Feature

KEY POINTS

- Electronic money (e-money) is the fintech version of cash at bank – it is essentially a digital equivalent to cash. Electronic money institutions (EMIs) (such as Revolut, Starling and Modulr) are a type of financial institution which are authorised to issue and manage e-money on behalf of their users.
- Deposit aggregators (Deposit Aggregators) (such as Flagstone, Raisin, Insignis and Moneybox) are fintech platforms which suggest to customers the banks and building societies a customer could place cash with via their platform, and then provide a platform for the customer to manage such cash and accounts.
- Security documents currently being entered into in the majority of financing transactions do not make a distinction between traditional bank accounts on the one hand, and e-money accounts and accounts with Deposit Aggregators on the other.
- Consequently, security principles relevant only to traditional bank accounts are continually applied when taking security over e-money and accounts with Deposit Aggregators. This may not, however, create valid or effective security and this does not provide the same level of protection to lenders or security trustees (chargees).
- A new approach is required to take effective security over such assets, and this article sets out the practical and legal considerations when taking security over e-money and deposits with Deposit Aggregators.

Authors Kerry Langton, Fiona Henderson, Julian Turner and James Dickie

Security over e-money and deposits with deposit aggregators: a new approach is required

INTRODUCTION

Over the last decade, fintechs (including EMIs (see definition in the key points above)) have transformed the payments landscape and have driven and facilitated the rapid shift by individuals and businesses away from cash to e-money. This article sets out the practical and legal considerations under English law when taking security over e-money and deposits with Deposit Aggregators (see definition in the key points above).

E-MONEY AND E-MONEY ACCOUNTS

What is an e-money account?

An e-money account is an electronic store of monetary value represented by a claim against the relevant account provider (known as an EMI) which a third party will accept as being equivalent to real money. The relevant regulations for e-money accounts and EMIs are The Electronic Money Regulations 2011 (EMRs).

When depositing cash into an e-money account, the deposit is used to buy an e-money balance with the EMI, with that balance being given a monetary value as represented by a claim against the EMI for the return of the cash deposit. An EMI is under a statutory obligation to allow its customers to redeem (that is, withdraw) the balance in their e-money account. Thereafter, the customer can use the money for payment transactions.

Safeguarding accounts

From a regulatory perspective (under regs 21 and 22 of the EMRs), when an EMI receives a cash deposit in exchange for issuing e-money, the EMI is required to back-up the electronic store of monetary value represented by an e-money account and comply with the safeguarding regime. An EMI can do this by:

- segregating the money into a special safeguarding account or accounts (being any traditional deposit account held with a third-party credit institution with the funds kept separately from the EMI's own money);
- investing the money in secure, liquid, low-risk assets which have been approved by the Financial Conduct Authority (FCA) and are held in a separate account by a custodian; or
- less commonly, holding an insurance policy or bank guarantee to safeguard the funds.

The Court of Appeal has held that whilst the safeguarded money, other assets and/or insurance policy(ies) or guarantee(s) are not held on trust for the customers (and therefore remain the assets of the EMI), on any insolvency of the EMI the customers are granted rights over that asset pool in priority to other creditors of the EMI (*Ipagoo LLP (in administration)* [2022] EWCA Civ 302). Further, if there is a shortfall in the asset pool that shortfall is to be made up from other assets of the EMI. The Payment and Electronic Money Institution Insolvency Regulations 2021 include a special administration regime for EMIs, and expressly provide that the administrator is to transfer an amount from the EMI's own accounts to make up any shortfall in the asset pool. It is not yet definitive if this right to make up any shortfall from the other assets of the EMI takes priority over the claims of the EMI's other creditors, in particular secured creditors. However, recent case law suggests that the EMI's customers' rights may have priority.

Security over e-money: key considerations

Security over e-money accounts and balances cannot be taken in the same way as security is taken over traditional bank accounts and cash at bank. In particular:

- security cannot be taken over e-money accounts or e-money; security can only be taken over the claim that the customer has against the EMI for the redemption value of their e-money and the proceeds of that claim;
- the safeguarding regime does not allow any security to be taken over the EMI's safeguarding accounts or the cash in these accounts as this would undermine their purpose (being a back-up of the e-money value). Money in the safeguarding accounts is not the customer's and it is not held on trust. Therefore, the customer has no interest in any safeguarding account over which security can be granted. Rather, the only interest the customer has is the claim against the EMI for the return of the cash deposit and the proceeds represented by that claim;
- it is not possible to block e-money accounts as the EMI has a statutory duty to allow redemption by the customer at any point and, in order to be an e-money account, the balance must be capable of being used for payment transactions (regs 39 and 40 of the EMRs). If an account is blocked, it cannot be used for payment transactions and is no longer e-money; and
- despite this, security documents currently being entered into are still requiring notices to be served on, and acknowledgements provided by, EMIs in the same way as notices and acknowledgements would be served on a bank in respect of traditional bank accounts. An EMI cannot accept any fetter on its statutory duty (which must allow redemption by the customer at any point) and therefore must reject (or at least not acknowledge) a security notice which in any way purports to block the e-money account. This is creating issues on transactions at financial close and resulting in failure to satisfy conditions precedent or subsequent.

Security over e-money: modernising the traditional approach

In terms of taking security over e-money:

- any e-money accounts held by an obligor should be identified and subject to due diligence;
- the terms and conditions of the e-money accounts should be reviewed. For example:
  - what is their governing law (taking into account the proposed governing law of the security document);
  - are there any restrictions on the grant of security by the e-money account holder over their e-money accounts (technically, their rights against the EMI to redeem the balance held in their e-money accounts and the proceeds of such claims against the EMI);
  - the details of how instructions may be given by an account holder and whether it can delegate its authority to others; and
  - any restrictions on the e-money account holder granting a (security) power of attorney in favour of the chargee, or in the EMI recognising the authority of such power of attorney;
- any security taken by a chargee will not be over the e-money accounts in the traditional sense of account security, rather it will be over the e-money account holder's rights against the EMI to redeem the balance held in their e-money accounts and the proceeds of such claims against the EMI;
- it is possible to take a purported fixed charge over the claims and include a suite of negative undertakings vis-à-vis the claims and the chargor's operation of the e-money accounts in the security document. However, there is currently no case law on the control required to create a fixed charge over the e-money account holder's rights against the EMI to redeem the balance held in their e-money accounts and the proceeds of such claims against the EMI. Accordingly, it could be argued that there is insufficient control exercised by the chargee, which may lead to a challenge or re-characterisation of the charge as a floating charge;
- it is possible to take a floating charge over the claims;
- notices of the fixed security should be served on the EMI, but these need to reflect that the security is over e-money and e-money accounts and not traditional cash and bank accounts. Once correctly tailored, EMIs rarely have issue with signing the acknowledgement, thereby creating a contractual nexus between the chargee and the EMI; and
- the inclusion of additional events of default and undertakings in the facility agreement may also require consideration. If an EMI is in financial difficulty, this may lead to action being taken under the EMI's own financial arrangements which could have implications for its bank accounts (including the safeguarding accounts). For example, it is not the case that redemption requests have to be paid out to customers directly from the EMI's safeguarding accounts. An EMI can, when complying with a redemption request from a customer, pay the proceeds from any of its accounts and then reduce the balance in the safeguarding accounts accordingly. Therefore, any disruption to its accounts as a result of financial difficulties (or otherwise) could affect the EMI's customers and access to their e-money (notwithstanding the safeguarding regime).

Enforcement of security over e-money

On the security becoming enforceable (assuming fixed and floating charges have been granted), a chargee could:

- appoint an administrator under its floating charge, provided it is the holder of a qualifying floating charge in respect of the chargor's property. The administrator would act as the chargor's agent, and could therefore redeem the e-money; or
- appoint a receiver over the assets subject to its security (which may require the charge to be crystallised if it is re-characterised as a floating charge). Likewise, the receiver would act as the chargor's agent and could therefore redeem the e-money.

DEPOSITS WITH DEPOSIT AGGREGATORS AND ACCOUNTS HELD WITH DEPOSIT AGGREGATORS

Are these accounts the same as e-money accounts?

No, these accounts are not the same as e-money accounts. Deposit Aggregators

Feature

Biog box
Kerry Langton is a partner and Fiona Henderson is a senior associate in the Fintech Team at CMS Cameron McKenna Nabarro Olswang LLP.
Email: kerry.langton@cms-cmno.com and fiona.henderson@cms-cmno.com

are fintechs which provide a platform for customers to place funds into different accounts with different banks and building societies and then to manage such cash and accounts. Deposit Aggregators are not banks and they are currently unregulated (albeit the Prudential Regulatory Authority is looking at them closely). A Deposit Aggregator will receive funds from a customer into an initial holding account (sometimes called a hub account, a Hub Account) and will then move the funds into specific deposit accounts with banks and building societies.

The platforms typically give a customer a range of account options as to which banks and building societies the deposit could be placed. The customer selects their accounts depending on their preference for instant access or notice accounts and depending on whether they wish to maximise interest or to ensure full protection from the Financial Services Compensation Scheme (FSCS) for all deposits (by ensuring that deposits with a single bank or building society, both as part of the Deposit Aggregator's services and outside of it, do not exceed the £85,000 FSCS protection threshold).

Hub Accounts and Deposit Accounts

Under the typical Deposit Aggregator arrangement, the Hub Account is not an e-money account but is rather a placement of cash which is held by the Deposit Aggregator on bare trust in an instant access payment account (for example, a current account) at a specific bank or building society and then deposited into one or more accounts in the Deposit Aggregator's name with the banks and building societies chosen by the customer on the platform (each a Deposit Account), with these again being held on bare trust for the benefit of the customer. Despite the Deposit Accounts being in the Deposit Aggregator's name (with the contractual relationships being solely between the bank or building society and the Deposit Aggregator), for FSCS purposes, deposits are treated as though they are held by the customer directly, although there is no direct relationship between the customer and the bank or building society. Usually, a customer will transact only through the Deposit Aggregator, but some banks and building societies offer both direct and indirect access.

Direct Accounts

There is a slightly less common structure operated by Deposit Aggregators where they arrange for one or more accounts to be opened in the name of the customer directly (each a Direct Account). Under this structure, Direct Accounts generally operate as though the customer had approached the bank or building society directly. That is to say, Direct Accounts will be in the customer's name, the customer will be both the legal and beneficial title holder to each Direct Account and the balance in it, and the contractual relationship will be between the customer and the bank or building society. These Direct Accounts will only hold the customer's funds and will not be operated as pooled accounts. In these arrangements, there is usually no bare trust over any of the Direct Accounts; instead, the Deposit Aggregator simply acts as agent in arranging and operating the Direct Accounts on behalf of the customer. These structures are generally only used where either:

- the receiving bank or building society objects to accounts being held on trust; and/or
- the customer is required to retain legal title to the money being deposited (for example, the monies represent client monies for the purposes of the FCA Client Asset Rules).

Security over accounts held with Deposit Aggregators: key considerations

Where the accounts are Direct Accounts, security can be taken in the same way as security over traditional bank accounts.

Security over Hub Accounts and Deposit Accounts and the balances on these accounts cannot be taken in the same way as security is taken over traditional bank accounts and cash at bank. In particular:

- security cannot be taken over Hub Accounts or Deposit Accounts and their balances; security can only be taken over the beneficial interest the customer has in the Hub Account and Deposit Account and the proceeds in these accounts;
- in theory, a chargee could request that a Hub Account is blocked since there is a direct relationship between the customer and Deposit Aggregator by serving notice on the Deposit Aggregator in relation to the Hub Account under the relevant security document requesting that either the account is blocked or withdrawals are not to be made without the consent of the chargee following a specific default or enforcement trigger. However, in practice, a Deposit Aggregator is unlikely to be able to comply with such a request as:
  - in relation to blocking the account, Deposit Aggregators often do not operate Hub Accounts as segregated accounts, rather the Hub Account will be a pooled account holding the monies of multiple customers; and
  - in relation to blocking withdrawals from the Hub Account (which would be possible even with a pooled account), the Deposit Aggregator is unlikely to be able to readily accept that this does not interfere with their duties as a trustee. In order for a Deposit Aggregator to accept this (and acknowledge any notice) the Deposit Aggregator would need to be satisfied that the request to block the withdrawal was being made by the chargee as agent of the beneficiary. However, the residual risk on the Deposit Aggregator from breaching trustee duties and the level of diligence required by the Deposit Aggregator to be comfortable with the risk of acting on a third party's instructions and potentially handling conflicting instructions is high. Therefore, in practice, blocking withdrawals would be difficult; and
- it is not possible to block Deposit Accounts, as the underlying accounts are in the name of the Deposit Aggregators. Even if notice were served on the bank or building society under the relevant security document requesting that no withdrawals be made without the consent of the chargee following a specific default or enforcement trigger, the underlying accounts are in the name of the Deposit Aggregator (not the customer) so the bank or building society would not be able

Biog box
Julian Turner is a consultant in the Restructuring and Insolvency Team and James Dickie is a senior associate in the Financial Services Regulatory Team at CMS Cameron McKenna Nabarro Olswang LLP.
Email: james.dickie@cms-cmno.com and julian.turner@cms-cmno.com

to comply with such a request as they can only deal with the monies in the Deposit Accounts following an instruction from the Deposit Aggregator (and the Deposit Aggregator will only give instructions to the banks or building societies with which the Deposit Aggregator maintains the accounts following an instruction from the Deposit Aggregator's customer; the Deposit Aggregator cannot exercise any discretion as they act as trustee in respect of the monies in the Deposit Accounts).

Security over Hub Accounts and Deposit Accounts: modernising the traditional approach

In terms of taking security over Hub Accounts and Deposit Accounts:

- any accounts held by an obligor with a Deposit Aggregator, and the account structure operated by the Deposit Aggregator should be identified and subject to due diligence;
- the terms and conditions of the accounts should be reviewed. For example:
  - what is their governing law (taking into account the proposed governing law of the security document);
  - are there any restrictions on the grant of security by the account holder over their accounts (technically, their beneficial interest in the accounts and the proceeds in these accounts);
  - the details of how instructions may be given by an account holder and whether it can delegate its authority to others; and
  - any restrictions on the account holder granting a security power of attorney in favour of the chargee, or in the Deposit Aggregator recognising the authority of such power of attorney;
- any security taken by a chargee will not be over the Hub Account or the Deposit Accounts in the traditional sense of account security, rather it will be over the beneficial interest the customer has in the accounts and the proceeds in those accounts;
- it is possible to take a purported fixed charge over the beneficial interest and include a suite of negative undertakings vis-à-vis the beneficial interest and the chargor's operation of the Hub Accounts or Deposit Accounts in the security document. However, there is currently no case law on the control required to create a fixed charge over the customer's beneficial interest in Hub Accounts or Deposit Accounts and the proceeds in these accounts. Accordingly, it could be argued that there is insufficient control exercised by the chargee, which may lead to a challenge or re-characterisation of the charge as a floating charge;
- for Hub Accounts, notices of the fixed security should be served on the Deposit Aggregator which reflect the relationship between the customer and Deposit Aggregator. The contractual nexus between the chargee and the Deposit Aggregator achieved by an acknowledgement is important. For Direct Accounts, notices should be served in the same way as traditional bank accounts. For Deposit Accounts, notices should not be served on the banks or building societies with which the Deposit Aggregator maintains the accounts as the accounts are in the name of the Deposit Aggregator and not the customer (although the proceeds in the accounts are held on bare trust for the customer); and
- it is possible to take a floating charge over the claim.

Enforcement of security over Deposits with Deposit Aggregators and Accounts held with Deposit Aggregators

On the security becoming enforceable (assuming fixed and floating charges have been granted), a chargee could:

- appoint an administrator under its floating charge, provided it is the holder of a qualifying floating charge in respect of the chargor's property. The administrator would act as the chargor's agent, and could therefore make a claim against the Deposit Aggregator to withdraw their funds; or
- appoint a receiver over the assets subject to its security (which may require the charge to be crystallised if it is re-characterised as a floating charge). Likewise, the receiver would act as the chargor's agent and could therefore make a claim against the Deposit Aggregator to withdraw their funds.

SUMMARY

- It is possible to take valid, effective, and enforceable security over e-money and deposits held with Deposit Aggregators, but the security cannot apply the same principles as if the accounts in which the chargor's funds are "held" were traditional bank accounts.
- Security documents in financing transactions need to be refreshed and modernised – they need to be tailored to the assets and rights that are capable of being secured, and the structure of the accounts.
- Lawyers acting for chargees should be advising their clients on the differences between security over e-money and deposits held with Deposit Aggregators, and security over traditional bank accounts.
- Lawyers acting for chargors should be advising their clients as to whether the security required or requested by a chargee can be granted, and if their account structure is likely to satisfy the chargee's requirements.
- E-money accounts, Hub Accounts or Deposit Accounts and their balances are likely to be unsuitable as charged property and/or where the chargee requires blocked accounts and will be relying on its fixed security as part of the transaction structure (for example, a blocked rent account in a traditional real estate finance transaction). ■

Further Reading:

- Take it on trust: "relevant funds" under The Payment and Electronic Money Institution Insolvency Regulations 2021 (2021) 8 JIBFL 566.
- Unfinished business? The payment services safeguarding rules after *Supercapital* (2020) 11 JIBFL 734.
- LexisPSL: Financial Services: Practice Note: E-money: passporting, outsourcing and use of distributors and agents.