SCL In-House Lawyers Group Event

Fraud – what are the key regulatory updates around fraud prevention in-house teams should be aware of?

Wednesday 1 November 2023

Chairs:

Ollie Clymow, Legal Counsel, Santander UK

Speakers:

Gary Brennan, Senior Counsel – Payments, Santander UK

Please note

Live captioning is being provided during this webinar by Zoom for the convenience of our viewers. The Society for Computers and Law is not able to review for accuracy any information that appears in the live captions. SCL makes no representations or warranties, and expressly disclaims and responsibility or liability with respect to, any errors or omissions in, or the accuracy, reliability, timeliness or completeness of, any information that appears in live captions during this event.

Welcome and thank you

Some housekeeping:

- This meeting is being recorded
- Any views expressed are the individual's own
- No-one taking part in this event, including the Chair, speakers or moderators are representing their employer
- No confidential or commercially sensitive information should be discussed
- If in doubt, only publicly-available information and items of general interest should be shared
- If you have any concerns at any point, please reach out to the meeting Chair immediately

What is Fraud?

In the UK "Fraud" is defined under the **Fraud Act 2006** – which replaces the older Theft Act 1968.

It can be divided into three key types –

(a) **Fraud by false representation** (making a statement to induce fraud);

(b) **Fraud by failure to disclose information** when there is a legal duty (failing to make a statement when there is a duty so as to induce fraud);

(c) **Fraud by abuse of position** (where a person occupies a position in which they are expected to safeguard and not act against the financial interests of another. But they do so).

In all cases Fraud needs to have the following ingredients:

(a) The defendants conduct must be dishonest;
(b) Their intention must be to make a gain (or cause a loss of another); and
(c) No gain or loss actually has to be made.

Typologies of Fraud

Fraud or Scams? We recognise that the terms are used interchangeably – however we would say "Fraud" **happens to you** and "Scams" **happen with you.**

Many scams will occur from "**Social Engineering**" (which is a manipulation technique used by fraudsters to get you to share personal and confidential information, or to perform an action for their benefit).

Common Social Engineering techniques include:

Phishing – Social Engineering via email;

Smishing – Social Engineering via Text SMS;

Vishing – Social Engineering via Voice Calls.

Remote Access – The scammer attempts to persuade you into giving them remote control over your personal computer. They do this by asking you to download a legitimate app or by simply getting you to click on a link.

Typologies of Fraud

Other types of scams:

Impersonation Scams - Impersonation scams happen when a fraudster contacts you pretending to be from your bank, the police, or another trusted organisation to convince you to send them money. They'll create a sense of urgency, a reason to panic to stop you from thinking straight.

Purchase Scams - These scams trick online shoppers into thinking they're dealing with a legitimate contact or company when it's actually a scammer. Fraudsters can advertise on social media, genuine selling sites, create fake websites or hack sellers' accounts. Related scam types are: (a) buying scams (these scams can happen when you find something online that you want to buy and once payment is made the seller disappears); (b) selling scams (these scams can happen when selling items online. You may send the goods as agreed and never receive payment, or you may be tricked into returning an overpayment).

Typologies of Fraud

Other types of scams:

Investment Scams – This usually involves the fraudster getting in touch and using intense, high-pressured sales techniques to convince you to invest in worthless or non-existent shares or other investments.

Invoice or Mandate Scams-These happen when a fraudster sends a bill, invoice, or other payment request to someone asking for payment following the supply of goods or services, even a house purchase. Often, they're received by email and will always look to be from a genuine business or contact.

The contact may even impersonate a solicitor, family member, friend, colleague, or a senior member of staff, asking for an urgent payment to be made.

Note - not an exhaustive list!

Why is Fraud an Issue?

Online fraud has become such a significant issue for individuals and businesses in the UK.

Estimates suggest it is now the most commonly experienced crime in the UK (making up 40% of all reported crimes in December 2022) and costs the UK up to a £7 billion pounds each year.

Seen by many as part of a trend as financial and technology institutions during the pandemic accelerated the shift towards digital operations. People in their personal life became much more comfortable with dealing with technology and not seeing the people they were working with.

This “new normal” has enabled fraudsters to target customers and businesses with increasing sophistication and success.

What are Financial Services and other industries seeking to do about this?

Regulatory Change - Authorised Push Payment Fraud

Customer fraud where a customer is tricked into making a payment to somebody who poses as a genuine payee is known as "**Authorised Push Payment**" or "**APP**" Fraud.

A number of Financial Institutions signed a voluntary code in May 2019 covering how and when they will refund APP Fraud suffered by Retail customers. This is known as the CRM Code.

The UK Government is seeking to put this on a regulatory footing via the **Financial Services and Markets Act 2023** which places a duty on the UK regulator for the Payment Systems (the Payment Systems Regulator or "PSR") to consult on a draft regulatory text within six months of FMSA 2023.

The PSR has published a Policy Statement in June 2023 and followed this up with a series of Specific and General Directions on Banks (and Pay.UK). The proposal is to include the obligation to refund within the Faster Payments Scheme Rules (and in time for higher value payments via CHAPS).

Regulatory Change - Authorised Push Payment Fraud

Some of the key changes proposed within the PSR's proposal on APP:

- The Sending and Receiving Financial Institution will need to split the refunded customer loses 50/50.

- There will be an ADR Mechanism to apportion loses if there is not agreement on the 50/50 split between institutions.

- The Sending Financial Institution will be given five business days in which to process and reimburse the defrauded customer's claim. It will be possible to "Stop the Clock" in certain limited instances.

- There will be a claim excess for payments as well as a maximum value of refund on APP scams. Both are subject to Consultation within the FPS Scheme rules.

- Importantly there will be no minimum threshold for an APP claim.

-There will be a customer standard of caution (below which customers will not be paid out unless they are vulnerable) and claim excess will not be applied to vulnerable customers.

Regulatory Change - Confirmation of Payee

Confirmation of Payee (or "**CoP**") is a key part of the Pay.UK scheme which aims to protect customers from fraud. It allows customers to name check for payments they make between UK based Sterling accounts and aims to reduce certain types of fraud as well as misdirected payments.

CoP lets people check that the name on the account they are paying matches the details they share when they set up a new payment. Customers receive either: (a) Yes – correct match; (b) No – partial match; (c) No – not a partial match; or (d) CoP check unavailable.

In August 2019 the Payment Systems Regulator ("**PSR**") issued Specific Direction 10 ("**SD10**") which mandated designed financial institutions to implement CoP across all of their accounts. This applied to retail, small business and larger corporate customers. This was further expanded in 2022 to accounts which have additional customer routing data (known as "**Secondary Reference Data**").

CoP has proved successful and the next stage is expanding the number of Financial Institutions in scope. Specific Direction 17 from the PSR mandated an additional 32 PSPs (Group One) to join CoP by October 2023, with the remaining PSPs in the UK (Group Two) by October 2024.

Regulatory Change - Quincecare Duty/Phillips Case

Aside from regulations – there are a number of decisions made in the courts which inform Financial Institutions conduct when a customer suspects or has suffered Fraud.

These include the decision in the case of *Barclays Bank v Quincecare [1992] 4 All ER 363.* This decision placed an obligation on the sending financial institution not to make a payment where it is "on enquiry" that the payment instruction was a fraud on the customer.

The Financial Ombudsman Service (or "**FOS**") made a number of decisions that appeared to extend this Quincecare duty to those where the customer had made an authorised push payment (or "**APP**").

The Courts have further clarified in the *Philipp v Barclays Bank [2023]* that the Quincecare duty is not relevant where the customer has authorised the payment and so would only apply to unauthorised payments and not APP Fraud.

Regulatory Change - Online Safety Act

The Online Safety Act has now passed and will compel social media platforms and search engines to “stamp out” fraudsters and scammers. It will imply a duty of care on larger platforms to protect users from fraud and other negotiate content.

The proposed new legal duties will impact:

- providers of internet services which allow users to access content generated, created or uploaded by other users (‘**user to user**’ services); and

- providers of search engines which enable users to search multiple websites and databases.

The most onerous obligations will fall on the largest and most popular platforms (known as “**Category 1**”), including the requirement to prevent paid-for fraudulent adverts appearing on their sites.

Search engines and platforms will have a duty of care to protect users of their services from fraud committed by users and require them to have proportionate systems and processes in place to prevent/minimise the publication of fraudulent advertising and remove it when aware of it.
Application is not limited to UK-based providers – those outside the UK may be in scope where they target UK users or have significant UK users.

We expect OFCOM to publish a Code of Practice describing recommended steps to ensure compliance with the new duties.

SCL 50th 1973/2023 Anniversary

Tech Law for Everyone

What can technology providers be expected to do?

Fraud and Tech – A missed opportunity?

We have seen a number of voluntary initiatives where Tech Firms have sought to support fight against fraud:

UK Finance – Take Five Initiative *– Announces as part of the "Take Five Stop Fraud" initiative that major technology companies including Google, Facebook, Instagram, Twitter, Amazon, Microsoft and TikTok have pledged to support the Take Five Stop Fraud initiative.*

The UK Government announced the "**National Fraud Strategy**" in May 2023 – it had been anticipated that this would go as far as requiring Tech Providers to reimburse customers if they suffer fraud loses as a result of actions/inaction by those providers (in a similar way to the APP Fraud scheme in place for Financial Institutions).

However, it was reported that this was removed at the last minute.

Whilst "SIM Farms" and banning of cold calling on financial products has been implemented – there have been arguments that this is "watered down" and will not tackle the route cause of fraud.