NICE ACTIMIZE

Real Time Payments – Learnings from a decade in the UK

White Paper

Real Time Payments – Learnings from a decade in the UK

Introduction - Instant Payments in 2019

It is clear there is an international trend towards payments that can be made in real time, with 2019 being a key year. The list of countries with real-time payments has dramatically increased in the last few years and the US is getting in on the act with Venmo first, then Zelle and now Real-Time Payments (RTP) network by The Clearing House (TCH).

The focus seems to be on utilizing the ISO 20022 messaging standard rather than legacy messaging standards, real time settlement or multiple batches, and the benefits to consumers and businesses of being able to make and receive payments in real time. Less is being said about the fraud risks.

But fraud *must* be a key concern of any Financial Service Organization (FSO) looking to participate in real-time payments. How systems, processes and customer education are built and delivered are all key in mitigating fraud and protecting customers, businesses and the overall eco-system.

The trend to real-time payments started by the UK back in 2008 provides over a decade of experience of real-time payment fraud and how to combat it. This white paper will provide a history of what happened, including the attack vectors, responses from Financial Institutions (FIs) and how the regulators are getting involved. It will also cover what FSO's can learn from this and how they can build an effective strategy to mitigate the fraud risks in 2019 and beyond.

What can we learn from a decade of real-time payments in the UK

In the mid-2000s, customers and businesses complained of the costs they incurred (lower credit or higher debit interest, for example) so UK regulators decided to make the industry move away from the slow movement of money. Checks and BACS (electronic payments similar to ACH) could take 2-6 days to be available for interest and as cleared funds to be used for meeting other payments. Further, a same day payment in the UK would cost approximately £25 via CHAPS (a guaranteed same day payment service, often used for house purchases) versus free for BACS for personal customers.

Faster Payments Scheme Evolvement

Faster Payments (FPS), as the system has become known in the UK, came into effect on May 27, 2008, just a short time ago for such a major shift. The maximum limit for a payment was £10,000. However, most banks had far lower limits, often under £1,000 for months and years after launch. There were exceptions, with at least one bank offering £10k from day one, and they felt the pain and costs of that decision.

The faster payments scheme limit has since risen to £250,000. All banks must be able to receive the current scheme limit, but can set their own outbound limits, which are often split by segment. In practice, for retail consumers it is often around £25k. The scheme limit may rise to £20m in 2019.

Faster Payments has also seen very high growth. In December 2008[1] volumes were circa 20,000,000 for the month, by November 2018 the volume was over 180,000,000. Value is growing too, with 22% growth rate year over year 2017 to 2018.

Fraud on Faster Payments

The majority of all domestic payment fraud transitioned almost immediately to faster payments rather than CHAPS or other existing schemes. Losses increased substantially and quickly, rising at 132% for 2008 versus 2007 (£52.5m for Online Banking)[1], as the banks had nearly no experience with the fraud and new attacks formed by fraudsters. Net losses also increased as cashing out fraudulent funds was faster and there were little chance of recovery compared to BACS.

Due to the payment limits set by banks, the fraud patterns looked a bit like AML structuring, where a fraud from a single defrauded account was broken down to multiple payments at the limit or close to the limit, e.g. £9,850. It is quite possible for the funds to be moved through five or more sets of accounts in a matter of a few hours before the final cash out, making them harder to trace.

Attack Vectors

As both banks and fraudsters have become more sophisticated, the number of attack vectors have also changed over the last 10 years. However, these are the key attack vectors that have been experienced in the UK.

- **Malware**

  - Malware started to become a major vector in 2009 with both Man-in-the-Middle and Man-in-the-Browser. These attacks were huge in the first few years, until banks implemented various changes to prevent this. The banks with the strongest defences were often attacked first, as they could respond quickly. Next, they could move on to the weaker banks who could take months to respond.
  - Often malware was simple and used just to collect the credentials either on the bank's site or other sites, e.g. social networking sites.
  - By 2015, malware had become more sophisticated, only targeting the payment pages, making it harder for malware detection services to spot or block.
  - Remote Access Trojans have had substantial success by fooling the banks' systems into believing that it is the customer trusted device that is accessing their account, when in fact it is being controlled by the fraudster.
  - In the last couple of years, as the sophistication of banks' toolsets has increased, banking malware in the UK has dropped away in favor of social engineering targeting the weak link - the customer.

- **Technology and Process**

  - Attacks often have targeted online processes, such as registration for online, mobile or telephony and abusing password reset processes. If these processes have weak points, they are exploited by the fraudsters to get around the two-factor authentication (2FA) that strengthens the FIs' front door.
  - With a mixture of 2FA types in the UK, from Card and Card Reader, other hardware tokens and phone or SMS, gangs have attacked 2FA in different ways.
  - For phone based 2FA, we've seen change of telephone, SIM Swap and SS7 Attacks.
  - For hardware it is different, with social engineering customers providing One Time Passcodes (OTPs) generated by hardware tokens, card readers or remote Access, either Trojans or via Vishing.

- **Data Compromise**

  - A key vector is data compromise, often via the purchase of customer credentials, (i.e: via the dark web) either directly for banking logins or buying card details and using IVR, and then using social engineering to obtain the credentials.
  - An alternative is obtaining other customer data to abuse the registration and reset processes.

  - Data compromise will be a contributory factor in a high proportion of attacks.

- **Social Engineering**

  - Phishing was the “go-to” attack method when faster payments were introduced as a way to obtain online banking credentials from unwitting customers. It has continued to the present day, although the sophistication has increased substantially.
  - More attacks have moved to Vishing, Smishing and also Twitter, i.e. pretending to be a Financial Service’s twitter account to elicit credentials and data.
  - There are various scams, but a favorite is to pretend to be the police or the bank’s fraud department and ask the customer to transfer the funds to a ‘safe account’.
  - A more recent variant involves changing account names via online banking, ahead of the call, to add weight to this lie.
  - In the last few years, there has been an escalation of attacks where payments to existing beneficiaries are made and then extending social engineering to the beneficiary to get the funds returned to an account they control.
  - There has also been a move to frauds involving businesses with all the above and specifically business email compromise/CEO frauds. Further, business accounts are being used as mules, as it’s harder to spot the transactions.

- **Hybrid Attacks**

  - Often the attacks can take a hybrid form, for example blending data compromise and social engineering.
  - In a variation, as a customer is socially engineered to download TeamViewer or other remote access software, this provides the fraudster access, under the guise of the customer ISP or Microsoft, and then empty the bank accounts.
  - Other variations are where credentials are already comprised, a loan applied for, which is credited to the account. The social engineering then involves the customer authorising a ‘refund’ to the caller.

FSO’s have also learned that fraud will move to the next weakest link. This may be another FSO or a weaker area in your own product and services, e.g. move from Digital to Telephony. Further, these weaknesses will be probed and exploited. Often gaps are hit hard and fast, so losses can spike while this is being addressed.

Current UK Losses

In 2018, a full 10 years after the service was introduced, the landscape now looks as follows:

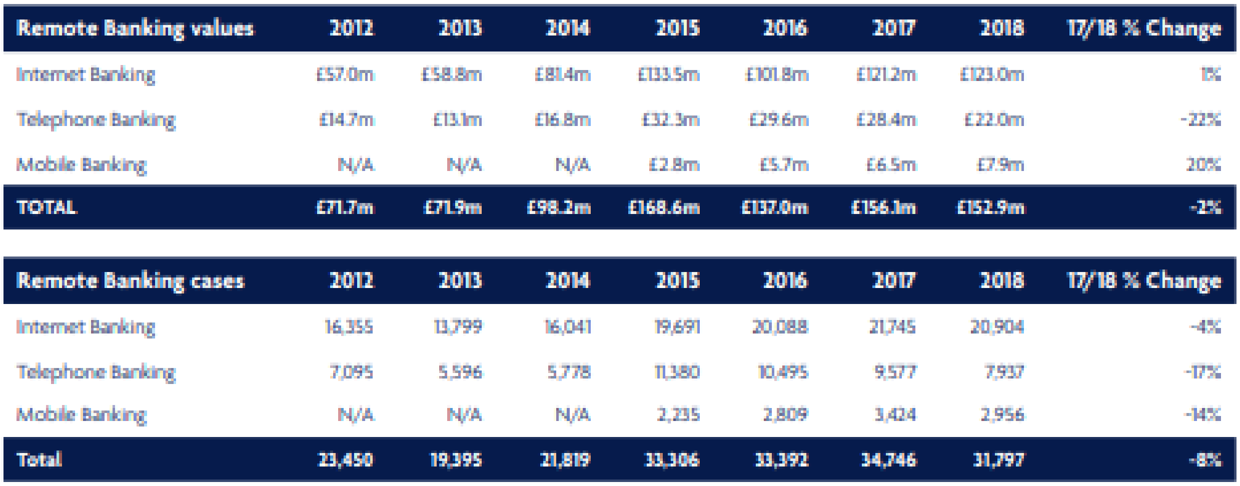
2018 Remote Banking (Digital, Mobile & Telephony) Fraud Losses[2]

• Unauthorized losses[3]	£152.9m
• Authorized (APP) losses[4,5]	£354.3m
• Prevented Unauthorized	£317.7m

This gives a total attack level of circa £825m compared with payments totalling £1.7tn in 2018[5].

These are significant sums and are after substantial investments in systems, processes, data and intelligence sharing, along with customer education programs at the industry level. The outcome of the investments in fraud prevention and detection are reflected in the prevention figures.

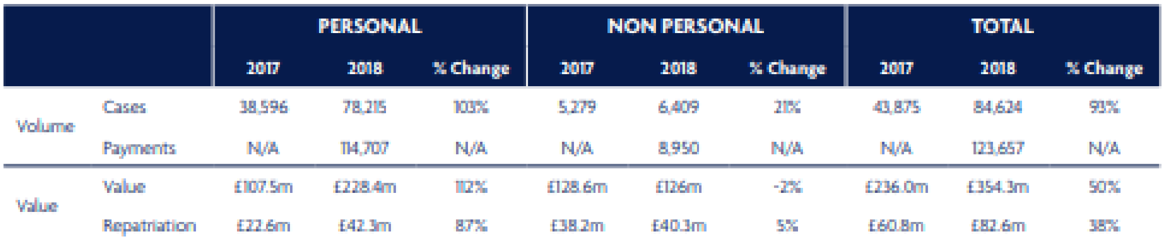
UK Unauthorised Fraud 2012-2018



Remote Banking values	2012	2013	2014	2015	2016	2017	2018	17/18 % Change
Internet Banking	£57.0m	£58.8m	£81.4m	£133.5m	£101.8m	£121.2m	£123.0m	1%
Telephone Banking	£14.7m	£13.1m	£16.8m	£32.3m	£29.6m	£28.4m	£22.0m	-22%
Mobile Banking	N/A	N/A	N/A	£2.8m	£5.7m	£6.5m	£7.9m	20%
TOTAL	**£71.7m**	**£71.9m**	**£98.2m**	**£168.6m**	**£137.0m**	**£156.1m**	**£152.9m**	**-2%**

Remote Banking cases	2012	2013	2014	2015	2016	2017	2018	17/18 % Change
Internet Banking	16,355	13,799	16,041	19,691	20,088	21,745	20,904	-4%
Telephone Banking	7,095	5,596	5,778	11,380	10,495	9,577	7,937	-17%
Mobile Banking	N/A	N/A	N/A	2,235	2,809	3,424	2,956	-14%
Total	**23,450**	**19,395**	**21,819**	**33,306**	**33,392**	**34,746**	**31,797**	**-8%**

UK Authorised Fraud (APP) 2017-2018



		PERSONAL			NON PERSONAL			TOTAL		
		2017	2018	% Change	2017	2018	% Change	2017	2018	% Change
Volume	Cases	38,596	78,215	103%	5,279	6,409	21%	43,875	84,624	93%
	Payments	N/A	114,707	N/A	N/A	8,950	N/A	N/A	123,657	N/A
Value	Value	£107.5m	£228.4m	112%	£128.6m	£126m	-2%	£236.0m	£354.3m	50%
	Repatriation	£22.6m	£42.3m	87%	£38.2m	£40.3m	5%	£60.8m	£82.6m	38%

Social Engineering, regulators and protecting customers

The authorized losses are essentially all social engineering. The unauthorized losses will also include significant volumes of social engineering at various points, possibly half.

This means that the UK regulators are now bringing pressure to bear, with a voluntary code (the Contingent Reimbursement Model, CRM) coming into effect May 28, 2019, for all the major banks. This will reduce the impact on the customer from Authorized Push Payment Frauds (APP). This will mean FSO's will need to have greater controls as the paying bank, but also as the receiving bank.

Example controls are:

- Customer behaviour analytics, incorporating fraud data and typologies - identify payments at high risk of being APP at both ends of the payment
- Risk-based warnings to customers as they are making payments
- Customer behaviour analytics, to identify customers at a higher risk of APP frauds.

Customer Experience

It is not just about the attack vectors - blocking attacks is simple, if you don't mind driving customers away. UK FIs have seen a shift in the customer experience because of the fraud attacks against real time payments.

First, moving to two-factor authentication (2FA) has often met with customer resistance and anger at the extra friction, although this has reduced in recent years. The frustration is partly due to the customer wanting to do the transaction there and then and not liking the friction, however, sometimes it is just because of the way the FI has implemented and/or communicated it.

UK banks have taken very different approaches in the past to 2FA. Some delayed deployment, trying to keep friction down or because of more pressing technical matters. However, all the major UK banks have had some form of 2FA for several years.

A number have gone down the route of EMV (Eurocard, Mastercard, VISA) Card Readers, that generate one-time passcodes (OTP) (they can also do transaction signing) if the debit card and pin are entered into the reader. While these offer good technical security, they are clunky for customers, especially when traveling, and are still susceptible to social engineering. However, as they are a standard, it is possible to have more than one; as it is the card that is important, not the reader, thereby offering customer the opportunity to have one at home and one in the office.

Other FIs have taken a different hardware approach, with a dedicated token to generate an OTP. Again, technically secure, and although small and portable, still add friction. One bank implemented these very poorly, leading to a lot of issues and subsequent back tracking. The design was such that you could not log in, even to check a balance without the token, causing a lot of complaints. Further, the communication was poor, so many customers thought they were one time only and threw them away, getting locked out for days.

Now, most banks offer the ability to log in to view balances and transactions without 2FA, either as a specific type of log in or by only requiring 2FA for high risk transactions, like new payments.

Some banks have taken a policy stance to this and others a purely risk-based approach. The first one gives consistency for customers, which can be important in helping prevent scams, at the expense of more transactions facing a 2FA challenge. The risk-based approach reduces friction but customers can't be sure when they will be challenged, meaning they will still need their 2FA method available for those times, adding friction, potentially at the wrong time.

Other banks have gone down phone call and SMS route for OTPs. This has primarily driven by reducing friction, by not requiring anything else to be carried but a mobile phone. However, these have fallen victim to SIM Swap and redirection attacks along with SS7 interception and mobile malware SMS listeners.

However, the trend for 2FA is coalescing, partly due to the Strong Customer Authentication (SCA) regulation under PSD2. Many FIs are moving to provide software OTP generators within their mobile apps and others are expanding into push messaging to the mobile app with biometrics and/or some form of OTP authentication. This only works for part of the customer base, so hardware tokens and SMS still have a place at present.

One thing banks have learned is some customers, like *some* friction in their banking, as it makes them feel safe. The new voluntary code, the Contingent Reimbursement Model (CRM) in the UK is starting to drive increased friction, by mandating warnings to consumers when they are making payments to help reduce losses to APP frauds.

Banks have also been keen to make registering for online and mobile banking simple and easy to do. This also extends to re-registration, due to forgotten or locked out passwords. If these processes are too simple and/or not protected by good levels of authentication and profiling, these will be targeted as attack vectors until they are fixed.

Lessons Learned: Tools and strategies to implement, both for the current threats and those of the near future

Based on the 11 years of experience in the UK outlined above, there are some key activities that FIs can undertake to protect their customers and themselves from fraud related to real-time payments.

First, **move from a fraud profiling solution to a fraud platform** that can act as hub for all customer transactions. **Bring as many of the transaction types and channels togethe**r, and where this may not be practical initially (perhaps the existing end solution is very good), bring key data points into the hub as part of a longer-term roadmap. This helps reduce silos, as fraudsters don't silo themselves.

Next, **enrich the hub with other data sources**, such as device profiling, and where possible, a single device profiling solution across the business covering, web, mobile and ecommerce card payments. This should also be flexible to respond to new attack vectors so new data sources and tools can be added or amended, i.e. add behavioural biometrics or change malware detection provider. Also let your system understand how where the user got to your site, i.e a known Phishing site, often called a Phishing referrer feed.

Go one stage further, and **bring in inbound payments**, looking to profile in real time for inbound fraudulent payments. This will reduce liability and **make the FI a hostile environment for fraud and financial crime.**

From here, make sure the platform can **apply advanced analytics across all the customer and transaction types**, allowing multiple models to be applied, profiling transactions and customers. Include the ability to add models as fraud attacks change.

Provide multiple types of authentication to suit your customers' needs. Also consider multi-factor authentication which should include multi-modal biometrics for the highest risk transactions.

Where possible, provide app-based authentication using biometrics, but ensure you secure the mobile first, covering key hygiene factors such as; jailbreak/root detection, certificate pinning, malware detection, device binding. Expand device binding to link the device to app, to customer, to phone number to SIM etc. This allows you to build trust and remove genuine customers from rules and provide less friction in services.

Where phone-based authentication is required, have 2-way solutions that allow customers to confirm the OTP as fraudulent, as well as SIM Swap/Redirection detection. Feed all this data directly to the hub. This should include where SMS is used for alerting customers or automated resolution activities.

Link the platform to your authentication delivery method, so it can be both policy and risk based, and able to flex to the customer demands and threats in real time. **Being able to build processes based on risk and adding the right amount of friction at the right time, will improve the customer experience and prevent complacency**. For example, this allows some customers to be offered a slicker password reset process than others, based on more data points that confirm it is the real customer.

Be able to block compromised credentials and go one step further to prevent devices being able to be used for authentication, once they are known to have been compromised.
It is also important to have a strategy for how to react to significant attacks. This should include playbooks on how to respond to different types of attacks, so that valuable time is not wasted, and include technical areas, as well as fraud strategy and fraud operations, in the discussions.

This should include a list of tools and configurable settings that can act as defensive measures on the website or mobile app, for example the ability to respond quickly to repel attacks especially malware, bots etc. This might be changing the page layout and settings to disrupt malware.

Be able to easily amend settings or switches to help manage attacks, while balancing the day-to-day customer proposition. For example, be able to alter the customer journeys that require 2FA or another Multi-Factor Authentication (MFA). Be able to easily amend payments limits, as these are held in tables and not hard coded. Have payment limits segmented to the real uses case of your customer base and not a one size fits all.

Recognize that fraud cuts across organizational boundaries, so building out industry data sharing and collective intelligence is important. This should cover:

- Intelligence on attacks, what, how, when
- Device, IP Addresses, Beneficiary Accounts
- Law Enforcement Officers (LEO) for disruption of key players based on intelligence
- Takedown services to remove phishing sites and fraudulent apps

Conclusion

The growth in use of real-time payments once they are available is clear, both in volume and value and this can still be high many years after launch. However, there is also significant growth in fraud, despite significant investments to counter.

Reviewing the learnings from the UK decade of fraud experience in real time payments is important to help reduce the fraud risk inherent in this proposition.

Success is not just about building better systems, but having a coherent and holistic strategy, covering authentication, customer experience, profiling and advanced analytics, along with data and intelligence sharing and disruption.

Remember that fraud attacks are from highly organized crime gangs who will move to the next weakest link. This may be another FI or it might be a weaker area in your own product and services, i.e. move from Digital to Telephony, so this must be part of the strategy.

As Financial Institutions launch real-time payments, they need fraud management strategies that are agile enough to stay ahead of fraudsters and their fast-changing attack methods. NICE Actimize has been protecting faster payments for over a decade. By combining our expert industry knowledge and machine learning, we can identify, detect and stop fraud faster than ever. Preparing for real-time payments requires a thoughtful strategy that includes real-time detection, specialized operations and agility. We've got the technology and best practices to help you get started.

ABOUT NICE ACTIMIZE

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

info@niceactimize.com | www.niceactimize.com/blog | @nice_actimize | /company/actimize | NICEactimize