THINCATS

Business Loans Network Limited ("ThinCats", the "Firm")

Business Continuity Policy ("BCP") v.2

July 2017

INTRODUCTION

ThinCats is an online peer to peer lending platform enabling investors to lend directly to companies (borrowers). Its main responsibility is to provide and maintain a virtual platform. The platform performs facilitative and administrative functions.

In the event that Business Loan Network (BLN) business operations are interrupted, or access cannot be gained to its Ashby office, the responsibility for the facilitation of the platform must continue with the least possible disruption and with no adverse impact on the ability to perform these functions.

The purpose of this document is to record the actions to be taken by ThinCats in respect of potential problems that the business may encounter in connection with the occurrence of an incident.

1. PURPOSE

This document describes how ThinCats would respond to a significant disruption to its business operations. It outlines plans that would mitigate the impact of such a disruption to BLN's clients and staff. It also sets out business continuity invocation, staff roles and responsibilities and the alternative arrangements that ThinCats has put in place for its operations.

The Management Team is responsible for the regular review of this document.

2. PLAN INVOCATION

In the event of an incident leading to an evacuation of the Ashby office during office hours, all staff will be expected to either return home where they can remotely access work email and group drives or travel to the London office. The Management Team will decide on who works from home and who has to travel to the London office depending on the incident. BLN's fire evacuation procedures are outlined in Section 9.

In the event of an incident that does not lead to an evacuation during office hours, The Management Team will decide upon the appropriate course of action.

2.1 OUTSOURCED PROVIDERS

BLN's current key outsourced providers are:

1. Baker Tilly Creditor Services LLP currently undertakes two key roles for BLN:

- The collections and payment service provider,
- Acts as primary 'Run-Off / Back-Up servicer in the event of BLN ceasing operation

2. Ocean Intelligent Communications provide a number of Corporate IT services. This includes desktop infrastructure, server infrastructure, network infrastructure, security services, file and standard software packages.

3. Clarion Communications Limited provide hosted telephony services.

Two independent software systems are employed to support BLN's business. One (TC Client Platform) to manage the platform including lenders registration and auction management up until the point when a loan is drawn down and thereafter repayment processing, interest calculation and lender cash

allocations. The other 'Street Serve' system is operated by an independent company that is authorized and regulated by the Financial Conduct Authority, Street UK ("Street"). Street provides borrower payment collection functions, administering all the direct debit collections from borrowers, accepting funds deposited into lenders accounts and mirrors the income allocation of the primary system. Additionally, it has an ability to independently calculate the interest earned by each lender if required. In the event BLN or the main TC Client platform ceases to operate, Street has all the data needed to continue to collect direct debits from borrowers and allocate funds to lenders.

Outside of office hours it is the responsibility of The Management Team staff member, who identifies the threat or event, to contact other staff who are subject to this policy either via email or telephone.

Issues to be considered and/or communicated include:

- What has happened – is this a live event or not
- Is the situation now stable or are future events likely to occur
- What time did the incident occur
- Where has the incident occurred
- Is this confirmed or unconfirmed and what is the source of the information
- Are there further immediate health and safety risks
- How is access to the office affected
- What is the extent of any physical damage to the office
- What is the impact of the incident to IT systems (if any)
- How will clients be impacted
- What is the potential impact to the business
- The likely timescale to recovery of normal operations and resolution of the incident

The Management Team will then decide:

- Their assessment of the disaster situation
- Who will be the key contact for all the staff
- Who will be the key contact between the London and Ashby offices
- Which areas identified by the initial report are priorities to address (people, business priorities, assets)
- The technology recovery strategy (if appropriate)
- Communication plans with other parties (staff, service providers, regulators, investors, etc.)
- Whether it is necessary to tell staff to work from home or London office for key functions i.e. operations, client on-boarding
- How best to assign specific responsibilities to address any critical issues identified

As incidents can take many different forms, there are no prescribed courses of action. The Management team are responsible for agreeing an action plan.

The Management Team have specific responsibilities for various business recovery areas as follows:
- Human Resources
- Facilities
- Operations

- Communication with London Office (CEO)

3. ROLE PROFILES

3.1 MANAGEMENT TEAM

The Management Team in Ashby is comprised of Damon Walford, Jill Sandford, Kevin Caley and Peter Brown. They are responsible for making strategic decisions throughout the recovery of business operations that best serve the joint interests of staff, clients and other stakeholders.

The Management Team's responsibility is to manage and co-ordinate the response to, and recovery from, a crisis. This role will continue through the restoration until the situation returns to normal. This function also involves gathering relevant information and options to enable accurate decision making, and to delegate and follow up tasks to ensure things actually happen.

Additional responsibilities include:

- Notifying and consulting with Senior Management in London
- Formulating response/recovery strategy
- Ensuring delegated tasks are completed
- Directing information gathering
- Ensuring obligations in respect of confidentiality are maintained at all times
- Acting as media spokesperson
- Agreeing alternate premises for the resumption of business (i.e. beyond the use of working from home or London office where necessary)

3.2   HUMAN RESOURCES

The Chief Operating Officer (COO) together with Emergency Contact (Maggie Komorowska) are responsible for handling issues regarding staff well-being and other HR related matters.

The responsibilities include helping to get people back to work as quickly as possible, while ensuring their personal well-being. The COO is responsible for ensuring that working conditions are reasonable even under stressful conditions (working hours, employee's general health, safety and welfare excluding the physical environment and continued salary payments). The COO is responsible for making staff assignments, hiring new or temporary staff, and maintaining communications with staff who are directed to stay at home or work from London office.

Responsibilities include:

- accounting for staff (Emergency Contact)
- staff and emergency contact communications (Emergency Contact)
- providing emergency contact information to authorities (COO)
- ensuring injured staff and relatives are contacted (Emergency Contact)
- maintaining payroll, ensuring accurate/timely salary payments (HR)
- helping get staff back to work as quickly as possible (COO)

- formulating formal staff communications (COO)
- post disaster assessment and review, and report to the Management Team (COO)

Information Requirements:

- Staff emergency contact details
- Contact information providers

3.3   FACILITIES

The Management Team's main function is to co-ordinate the external resources required to safeguard BLN staff and provide working access to the office premises. They are not responsible for physically executing all the actions but coordinating the outsourced resource to ensure the actions happen. The Management Team's initial responsibility is to safeguard staff from any hazards resulting from a physical incident. Evacuations Officer, Maggie Komorowska is responsible for managing evacuation and preventing access to the building until the area has been declared safe. Vik Lad is the deputy evacuation officer. The Team's primary focus will then be to coordinate working access to the office premises.

3.4   INFORMATION TECHNOLOGY

As the IT systems are hosted by outsourcing partners, the Business Continuity Plan (BCP) and Disaster Recovery (DR) processes for IT systems are linked to the related BCP and DR processes for those providers.

There is a separate Information Technology Business Continuity Plan owned and maintained by the Chief Technology Officer.

As the business is a 'Digital' business and applications are hosted in secure data centers offsite then access to those systems can happen from any location where internet services are available. This means that in the event of a disaster at a BLN business location it will be possible to continue to run the business from alternative locations with minimum disruption.

For Corporate IT applications, the hosted server infrastructure is constructed as a virtual estate with daily backups of all data. There is a DR recovery level of 8 hours.

For the main client application, the hosted server infrastructure is constructed as a virtual estate with daily backups of all data. The contract provides for a DR recovery service level of 8 hours.

For the loan administration application, there is a primary and secondary hosting location with replication of data between sites. There is a DR recovery service level of 6 hours.

The Chief Technology Officer or his delegate is responsible for overseeing the testing and maintenance of computer and communications system supported by Ocean/ TCP including all telephone and fax communications. The scope of their responsibility encompasses all core computer systems, applications, telephony, system and associated equipment cabling. In addition, the CTO is responsible for all key applications, connectivity, local area network and personal computers, including hardware, cabling, system and application software, data communications systems (hardware and software), and associated equipment cabling. In a crisis, the CTO will assess the damage and determine the impact. If further damage can be minimized, he will be responsible for

applying protective measures and salvaging equipment. The highest priority will be given to restoring, supporting and providing access to the core business systems.

Responsibilities include:

- Assisting in determining business impact
- Establishing technology recovery strategy
- Mobilisation and tasking of Ocean
- Minimising damage and salvaging resources (where worthwhile)
- Determining telecommunication and system priorities
- Restoring hardware, software and cabling
- Locating, acquiring & redeploying hardware
- Restoring telephony software, client data and system data from backup
- Testing voice comms and data system operations
- Testing all system operations
- Identifying power requirements
- Monitoring of progress at office site to ensure speedy recovery and return

3.5   EXTERNAL COMMUNICATIONS

The Head of Marketing's responsibility is to channel and coordinate all formal communications between external parties. The Head of Marketing will act as primary contact for all media agencies and will notify them as appropriate.

Responsibilities include:

- Gathering accurate information
- Notifying media agencies of briefings
- Drafting any media release and authorising as appropriate
- Liaising with emergency service PR unit
- Advising staff on media comment
- Acting as primary media contact

3.6 CLIENTS MONEY RESOLUTION PLAN (CASS RP)

BLN maintain a CASS RP which must be reviewed on a regular basis. This is to ensure that its records are up-to-date and can assist an insolvency practitioner on a primary pooling event. The CASS RP provides relevant practical information and ensures records are readily accessible to the insolvency practitioner, facilitating a prompt return of client money in case of platform failure.