facilitate their investigation.

In Europe, harmonization of direct debits and credit transfers has been running the Single Euro Payments Area (SEPA) for 10 years. Work on developing immediate payments environments has been ongoing within separate countries and EU-wide for almost as long. In November 2017, the European Payments Council (EPC) went live with SEPA Instant Credit Transfers (SCT Inst) enabling pan-European credit transfers with the funds made available on the account in less than 10 seconds.

Much like other global regions, the EPC’s reasons for launching an on-demand payments service point to changes in the digital economy and customer-enabled technology. According to the EPC, “With the spread of smartphones and electronic commerce, the digitalization of the economy entails a general acceleration of payments. Customers make internet purchases anywhere and at any time, including during evening hours, weekends and holidays — periods when most traditional electronic payments are not operational. Suppliers, on the other hand, want the certainty of being paid as soon as they sell their goods and services.”

The SCT Inst goes further than other immediate payments services as it also aims to support businesses, large companies and administrations, as well as consumers. The SCT Inst works like a regular SEPA credit transfer, but instead of having to wait up to one business day, beneficiaries receive funds in a matter of 10 seconds maximum. That means that the checks performed by the beneficiary’s payments service provider and the clearing and settlement of the transaction have to take place within this 10-second threshold.

The EPC itself admits that “this is a challenging undertaking for PSPs in terms of risk management. To limit the risk of fraud, the maximum amount per SCT Inst transaction is limited to 15,000 euros for the time being.” The transaction has to be denominated in euros, even if this is not the currency of the account of the originator and/or beneficiary of the payment.
According to Ignacio Echevarria Gayubo, head of treasury solutions Europe at BBVA, the SCT Inst scheme extends the geographic reach of real-time irrevocable payments to SEPA. Launched in October 2016, 27 Spanish banks launched Bizum, a mobile phone payments service that links a mobile phone number to a bank account and enables immediate transfer of funds without having to know the account number or any other beneficiary data to make a payment. Bizum can now be extended throughout the eurozone using SCT Inst as a railway system to SEPA.

In conjunction with the EPC’s SCT Inst, EBA Clearing launched RT1, an infrastructure solution for the processing of instant SEPA credit transfers at a pan-European level. It supports payment service providers in transferring euro transactions between payment accounts in less than 10 seconds end to end, with immediate availability of the payment amount to the beneficiary.

Late in 2017, the US saw the first major change in its payments infrastructure in many years when the American bank-owned ACH The Clearing House (TCH) launched its real-time payments system (RTP). The RTP enables consumers and businesses to send and receive domestic payments in seconds, rather than days. BNY Mellon and US Bank carried out the first payment on the system, with several of TCH’s 25 owners, including Citi, JP Morgan and SunTrust, set to follow suit as early adopters. Open to all US depository institutions, the system is expected to be used by banks holding more than half of all deposits by the end of 2018. TCH hopes the service will become "ubiquitous" by 2020. That platform was developed by Mastercard-owned Vocalink, which has helped build the RTP system, ensuring that it not only supports fund transfers, but also the ability to both request payments and provide critical information.

This, says TCH, means RTP will support more seamless and efficient e-invoicing, bill payments, insurance claim payments, cash-on-delivery payments and more. The platform also provides transparency and certainty with immediate confirmation notices that payments have been sent and received and instantaneously settled.

According to the TCH, banks are looking to reduce their own processing costs but will initially have to spend time and money to configure their own systems to route payments in and out of the plumbing of RTP. Existing systems have largely sent payment instructions in batches through industry pipes, usually toward the end of the day. The existing systems have tools to check for mistakes and guard against money laundering, and those steps will have to be sped up to use RTP.

Speaking to payments newswire PYMTS.com, Dan Massey, SunTrust Bank’s Chief Technology Officer, talked about becoming one of the early adopters of TCH’s RTP technology and announced a new integration with person-to-person payments network Zelle.
“Our purpose is really to help light the way to financial well-being and financial confidence for our clients, and we consider faster payments to be a really important part of that,” he said. “It’s about making sure they can move their money and manage their money faster, more conveniently and with more confidence in the security of those transactions,” said Massey.

SunTrust was one of four other banks — on a list that included JPMorgan Chase & Co., Citigroup and PNC Financial Services Group — to become early adopters of RTP in the US.

The company’s adoption of same-day ACH technology was the “culmination of a three-year-long effort” to make faster payments capabilities a reality, Massey said.

After bringing the TCH RTP system live to its customers, SunTrust Bank also partnered with Zelle, which competes with the well-known P2P payments network Venmo in the US. The partnership, which launched in December, gives SunTrust customers the ability to make transfers and split payments using its mobile or online banking solutions.

SunTrust is planning several faster payments initiatives in the early months of 2018, Massey said. Those include changing certain aspects of existing offerings, adjusting transfer limits and dealing with new usage patterns or cybercrime threats.

On demand, down under

The most recent system to go live is the New Payments Platform (NPP) in Australia, which opened business to consumers in February 2018. The NPP enables real-time clearing and settlement for simple or complex payment solutions, between two or more people. It can simplify payments through an Addressing Service, as well as offer the ability to include more information with payments, such as text or links to externally hosted documents.

It is being collaboratively developed by NPP Australia Ltd. and 13 financial institutions, and when it goes live later this year a large number of additional financial institutions will also connect to the infrastructure through one of the initial participants.

According to a spokesperson for NPP Australia Ltd., Australian financial institutions implemented same-day direct entry clearing and settlement several years ago, so they have a good understanding of the challenges of fraud (unauthorized transactions) detection in a shortened clearing cycle. Mobile and online banking is also well established, with very good industry practice around customer identity verification, authentication and transaction monitoring/pattern detection.

However, the role of the consumer in fraud prevention is also important to Australia’s real-time payments project. The spokesperson argues that the “potentially more significant category of potential loss relates to scams, which result either in customers making authorized transactions to scammers, or disclosing their online banking credentials to scammers, resulting in account compromise.”
The NPP will support payment initiation by PayID (a proxy for an account) and by BSB/account number. Where a payment is PayID-initiated, the name associated with the account is displayed to the payer before payment is authorized. The use of the PayID name display function is expected to reduce the risks of authorized payments relating to ID takeover scams. “As always, consumer scam awareness and consumer education about tactics scammers use are central to minimizing this category of loss,” says the spokesperson. NPPA has produced some scam awareness collateral that will be publicly available once the NPP becomes publicly available. Participating banks and financial institutions have traditionally taken the lead in educating and protecting consumers about security and scams - this will continue once the NPP is available.

It is the sharing of information and industry collaboration that factors high in any region’s fraud prevention tactics. “There are a number of collaborative industry fora established to enable this collaboration, but perhaps the most fully resolved is the Australian Financial Crimes Exchange (AFCX). It was established by the major banks with the backing of the Commonwealth Attorney General’s Department, but is open to all financial institutions. It brings together ‘businesses, government, law enforcement agencies and industry groups to protect Australian consumers and businesses from the growing threat of fraud and financial crime by providing leading security capabilities, technology and intelligence in one central platform’,” says the spokesperson.

Australia is well versed in many of the lessons learned from other real-time payments environments around the world. There is a consensus that while faster payment systems create no new fraud risks, the payment processing velocity and payment irrevocability does create new challenges for financial institutions, consumers and consumer protection agencies.

The Australia authorities are looking out for various types of fraud. According to the spokesperson, those include:

Fraud (unauthorized transaction) detection/prevention, particularly for institutions that are unused to shorter clearing cycles (i.e., overnight batch systems) — “Australian banks are well-placed to meet the challenge of preventing unauthorised transactions. They have existing experience in providing mobile and online banking services where short clearing cycles have been in place for several years” said the spokesperson.

Dealing with scams — In this regard, consumer awareness and education about scam typologies and device/password security are vital, perhaps the single strongest tactic to prevent customer losses. “We also expect the PayID name display functionality to help reduce the risk of customers making payments to perpetrators of ID takeover scams,” adds the spokesperson.
Section 2: What impact do real-time payments have on fraud?

Keeping pace with the fraudsters

Any financial system, especially one that deals with the transaction and transfer of money, is subject to a wide array of security threats. Pickpockets, confidence tricksters and other nefarious characters have been scamming ordinary people and businesses for centuries. However, the advent of the digital age has offered fraudsters new gateways and avenues in which to steal funds. Within a real-time payments infrastructure — where the time it takes to request, send and receive a payment is seconds, rather than days — the need to find more dynamic and quicker prevention and response strategies is ever more apparent. Throughout the internet age, it became convenient to steal credit card numbers in batches, either by hacking the merchant directly or by setting up dummy merchant accounts — a type of identity theft in order to commit fraud. Regulations and mandates on the security around storing and handling card data helped a bit to combat this type of criminal behavior. Today we’ve seen card schemes such as Mastercard and Visa, as well as merchants, add increased verification checks for online purchases.

The introduction of EMV (or chip and pin) for plastic cards has also significantly reduced card-present fraud worldwide. According to a report from Aite Group and Iovation, as more US-based merchants become EMV-capable, counterfeit fraud will fall from a high of $4.5 billion in 2016 to less than $1 billion in 2020.

However, that report also predicts that card-not-present fraud will cost retailers and financial institutions $7.2 billion in the US by the end of 2020. The report also found that bank account takeover losses will increase from $644 million in 2015 to more than $1 billion by 2020.

As the payments ecosystem evolves, with contactless payments within the Internet of Things, and other forms of biometrics payments, the availability of multiple channels and the interconnectivity of omni-channel offer additional avenues for fraudsters to explore. So we know that all payment systems, whether real-time or not, are subject to a wide array of security threats and other risks that are ongoing and constantly changing.

Real-time payments — real-time fraud

While fraud and crime are not new, real-time payments systems are being exploited to rapidly move the proceeds of crime between accounts, to a large degree thwarting the analysis and efforts by FIs to identify and track illicit funds and create a path for repatriation.

Vocalink, the Mastercard-owned, UK-based, real-time payments platform provider (which underpins both the UK’s Faster Payments and the immediate payments system in the US), has identified a common scam exacerbated by Faster Payments — mule fraud.
Money laundering and mule networks are not new. Organized crime often set up accounts in order to move the proceeds of crime through a network, obscuring their source, and extracting funds. This makes recovery by financial institutions nearly impossible.

Broadly, mule networks are a collection of linked accounts, belonging either to individuals or businesses, that are used — sometimes without the knowledge of the account owner — to move proceeds from criminal activity, effectively laundering the money.

While new payments infrastructures, which are available 24/7 and on demand, are efficient and convenient to consumers and businesses, those same payments infrastructures also offer those benefits to criminals. While mule fraud relies on a series of linked accounts, the speed at which money is now transferred via a real-time payments environment puts an immense amount of strain on legacy technology and manual anti-money laundering processes.

Once a payment leaves an account via a real-time payments scheme, the bank or financial institution has a limited view of the entire payments flow. They don’t see what happens to payments once they leave them and enter the system. This also makes it difficult to see and trace patterns that could point to criminal activity.

The UK did see a spike in fraudulent activity such as mule fraud once UK Faster Payments went live 10 years ago. Bank accounts set up prior to the launch of UK Faster Payments served as the links — or mules — for money laundering. Bank accounts were compromised quickly and easily. Payments between consumers and businesses were intercepted using malware and then redirected to the mule accounts. Once this fraud was recognized, some UK banks moved to address the issue by implementing real-time fraud detection software with a machine learning model that enabled banks to block payments.

Analyzing two years’ worth of UK Faster Payments data, Vocalink found that money mule networks in the UK extend across the industry, are not localized and affect all FIs. Analysis shows a fundamental difference in the behavior of suspect mules compared with normal accounts, and that they move money rapidly through networks of accounts in order to hide the true origins of funds. Finding and identifying these mule dispersions is key to combating this fraud. Because mules bounce between accounts, individual transaction activity does not signal any red flags within risk management systems. However, viewing these individual patterns of behavior as a whole can be a strong indicator of illegal financial activity.

The National Crime Agency estimates that money laundering activity can amount to some 2.7% of global GDP or US$1.6 trillion in 2009. The NCA assesses that many hundreds of billions of pounds of international criminal money is laundered through UK banks, including their subsidiaries, each year.
Invoice fraud is common and simple. Many in the banking community point to the upcoming requirements in the UK to ring-fence parts of the banking business as being linked to an increase in instances of invoice fraud. Ring-fencing of day-to-day banking services is one of the reforms brought in by the UK government, aiming to strengthen the financial system following the financial crisis that began in 2008. By April 2018, banks will need to set up a new ring-fenced bank, serving both consumers and businesses, which will be separate from other parts of the bank — such as the investment bank.

However, with Faster Payments, if invoice fraud is not caught early, funds are transferred and gone from accounts in a very short space of time. Many of the UK banks are aware of invoice fraud and go to lengths to educate and inform their customers about the dangers. For example, one of the main UK incumbent banks, Barclays, writes on its website:

“Barclays is aware of incidents where companies have paid out sums in excess of £1 million to fraudsters, in the belief they were paying a genuine supplier. Often the error is only spotted when the genuine supplier chases a payment that they haven’t received — by then it can be too late and the fraudsters have withdrawn or moved the money.”

Invoice fraud depends on humans not noticing errors in account details. For example, a fraudster will send a change of bank details request by post, email or even by phone. They can also intercept genuine emails containing invoices and change the bank details or send an invoice including new bank details.

Fraudsters will often impersonate known suppliers of accountholders, relying on an element of trust. If the scammers are successful in getting an accountholder to pay an invoice, with fraudulent details, they will then submit multiple invoices until the fraud has been discovered.
According to DCI Andrew Gould, a detective on the Metropolitan Police’s anti-fraud taskforce: “Invoice fraud can be devastating. It is important that employees are able to spot the signs of an attempt and that a strict policy is in place when making changes to payment details. This should require checking the changes with the company concerned by contacting them directly through existing contacts, as well as requiring a manager to check and sign off the changes.”

UK Finance lists a number of strategies to combat invoice fraud. Those include:

- Always verify requests for changes to a supplier’s bank details using details previously held on file.
- If you are suspicious about a request made by phone, ask the caller if you can call them back. Fraudsters will attempt to pressure you into making mistakes — take the pressure off by taking control of the situation.
- When an invoice has been paid, inform the supplier, including the account the payment was made to. Again, use details previously held on file.
- Consider removing information such as testimonials from your own or your suppliers’ websites or social media channels that could lead fraudsters to knowing who your suppliers are.
- Look carefully at every invoice and compare it to previous invoices received that you know to be genuine — particularly the bank account details.
- Check the company logo — you will often find blurry logos on fake invoices.
- Check the email address that you’ve received an invoice from carefully. Fraudsters will use addresses that are similar to a genuine address; for instance, ending in .org instead of .com.
- Apply the same principles to requests from within your own organization.

If invoice fraud is suspected by a customer, most banks suggest that you contact them immediately, giving the bank a greater chance of recovering the funds. In the UK, it is also advised to report fraud to ActionFraud — the police’s national fraud and cybercrime reporting center. [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

A subset of invoice fraud is Boss or CEO fraud, where someone poses as a boss of a company instructing staff to make a wire transfer into the fraudster’s account. Fraudsters pressure victims into acting quickly, without thinking, usually during a busy period — which is a standard feature of this type of fraud.

This type of scam is effective because emails that seem to be from the CEO can easily bypass spam filters and antivirus security systems, since there are no attachments nor malware with the email. The fraud is perpetrated by a simple conversation.

Fraudsters use publicly available corporate data, such as from LinkedIn, to make the emails as convincing as possible. Staff are less likely to question instructions purporting to come from on high. It’s a psychological manipulation, often accompanied by a sense of urgency — that is a major factor in the fraud’s success.
Faster Payments Task Force

Instrumental to the launch of an immediate payments service in the US, the Faster Payments Task Force is a group of stakeholders with representatives from financial institutions, non-bank payment providers, businesses (merchants and corporates), consumer groups, federal and state government agencies, regulators, standards bodies, industry trade organizations, consultants and academics. Acting as a catalyst, the Federal Reserve convened these stakeholders to work collaboratively to identify and assess alternative approaches to implementing safe, ubiquitous, real-time payments capabilities in the United States.

Since concluding its work of reviewing real-time payments solution proposals, the Task Force presented a roadmap for Faster Payments that makes several reconditions for security and fraud prevention. The report highlights several risk factors related to payments fraud and real-time payments environments. Namely, the time (or lack of time) allocated for risk analysis, the irrevocability of a payment and the responsibility of the industry to consumers who have been victims of fraud.

Within the report, The Faster Payments Task Force — Final Report Part Two: A Call to Action, the Task Force in the US concluded that addressing these risks in an effective way encompasses several elements.

- Strong security to protect data and transaction legitimacy, and minimize and contain data breaches, cyberattacks and other threats.
- Effective processes, practices, and controls within and across solutions in order to minimize and mitigate fraudulent and erroneous transactions.
- To establish effective dispute resolution processes and end-user protections to safeguard against financial and other losses.
- Effective management of settlement risk for minimizing potential losses due to one or more service providers being unable to meet their settlement obligations.

As the Faster Payments scheme is still in its infancy in the US, the Task Force encouraged the industry to take advantage of this period of transition. According to the report: "Before new, real-time solutions are broadly adopted, the industry should embrace a security-first mentality. While it will never be possible to completely thwart ever-evolving payment security threats, implementation of these new, real-time payments solutions presents a once-in-a-generation opportunity for all participants (solution operators, service providers, financial institutions, government agencies, businesses and consumers) to embrace the latest best practices and security features in a comprehensive, holistic manner."

As outlined earlier in this report, a real-time payments structure means that accurate identification of payers and their accounts must occur during a short vetting window, making it challenging for payers’ service providers to recognize identity theft, account fraud and account takeover.
Several recommendations from the US Task Force are outlined as part of the roadmap. These include:

• Robust techniques for data protection, authentication, enrollment and payment identity management (e.g., end-to-end encryption, tokenization, behavioral biometrics and device fingerprinting) can and should be leveraged to protect data and stop fraud before it happens.

• Effective rules and standards can help encourage proper use of these security and fraud prevention techniques.

• In addition to real-time information exchange, the ability to flag exceptions quickly will be necessary to ensure trust in the integrity of the faster payments system.

• In order for e-commerce retailers, billers, government entities, processors and financial institutions to handle payment exception processing in real time, many participants will need to upgrade their technological capabilities as well as their operational and managerial controls.

As it is with other immediate payments schemes around the world, the real-time payments rollout in the US combined the availability of funds in real-time and irrevocability of the payment. Not surprisingly, the Task Force cites this as a “risk factor.”

However, according to the roadmap, “irrevocability is not the same as indisputability,” pointing out that “end users will want to be able to dispute unauthorized and erroneous payments.” To this end, the Task Force recommends that consideration needs to be given to the design of payer authorization processes and strong fraud and/or error resolution processes. “Poorly designed authorization processes can result in confusion and user errors, which could in turn lead to unauthorized payments and customer dissatisfaction,” according to the roadmap.

The main crux of the recommendations surrounding real-time payments and fraud in the US revolves around trust. The Task Force asserts that it is critically important for real-time payments solutions to have clear rules and effective processes for handling disputed payments, depending on whether those payments are authorized by the payer (such as victim-assisted fraud) or unauthorized (such as lost, stolen, counterfeit, account takeovers, or in some cases debit-pull arrangements that were not explicitly agreed to by the payer).

Very similar to the conversations in the UK, within the payments regulators and industry participants, in response to the Which? Super Complaint (which will be discussed in section 3), the US Task Force highlights that “guarantees and/or indemnities that protect end users from unexpected losses due to error or fraud may be necessary.”

In addition to the Faster Payments Task Force, the US Federal Reserve set up the Secure Payments Task Force (SPTF), a collaborative industry effort working to address payment security challenges broadly and advising this task force on real-time payments related security issues.
While previous efforts of the SPTF have focused on addressing the challenges of existing payment systems, the task force is now supporting analogous work streams for real-time payments, which they believe is critical to ensure the safety and security of the emerging real-time payments system. As recently as April 2017, discussions between members of the SPTF pointed to feeling “excluded” from governance surrounding fraud prevention and Faster Payments in the US. Barbara Bennett, Federal Reserve Bank of San Francisco, is on record assuring members of the SPTF that this feeling of exclusion was “not the case; rather, that the faster payments governance should be self-sufficient, not handing off responsibility to another group, and would coordinate with the SPTF.”

Within the remit of the Faster Payments Task Force, one of the recommendations pertaining specifically to the SPTF is the Fraud Data Sharing recommendation, which now includes fraud detection and reporting, not just data sharing.

Additionally, the responsibility for this recommendation now sits within the FPTF governance framework in coordination with the SPTF.

Fraudsters are humans, too

Keion Dalton is the Global Program Senior Director at Aspect Software, which provides insight around mobile and the challenges around compromising someone’s mobile identity.

According to Dalton, one of the most peculiar aspects of fraudsters is that they are humans. “Our patterns of fraud detection suggest that this is ‘their job,’” as in they work 9:00 am to 5:00 pm, Monday through Friday. “We also notice a pattern of reduced fraud during summer months as they go on holiday. So it’s safe to say, the fraudsters do travel but also utilize an industry of their own to manipulate the vulnerable in carefully targeted countries.”

In terms of best practice to combat fraud, industry collaboration is “slightly cliche but it’s vital,” says Dalton. “The timing pressure means it becomes a collective fight, as otherwise it will be too late.”

Because of this pressure, from a technology perspective, insights are needed from relevant dynamic data sources. This sometimes means looking for answers without having to access data from legacy technology within banks. Dalton calls this “trust agility.”

We use the term “fraud follows the channel.” Adoption of mobile, SMS, etc., means the fraudsters tend to follow the trends established — looking to channels as they become more prevalent — mobile and online, for example, says Dalton. In particular, fraudsters will look for loopholes in education and target the vulnerable. With immediate payments, takeover accounts and payments can allow the scammers to be gone before corrective action can take place.

But then, in the fight against crime, and the adoption of new methods of payment, “it becomes a fight for customer experience at the expense of fraud,” he adds.
Section 3: A look at the Which? Super Complaint — Is there a fine line between responsibility and liability?

In September 2016, Which?, an independent, non-political consumer organization in the UK, published a “Super Complaint” aimed at the financial services and payments industry to consider customer safeguards in the market for push payments. Push payments include BACS, CHAPS and UK Faster Payments.

The Which? Super Complaint provides relevant insight for any geography newly adopting real-time payments on what can happen when consumers are given the burden of liability for fraud.

The main gist of the complaint concerns when consumers are tricked into transferring money to a fraudster via a “push” payment (such as when the consumer instructs their bank to send money). The complaint argued that there is not an appropriate level of protection compared to other types of payments.

As was outlined in section 1 of this paper, once a payment has been made via UK Faster Payments, reversing that payment is impossible. This shifts the responsibility for fraud prevention to the person sending the payment, and it also shortens the time needed for risk assessment by the bank to a few seconds.

Specifically, Which? believed an investigation was needed to address the following:

• The extent to which banks could change their conduct to reduce consumer harm from scams that trick people into authorizing push payments to a fraudster.

• Possible changes to legislation or regulation to change the incentives on banks and payment system operators, and to ensure that more is done to manage the risks from these types of scams and to protect consumers from harm.

Which? argues that victims of authorized push payments (APP) scams do not receive sufficient protection from fraudsters in comparison to other types of payments (such as card payments and direct debits).

APPs are made when consumers instruct a bank to make a payment from their account to another account. This can be done over the phone, via online banking or in person. Most APPs are completed instantly. Scams involving APPs occur when consumers are tricked into authorizing a transfer of money to an account that they believe belongs to a legitimate payee.

Many participating banks in the UK have set up a working group to respond to the Which? Super Complaint. The Payments Systems Regulator, part of the UK Financial Conduct Authority, published a lengthy response to the complaint in December 2016.
The PSR responded that “in a short space of time” they built up a clearer understanding of the issue, and believe that this is a growing problem that needs to be tackled. Based on their investigation in 2016, the PSR concluded that:

- The way in which banks work together in responding to reports of scams needs to improve.
- There is some evidence to suggest some banks could do more to identify potentially fraudulent incoming payments and prevent accounts coming under the influence of scammers.
- The data available on the scale and types of APP scams is of poor quality.

However, most importantly, in 2016, based on the evidence the PSR had so far collected, “it is not sufficient to justify a change in liability, i.e., making banks liable for reimbursing victims of APP scams. However, as our work progresses and additional evidence comes to light we will consider whether it would be appropriate to propose changes to the obligations or incentives of banks for these scams.”

While important, liability is not the only driver for banks to tackle APP fraud. As the Which? Super Complaint shows, reputations are at stake and victims of fraud have been quick to go to the papers with their tales of loss. It is widely perceived that the banks can do more; for example, it is often commented that while an individual cannot easily carry out a behavioral risk analysis based on their transactions, a bank with the access to a wide dataset and the necessary tools can.

A year later, and work has been done

In November 2017, the PSR released a further statement on the work it has done to combat APP scams and address the Which? Super Complaint. New statistics published by UK Finance show that in the first six months of 2017 there were 19,000 victims of APP scams involving a total amount of over £100 million.

Showing a slight change from their findings in 2016, in 2017 the PSR began working to explore solutions that mean victims are less likely to be out of pocket. The PSR “think that a ‘contingent reimbursement model’ should be introduced to compensate victims in certain circumstances, and are now consulting to gather views on this.”

When the PSR published the December 2016 response, the regulator recognized that there were concerns around the lack of reimbursement for victims of APP scams. The regulator is now exploring a potential model that sets out the circumstances when APP scam victims would get their money back, and where it would come from. The PSR says: “We think that industry is best placed to lead the development of the model and that it should be implemented by end of September 2018 — we propose to actively monitor this work.”

However, as with most crimes and scams, the PSR reminds the industry that there is “no single solution, or ‘silver bullet,’ that can prevent all APP scams.” However, the regulator believes that the initiatives underway and the introduction of a reimbursement model should go a long way to help better protect consumers.
However, the PSR did publish this infographic to help identify and prevent scammers. In addition to examining the reimbursement model, the PSR lists several initiatives in response to the Which? Super Complaint.

- Industry has published the first set of robust statistics on APP scams, and from 2018 it will collect and publish more detailed data.
- The industry has now developed best practice standards that PSPs will follow when a victim reports an APP scam. This should improve victims’ experience and PSPs’ response times.
- The industry has developed a common understanding of what information PSPs can share under current law when responding to APP scam claims. Industry will be seeking to ensure that PSPs can continue to share this information under future legislation and will assist in work to facilitate the recovery of victims’ funds.

There are also a number of further relevant industry initiatives underway, such as Confirmation of Payee, sharing financial crime data and information, and transaction data analytics. Taken together, these will do more to prevent scams in the first place, assist with responding faster when they do happen, and help in recovering the victims’ money, according to the PSR.

The FCA also reviewed the way PSPs handle APP scams. It found PSPs’ procedures were inconsistent, their existing fraud detection systems could not easily detect APP scams, and they didn’t collect enough data.

## UK Finance Takes Five
A recent study by UK Finance, a trade organization for the UK banking and financial services sector, in response to the Which? Super Complaint, has shown:

- **Almost 7 in 10** business leaders admitted they hadn’t taken any action to protect their business and employees from an incidence of fraud.
- **A quarter** of businesses have admitted they have fallen victim to scams or had scams attempted.
- **Almost half** of all business leaders surveyed do not believe an act of fraud will be committed against them.
- The most common targets for fraudsters are senior management and business owners in SMEs (67%).

UK Finance represents nearly 300 of the leading firms providing finance, banking, markets and payments-related services in or from the UK. UK Finance has been created by combining most of the activities of the Asset Based Finance Association, the British Bankers’ Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association.

A constituent part of UK Finance, Financial Fraud Action UK, responsible for leading the collective fight against financial fraud on behalf of the UK payments industry, published a guide to potential fraud and advice for prevention in response to the Which? Super Complaint.
Financial Fraud Action UK says that while fraudsters are turning to more sophisticated methods of scamming people and businesses out of money, businesses are increasingly a target. Common tactics used include:

- **Sending spoof emails** impersonating a senior member of staff and trying to deceive employees into transferring money. The email usually requests an urgent payment, is made outside of normal procedures, often giving a pressing reason such as the need to secure an important contract.

- Criminals posing as regular suppliers to the company or organization make a formal request for bank account details to be changed. This is known as invoice fraud and fraudsters may trick a company into changing their bank account payee details for a sizeable payment.

- Criminals who specialize in invoice fraud are often aware of the full details of the relationship between companies and suppliers — they know when regular payments are due and, equipped with sophisticated information, they make contact with finance teams within companies and pose convincingly as suppliers.

- Mandate fraud criminals convince firms to change a direct debit, standing order or bank transfer mandate by pretending to be an organization the business makes regular payments to; for example, a subscription or membership organization or supplier.

While UK Finance estimates almost £100 million was lost to scams in the first six months of 2017, financial providers returned £25.2 million — almost a quarter of the losses. However, there are calls for legislative changes to ensure they do more.

Commenting on the PSR’s response to the Which? Super Complaint, Stephen Jones, Chief Executive of UK Finance, said:

“We are under no illusion that more needs to be done and we support the PSR’s desire to develop a mechanism to return more stolen funds to victims. We look forward to working with the PSR to secure the vital changes to legislation needed to enable the proposed refund model to work, and help deliver further positive change for customers as quickly as possible.”

Commenting on new industry data on authorized push payment fraud, Katy Worobec, Head of Fraud and Financial Crime Prevention, Cyber and Data Sharing at UK Finance, said:

“These figures confirm that criminals are enjoying a great deal of success targeting customers directly and tricking them into falling for their scams. There is no fast or surefire solution, but the industry is determined to crack down on these criminals on all fronts. Raising customer awareness is one weapon in the fight to stop these scams, which is why we are investing in the Take Five campaign.”
The Take Five campaign is a national awareness campaign led by FFA UK (part of UK Finance), backed by the UK government and delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector. It is aimed at increasing awareness of known scams and dispensing advice to consumers to combat fraud.

According to UK Finance, criminals use a range of tactics including invoice scams, house purchase scams and email hacking to target victims, and their scams can be very convincing. If a customer authorizes the payment themselves, current legislation means that they have no legal protection to cover them for losses — unlike other financial frauds where the criminal makes a payment without a customer’s consent.

While banks will always endeavor to help customers recover stolen money, customers typically only approach their bank after the payment has been processed, when they realize they have been duped. By this time, the criminal has often withdrawn the stolen funds and the customer’s money is gone.

In addition to building consumer awareness, the UK financial industry is considering a number of approaches to combat fraud and answer the Which? Super Complaint. Those include:

- **Repatriation of funds**: UK Finance says the industry is working with government and law enforcement on how to freeze and seize more stolen money to return it to victims. The implementation of the Criminal Finances Act will assist with this, but legislation is also being reviewed to see what changes are required to provide banks with a greater ability to return funds to victims. A change in the law would also allow criminal funds, currently frozen in bank accounts, to be potentially used to tackle fraud and scams and to help victims.

- **Collating industry data** to establish the scale of the issue and to monitor it going forward with updates provided twice a year. This data will help industry and law enforcement to tackle authorized transfer scams more effectively.

- **Considering longer term innovations to help customers better identify who they are dealing with**. This may include a system to verify payee name details before a payment is made. UK Finance supports the proposal to make such an innovation available as outlined by the Payments Systems Regulator’s strategy setting body — the Payment Strategy Forum. UK Finance believes this should be developed to provide assurance to customers that they are paying the intended recipient, while acknowledging that this system would only be possible with legislative changes to allow more data to be shared.

- **Putting measures in place to ensure customers who have fallen victim to fraud and scams get the help they need, no matter who they bank with.** Best practice standards will address issues such as around-the-clock availability of fraud specialists, consistent processes for notifying and assessing customer claims and blocking frauds.

- **Work with government on making possible changes to legislation concerning account opening procedures** to help the industry act more proactively on suspicion of fraud and prevent criminals from accessing financial systems.

- **Sponsoring a dedicated police unit** that specializes in tackling financial fraud and scams head on.
Following a restructuring of how the FCA grants banking licenses in the UK, the country has seen quite a few new “challenger” banks emerge to take on the dominance of the incumbent banks, such as Barclays, RBS, Lloyds Banking Group and HSBC. Two of the more well known challenger banks, and participants in FPS, are app-only Monzo and Starling Bank.

Starling Bank was launched in January and its application was made available on app stores in April 2017. Starling Bank’s age means that — unlike their older, larger banking rivals — Starling launched in the British market already connected to the FPS scheme, says Julian Sawyer, Chief Operating Officer at the bank.

The issue with Faster Payments is that the payments come from a restricted market. If you make a payment within SEPA, or via Swift or over Mastercard or Visa, you have a “murkier view” of the senders, but you have trust in the network, says Sawyer. For example, with FFP, Starling “can’t do AML checks on the sender” of a payment, he says. The bank has to “trust that if the payment comes from an account at Barclays, Barclays has done their checks,” adds Sawyer.

Sawyer says the issue isn’t around whether a real-time payments environment invites new types of fraud, but that the decision by the bank of whether or not to accept a payment has to be made in real time. “If they find out that transaction is fraudulent — then that money has left the banking system very quickly. A lot of banks have struggled with real-time analysis,” he says.

Although the time to react and analyze is truncated, Starling still employs similar fraud prevention practices used by any account-offering bank — namely looking out for unusual activity within customer current accounts. “We look for small payments that immediately leave — say £250 in, £250 out in a short period of time — that is not standard behavior, especially if it happens more than once,” says Sawyer.

Starling keeps tabs on regular income, such as from a monthly paycheck. “When you see a large unknown payment come in, you need to ask ‘are they trading Bitcoin? Or are they an EBAY seller.’ You look at the transaction and find information from the customer. If the client cannot convince the bank of the legitimacy of the payment, the bank can shut the account down,” he says.
Being a new bank, Starling anticipated that it would be a target for professional criminals at launch. Starling is a mobile and app-only bank. Accounts are opened online and not in a physical branch, like more traditional banks.

“Any new financial offering will always get hit. We knew we were going to be,” says Sawyer. In anticipation of the launch, Starling “raised the barrier” against fraudsters, he says. These strategies included:

- Real-time monitoring
- Giving staff the ability to change rules that could hinder customer onboarding or stop payments.
- Full engagement across customer service — to understand their role in fighting fraud.

Key to fraud prevention at Starling is humans. Its customer service staff are empowered to monitor onboarding and make decisions about unusual activity on customer accounts.

“Some might say that the key to fraud management is not to do real-time payments,” says Sawyer. “But we download movies in real time; payments should take only a handful of seconds. We feel, why shouldn’t it?”

For payment service providers outside of the UK, the Which? Super Complaint provides a valuable example. The issues raised are universal and have led to accusations of poor customer service and negative press — and many banks simply want to protect their customers. Those in geographies that are newly adopting real-time payments should take heed and consider the measures they can take to protect their customers and their reputations.
Section 4: Strategies around technology and innovation

How can AI, distributed ledger technology or tokenization aid in supporting fraud prevention strategies?

As we saw with section 2, while fraud isn’t new, a real-time payments environment can present new opportunities for criminals intent on stealing funds. Account takeovers, online banking fraud and cross-border transactions become more difficult to combat within new payments ecosystems. This is where technology can lend a hand. However, with any security method and technology, there tends to be a difficult balance between safety and user experience.

According to Financial Fraud Action UK, financial fraud losses across payment cards, remote banking and checks totaled £768.8 million in 2016, an increase of 2% compared to 2015.

However, at the launch of Faster Payments in 2008 fraud was up, according to several citations, as much as 300%. [https://www.financialfraudaction.org.uk/fraudfacts17/; https://www.biocatch.com/blog/faster-payments-faster-fraud; https://www.pymnts.com/news/2017/faster-payments-faster-fraud-biocatch-uri-rivner/]

While the infrastructure of Faster Payments in the UK in 2008 was strong, the new ecosystem offered weak entry points to transaction initiations, which were exploited by fraudsters, according to several observers.

Authentication was one issue that was highlighted as a weak spot. The players involved with Faster Payments introduced two-factor identification, tokenization and smart card readers to help combat this. In the past 10 years, fraud loss rates have significantly dropped as a percentage of the total value of faster payments transactions — they are now at lower levels than card payments.

In addition, Faster Payments requires all participants to adhere to a security code of conduct. This code outlines the controls participants must implement on their own payments systems and gateways and provides rules that financial institutions must follow to protect their end customers. This ensures that banks put sufficient controls in place while keeping the user experience consistent across different institutions.

The core risk issue is poor identity management. In order to prevent fraud, payment initiation needs to be more secure. This means using multi-factor identification to confirm payment parties. The use of behavioral analytics and biometric information are also being used when combatting criminals using remote access attacks and malware.
In addition to stronger authentication methods such as two-factor identification, other efforts include tokenization or smart card readers. Bank users in the UK are well acquainted with using tiny card-reader devices to enter on-demand passwords for payment requests. For users, this is very secure, however, fiddly and at times annoying to use — particularly if they need to make a payment on the go and don’t have the card reader with them. These stronger security methods just mean that fraudsters use other ways to obtain access to customer accounts; for example, browser attacks where, post authentication, malware could hijack a session and move money automatically.

The past few years, behavioral biometrics have been in use at several UK banks. Fraud driven by remote access seeks to understand and then mimic user behavior. Actions such as how customers interact with their devices, the keyboard and mouse to how they scroll through pages provide insights in order to fool multiple levels of payments vigilance. Behavioral biometrics can be deployed to detect robotic behavior and uncover malware as it tricks users.

Learning the lessons — across the pond

As the US embraces real-time payments, many banks are looking to integrate multiple layers of security into the design of the new systems. The ability to authenticate and verify payments depends on good identity management.

Anti-fraud mechanisms — such as multi-factor authentication, tokenization, analytics, rule changes, codes of conduct and individual bank policies — will need to ensure the overall security and stability of a real-time payments system. All of this means that payment providers need to take an enterprise-wide, layered, customer-centric approach to addressing fraud in real time.

According to Dr. Leo Lipis, Founder of Lipis Advisors, the best way to prevent fraud in systems of any speed is by making payment initiation more secure. Writing a blog for The Clearing House in the US, prior to the launch of faster payments, Lipis lays out the following groundwork.
Multi-factor authentication

The use of two separate devices and channels is the most effective way to do this. In addition to the username and password required to log on to online banking (first factor), customers must also input a one-time security code in order to send a transaction (second factor). This code can be sent via a mobile phone, generated via a token such as a key fob, issued via a hardened browser stored on a secured USB stick, or it can come from a paper-based slip with multiple one-time use codes. The central issue is that authentication takes place with a different device than for initiation.

Tokenization and analytics

Two of the most promising real-time use cases for mobile are point-of-sale applications and peer-to-peer products. Many consumers are uneasy about giving out their bank account details, but this concern can be alleviated by replacing the exchange of bank account information with a non-sensitive data element (token) that links to a customer’s bank account details, which remain concealed.

The token can either be a one-time use element that is generated at the moment of payment initiation or it can be a persistent proxy number such as a phone number or email address linked to a person’s bank account details via a secure database. In addition to the added security of not having to share one’s bank account details with another person or business, the use of proxy numbers also promotes ease of use since most people have not memorized their bank account details. Instituting a proxy number database does create an attractive honey pot for fraudsters, but securing it does not present more of a security challenge than current bank back-office infrastructure. More important, assuaging customer concerns helps drive adoption of real-time system technology and the products and services built on top of it.

The UK has created a national universal database for all banks called Paym that is operated by its national clearing house, Vocalink, and stores proxy numbers for registered bank accounts in the country. Sweden has developed a service that individual banks can join, Swish, that enables customers of participating banks to send and receive mobile payments in real time. Denmark has opted for a competitive model with multiple proxy databases that bank customers have to sign up for individually. Given the diversity of the US banking market, the Danish model seems like the best fit for this country, where the key issue will be ensuring the interoperability of multiple mobile platforms.

The use of data analytics is also essential for preventing fraud in a real-time environment. The onus for fraud detection is mostly on originating banks, but payment system operators can use analytics to run pattern and velocity checks. Operators performing fraud checks with analytics may even be able to see fraud that individual banks cannot, such as cases where a suspicious number of transactions are destined for the same receiver account, which indicates it may be a mule account.

Rule changes and bank policies

Prime examples are omitting direct debits from the real-time system and checking for a valid authorization before funds are transferred. Direct-debit rules are more complex than those for credit transfers, and direct debit refund rights are also more generous. Preventing the ability of customers to initiate a pull transaction in real time (where the payee initiates an ACH payment) is a best practice that has been adopted by every real-time system in existence today.

Payment initiation

Prevailing account-opening procedures need to be adequate to prevent fraudulent accounts. Some best practices from other countries include accessing a national fingerprint database to verify identity, as South African banks do. Denmark offers a more practical model to follow. Banks there have built-in delays that prevent users from making payments for several days after opening an account. As this country transitions to a real-time system, banks should review what information a customer needs to provide in order to open a bank account and how long they need to wait before using it.
Tony Wicks, head of AML initiatives at Swift, suggests that as immediate payments environments are launched globally, the techniques used by fraudsters move as well. And the tools and techniques they use spread to other scammers. “Criminals work as a business. They are toolmakers and tool sellers,” he adds. “You see those characteristics move as solutions change or a new scheme is launched — they are using the new friction that is created.”

As outlined above, Wicks agrees that a “layered approach” is the best way to combat the increasingly sophisticated and agile fraud techniques. “There is an end-to-end-point security to this. From a mobile device with an internet connection all the way to the delivery of a transaction,” he says. That includes introducing additional traditional flow monitoring techniques within the payments network.

After cyber criminals breached the back-office systems of Bangladesh Bank in 2016 and stole $81 million by sending fraudulent payment instructions over the network, SWIFT launched the Customer Security Programme. “At the core of the Programme is a commitment that Swift-connected banks comply with good process hygiene within their payment environments,” says Wicks.

“Fraudsters are constantly adapting to change and growing more sophisticated and organized every day. The Customer Security Programme has both raised awareness and generated actions. As a result, there is now more thought when people introduce new payments schemes or when making scheme changes to mitigate threats and anticipate those threats,” he adds. As of early 2018, 89% of Swift banks have complied with the “minimum standard baseline” of the Swift Customer Security Programme.

Good process hygiene depends on the type of payments environment a bank or financial institution is operating in. “Fraudulent approaches can vary based on the types of payment,” says Wicks. “Payment ecosystems that operate real-time confirmation may provide additional opportunity for fraud preventions and security checks. Payments that are irrevocable, where real-time settlement is applied, need more sophisticated security methods, possibly using artificial intelligence and machine learning to be able to make decisions on payments in fractions of a second,” he adds.
Section 5: How FICO helps prevent fraud in a world of real-time payments

A payments ecosystem that includes real-time payment schemes fundamentally changes how payments happen. As well as offering people and businesses quicker ways to pay, they also offer fraudsters new ways to attack. Criminals can access funds and move the proceeds of crime out of the reach of the authorities and their victims faster than ever. As this white paper has shown, this impacts financial crime both directly and indirectly, making a number of frauds more attractive to criminals, including:

- **Authorized push payment fraud**
  In this fraud, criminals use a variety of social engineering techniques and interception of communications to trick victims into making a payment to them. This fraud comes in a number of guises, including fake invoice fraud and CEO fraud, and is perpetrated against individuals and businesses. While these frauds are nothing new, real-time payments make them more attractive to criminals as the payments made are instant and irrevocable.

- **Account takeover fraud**
  Fraudsters have always been interested in taking over people's accounts, but real-time payments make it more attractive. They can move money from the accounts into their control more quickly. Types of bank accounts that offer customers the ability to send money instantly, especially if they allow for relatively large value payments, are likely to be a target for fraudsters.

- **Money mules and money laundering**
  In order to realize the benefit of criminal activity, funds must be moved into the control of the criminals and out of the reach of law enforcement. Real-time payments allow money to be “skipped” across multiple accounts in near real-time to make the funds more difficult to trace. The movement of criminal proceeds requires access to multiple bank accounts, therefore the criminals look to recruit otherwise legitimate accountholders to allow them to use their accounts as money mules.

- **Account opening fraud**
  The criminal activity facilitated by real-time payments also indirectly impacts account opening fraud. Fraudsters need the money generated by activity related to real-time payments to end up in an account that they control. To do this, they are opening accounts using stolen or synthetic identities. In cases where the money going into these accounts is from a fraud such as authorized push payment fraud, the victims may seek restitution from a bank that has allowed a fraudster to open an account using a stolen or synthesized identity.
At FICO we take a holistic, enterprise-wide approach to managing fraud that takes this complexity into account. We help financial institutions to detect fraud across all vectors of attack and can help you manage your consumer bank accounts with:

- Behavioral analysis that can spot the anomalies that indicate social engineering has been used to trick accountholders into making a payment. This can be deployed by banks for payments being both sent and received into their accounts. Analysis is in real time so that fraudulent activity can be stopped before loss happens.

- On-going analysis of bank accounts and activity on them that suggests account takeover attempts. For example, suspicious behavior related to change of account information such as contact data.

- Detection of money-mule activity and money laundering through identification of transactions that are unusual for an account, or that match the behavior seen in known money laundering transactions.

- Analysis of information in account originations to detect activity by fraudsters looking to open accounts using stolen or synthesized identities.