BCLP. Client Intelligent

Insights

PAYMENT FRAUD: PSP'S OBLIGATIONS

Jun 09, 2020

In accordance with recent UK Finance statistics, in 2019 banks and card companies prevented £1.8 billion in unauthorised payment fraud and between 2018 and 2019 APP fraud (see below) losses increased by almost 30% to £456 million. In these challenging times due to Covid-19, while firms and consumers are adapting to the "new norm", criminals are, unfortunately, also adapting. There is preliminary evidence that new forms of frauds are appearing and payment fraud is on the rise, particularly with online payments. Due to Covid-19 there has been a decrease in cash payments adding extra pressure on online payments. Online payment fraud is often identity theft of cardholder's details, however the mechanism for fraudsters to obtain these details is becoming more sophisticated and harder to detect, making the ability of PSPs to identify fraudulent payments more onerous.

Under the UK regulatory regime, there are multiple fraud-related requirements and obligations on payment service providers ("PSPs"). The pandemic is putting these requirements/obligations into sharper focus. It is, now more than ever, crucial for PSPs to have a clear understanding of these for the purposes of both regulatory compliance and reputation management.

We provide an overview of these fraud-related requirements/obligations which can be summarised into three headings: statutory requirements; regulator rules and guidance; voluntary standards.

STATUTORY REQUIREMENTS

The Payment Services Regulations 2017, as the main legislation regulating payment services, has various provisions that have a bearing on the prevention/detection of fraud. Some of these obligations are express and specific, whereas others are implied and included as part of the appropriate systems and controls a PSP must maintain.

The express obligations include, for example, those under the strong customer authentication ("SCA") regime the underlying purpose of which is to fight fraud. Further, a PSP, once it knows that an executed payment was unauthorised, must refund the customer by the next business day (subject to certain limited exceptions).

With respect to the obligations that are embedded in the relevant internal control requirements, these include, for example, the general requirement that PSPs subject to the safeguarding requirements must have organisational arrangements sufficient to minimise fraud and other financial crimes. PSPs that engages in the account information service and/or payment initiation service must also have a professional indemnity insurance or guarantee regarding its potential liability for fraud.

In addition, PSPs must also report, either once or twice annually (depending on the firm type), fraud statistics to the Financial Conduct Authority ("FCA").

Note that in certain circumstances where there is a fraud (e.g. one committed by the customer herself), the PSP may be able to exclude itself, partially or wholly, from the relevant liability.

FCA RULES

For non-bank PSPs (e.g. payment institutions and electronic money institutions), the FCA Handbook essentially does not apply; they are subject to a separate supervisory regime where the relevant FCA rules and guidance are contained in the FCA Approach Document for Payment Services and Electronic Money.

However, since August 2019, the overarching Principles of Business in the FCA Handbook have applied to non-bank PSPs. There is considerable uncertainty as regards how these Principles apply in practice to non-bank PSPs. Some of the Principles that may have a bearing on the prevention of fraud include e.g.: Principle 1 which requires a firm to conduct its business with integrity; Principle 3 requiring a firm to organise and control its affairs responsibly and effectively, with adequate risk management systems; Principle 5 whereunder a firm must observe proper standards of market conduct.

The FCA now also allows victims of authorised push payment fraud ("APP fraud") to raise certain complaints against either their own PSP or the payee's PSP. An APP fraud is where the victim, being the payer, actually authorised and made the payment herself (i.e. 'push' payment) but she was tricked into doing so. This new rule has been in place since April 2019.

VOLUNTARY STANDARDS

There are multiple sector-specific requirements, rules, best practices or market standards that are either recommended by trade bodies or commercial in nature (e.g. the relevant rules set by card associations). PSPs are bound by these either on a voluntary basis or as a matter of contract law. However, some of these may be best described as a hybrid of industry practice and regulatory obligation, given the express or implied backing from regulators. Two examples are the Confirmation of Payee service and the Contingent Reimbursement Model Code both of which are part of the Payment System Regulator's strategy to fight APP fraud. But the actual content and requirements under both are formulated and agreed by the industry.

Confirmation of Payee

The Confirmation of Payee service is being rolled out by Pay.UK (the operator of UK's payment systems). It essentially requires the payer's PSP, together with the payee's PSP, to match the name of the person the payer wishes to pay with the name registered to the account of the intended payee, with respect to payments made via Faster Payments or CHAPS (currently, account names are not checked as part of the payment processing).

As directed by the PSR, the scheme currently is mandatory for the UK's six largest banking groups only ("PSR6") which are required to implement it by June this year. However, the PSR encourages all PSPs to join the scheme voluntarily and has suggested that it may make it mandatory for all PSPs if voluntary up-taking is not satisfactory.

Note that there may be difficulties for PSPs (other than the PSR6) to voluntarily join the scheme as e.g. many documents (particularly technical specifications) are not publicly available.

Contingent Reimbursement Model Code

The Code sets out a mechanism for how and when victims of APP fraud should be compensated by their PSPs. Notwithstanding it being a voluntary code of conduct, the Code is essentially required to be taken into account by the Financial Ombudsman Service when handling complaints against PSPs arising from APP fraud. The FCA also expects PSPs to implement the Code consistently and may potentially take enforcement action as a result of arbitrary interpretation of the Code (e.g. on the basis of some of the general Principles above).

On a recent conference call (30 March 2020) the PSR expressed dissatisfaction with the current progress under the Code and noted "some cause for concern that outcomes are not where we all want them to be".

Note that there are still outstanding issues with the Code itself, the most important of which is how the no-blame compensation (i.e. where neither the victim nor the PSPs are to be blamed) should be funded.

CONCLUSION

There are different types of PSPs, which means the obligations applicable to each PSP may vary. For banks which are subject to complex and wide-ranging regulation, other general or specific requirements (that are, in and of themselves, not related to payment services) may nonetheless affect the banks' procedures and processes relating to payment fraud. As noted above, while some of the requirements may be expressed as voluntary, given the relevant regulatory backing and the increasing regulatory focus on firm culture, firms should consider carefully how "voluntary" these should be treated, particularly where there seems to be no strong justification for not participating in the relevant schemes or codes.

MEET THE TEAM

Samantha Paul

London

samantha.paul@bclplaw.com
+44 (0) 20 3400 3194
