
Mind Your Own (Micro)Business: Fraud, Risk and Microbusinesses

DEVON AIREY AND JODI GARDNER

1. Introduction

This chapter calls for an increased focus on the inherent risks associated with operating as or contracting with a microbusiness ('MB') in the world of commercial contracting, particularly those risks related to fraudulent transactions. The lack of focus, by academia or regulators, on MBs creates a range of risks – both to the business themselves and trading with them.

First, MBs are provided with little-to-no tangible protection against larger companies despite their relative lack of expertise in purchasing products or services, high opportunity costs of time spent making such decisions, and poor bargaining power.¹ For the purposes of commercial law, both legislative and common, MBs are treated the same as larger businesses.

Secondly, MBs are increasingly vulnerable to fraud – as they tend to have limited awareness or resources to protect themselves from exploitation. The Department for Digital, Culture, Media and Sport recently reported 38% of MBs fell victim to cyber-fraud in 2021; a third of which suffered significant financial loss as a result. Despite these real concerns, 80% of MBs do not see cyber-attacks and data loss as a considerable threat to their business.² This lack of awareness means that they do not take steps to protect themselves and therefore remain vulnerable to these fraudulent activities.

¹ A Fletcher, A Karatzas, A Kreutzmann-Gallasch, 'Small Businesses as Consumers: Are they Sufficiently Well Protected?' (Centre for Competition Policy, 2014). *National Westminster Bank plc v Morgan* [1985] AC 686 (HL), 707–708 (Lord Scarman) who dismissed Lord Denning's view in *Lloyds Bank Ltd v Bundy* [1975] QB 326 (CA) 339).

² The Department for Digital, Media, Culture & Sport, *Cyber Security Breaches Survey: 2022*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1089586/Cyber_Security_Breaches_Survey_2022_Infographic-Micro_Small_business.pdf (last accessed 30 May 2023).

The chapter has six sections. The second outlines the framework of MBs, focusing specifically on the United Kingdom (UK), Singapore and Australia. It outlines the background, regulatory environment and recent developments in MBs in the three countries, and highlights that MBs are more likely to be both victims and perpetrators of fraud in commercial transactions. The third section develops this outline by discussing how MBs fall victim to fraud in the three countries, while section four considers the rate and situations where MBs can be perpetrators of fraud – with a particular focus on COVID-19 transactions. The fifth section provides suggestions for regulatory reform in order to ‘level the playing field’ for MBs, both in terms of their transactions with consumers but also with other businesses. The sixth section concludes the chapter.

2. Show (Micro)Business: The Framework of MBs

In the UK, MBs are defined under the Companies Act 2006, s 384A as a business consisting of not more than 10 employees with a turnover of no more than £632,000. In Australia, there is no single definition of a MB. The Australian Bureau of Statistics (‘ABS’) defines an MB as a small business with 0–4 employees, and a small business as having 5–19 employees. In contrast, the Corporations Act 2001, s 45(2) defines a ‘small proprietary company’ as a company which has at least two of the following: (a) a consolidated gross operating revenue for the financial year of less than AUD10 million; (b) a value of the consolidated gross assets at the end of the financial year less than AUD 5 million; and (c) fewer than 50 employees. In Singapore, the Ministry of Trade and Industry defines SMEs (Small and Medium-sized Enterprises) as a business with an annual sales turnover of under S\$100 million, or one that employs less than 200 workers.

The focus of this chapter is not to address these differences or provide a comprehensive definition of MBs that can apply globally.³ It is important to recognise that MBs are a specific and unique type of small business that generally has the resources, skills, and knowledge more aligned with a consumer than a standard ‘business’ party to a transaction.

Despite their size, MBs are vital organs of the local and global economies. In the UK, there are approximately 5.3 million MBs, accounting for 95% of all businesses,⁴ contributing c.£5.5 billion annually to the economy and employing one-fifth of UK workers.⁵ MBs are also on the rise in Singapore. Whilst no specific

³ We do note that there have been calls for a more robust definition of MBs to be developed and we agree with this call: see The McKell Institution, *Micro but Mighty: Magnifying Microbusinesses in Australia* (2023) (last accessed 21 August 2023) p 17.

⁴ Commons Library Research Briefing, ‘Business Statistics’ (21 December 2021), 12. Available at: <https://researchbriefings.files.parliament.uk/documents/SN06152/SN06152.pdf> (last accessed 30 May 2023).

⁵ *ibid.*

figures are currently available, SMEs in Singapore make up 99% of all enterprises and provide employment to 70% of the workforce.⁶ The numbers of MBs are generally increasing year-on-year as jobseekers are drawn to the entrepreneurship, freedom and flexibility afforded by MBs compared to larger, more traditional businesses.⁷ In Australia, MBs employ 2.9 million people (in a country of just under 26 million people) and generate \$265 billion for the economy.⁸

Following the COVID-19 pandemic, reports of MBs as victims and perpetrators of fraud have made headlines.⁹ There is limited research on the relationship between fraud and MBs from a legal and regulatory perspective. This is unfortunate. The vital role MBs play in the global economy, and the considerable size of the MB population, combined with their limited experience in fraud prevention, makes them fertile ground for fraudulent activity. Nonetheless, MBs often evade the scope of legislative or common law protections. It is beyond the scope of this paper to analyse the motivation of fraud offenders, however such fraudsters are often motivated by a mixture of economic need, created by a decline in business activity and loss of jobs, and personal greed driven by apparent opportunities to access extra capital, especially in a time of crises where there is a perceived reduction in fraud controls.¹⁰ Additionally, fraud arises from the absence of capable guardians, who can act as an inhibiting factor in the decision to act illegally and/or dishonestly. In particular, law enforcement priorities have often excluded MBs from the scope of their supervision, concluding that such regulation presents unnecessary and burdensome ‘red tape’.

In the sections that follow, this chapter shines a spotlight on MBs as both victims and perpetrators of fraud, and the legislative and regulatory environment that makes engaging with MBs a ‘risky business’.

3. Risky (Micro)Business: MBs as Victims

It is a common trend in multiple countries around the world that MBs are significantly more likely to fall victims of fraudulent activities. For example, a survey and report from Xero from 2021 showed that nearly one in five Australian small businesses had been victims of ‘invoice fraud’ and, as a result, falsely paid out

⁶ Singstat, “Enterprise by SMEs and Non-SMEs” (28 March 2023). Available at: <https://tablebuilder.singstat.gov.sg/table/TS/M600981> (last accessed 30 May 2023).

⁷ Office of National Statistics, ‘UK Business; activity, size and location: 2021’ (4 October 2021). Available at: www.ons.gov.uk/businessindustryandtrade/business/activitysizeandlocation/bulletins/ukbusinessactivitysizeandlocation/2021 (last accessed 30 May 2023).

⁸ The McKell Institution, *Micro but Mighty: Magnifying Microbusinesses in Australia* (2023) 20.

⁹ See, eg, Sky News, ‘£1.1bn of COVID small business loans identified as fraud, claims government source’ (3 September 2022). Available at: <https://news.sky.com/story/1-1bn-of-covid-small-business-loans-identified-as-fraud-claims-government-source-12688393> (last accessed 30 May 2023).

¹⁰ M. Levi and R.G. Smith, *Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19*, Research Report 19: Australian Institute of Criminology (2021).

AUD\$15,500 on average.¹¹ Data from Scamwatch further supported this, stating that MBs are the fastest growing scam victims in Australia, with a 130% increase in activity between 2021 and 2023. An example was provided of a farmer from Western Australia who lost over \$1 million when their email account was compromised. The scammers then fraudulently updated two invoices for payments – one for grain and one for agricultural machinery – with different bank details.¹² As MBs are struggling to survive in a post pandemic cost-of-living crisis, this amount can have an overwhelming impact on their survival and longevity.

The consequences of fraud are also exceptionally severe for MBs, as they are less likely to have mechanisms in place to protect themselves and therefore more likely to have long-term detrimental impacts. For example, in 2022 the United States Securities and Exchange Commission ('SEC') reported 60 per cent of SMEs went out of business within six months of a data breach or cyber-attack.¹³ The SEC commented that 'Cyber security is clearly a concern that the entire business community shares, but it represents an especially pernicious threat to smaller businesses'.¹⁴ Despite having similar resources, knowledge and ability to protect themselves, small business fraud is three times more profitable than consumer fraud.¹⁵ This is not, however, a new issue: in 2015 the SEC Commissioner Luis A. Aguilar issued a statement about the issues of cyber fraud and small businesses. In this he commented that SMEs 'are not just targets of cybercrime, they are its principal target'.¹⁶

One of the main reasons MBs are more likely to be victims of fraud is that they often do not have the size or resources to adequately protect themselves. The SEC review discovered that the smaller the business, the less they prioritise protection from fraud, particularly cyber-fraud. This means that MBs are particularly vulnerable and likely to be victims.¹⁷ For example, the Xero survey discovered that nearly three in 10 small businesses in Australia do not spend *any* money on cyber-protection or education for their business.¹⁸

¹¹ Xero, 'Nearly one in five Australian small businesses a victim of invoice fraud', (8 November 2021). Available at: www.xero.com/au/media-releases/nearly-one-in-five-australian-small-businesses-a-victim-of-invo/ (last accessed 30 May 2023).

¹² Australian Competition and Consumer Commission, *Targeting scams: Report of the ACCC on scams activity 2022* (April 2023). Available at: www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-report-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2022 (last accessed 21 August 2023) 26.

¹³ MoneyBusiness, 'More than half of small businesses close after a cyber attack', (24 February 2022). Available at: www.mybusiness.com.au/resources/news/more-than-half-of-small-businesses-close-after-a-cyber-attack.

¹⁴ *ibid.*

¹⁵ Experian (2009) *Identifying Small-Business Fraud* (An Experian White Paper) p 1.

¹⁶ Luis A Aguilar, 'The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses', 19 October 2015. Available at: www.sec.gov/news/statement/cybersecurity-challenges-small-midsize-businesses (last accessed 30 May 2023).

¹⁷ *ibid.*

¹⁸ Xero, 'Nearly one in five Australian small businesses a victim of invoice fraud', (8 November 2021). Available at: www.xero.com/au/media-releases/nearly-one-in-five-australian-small-businesses-a-victim-of-invo/ (last accessed 30 May 2023).

This situation is exacerbated by the fact that fraud, particularly to small businesses, is of decreasing importance to law enforcement around the world. Nowhere is this more obvious than in the United States, where fraud is steeply rising but support from law enforcement for investigating and prosecuting fraud cases is decreasingly significantly. For example, data from the US Justice Department highlights those prosecutions of frauds against financial institutions dropped 48 per cent from 2000 to 2007.¹⁹ This is particularly evident for MBs, as the smaller the fraud committed, the less likely that the police will investigate and, where appropriate, prosecute.²⁰

4. A (Micro)Business Affair: MBs as Perpetrators and Facilitators

Frequently overlooked is the role of MBs in perpetrating and/or facilitating fraud. Three prevalent practices are discussed in this section. The first concerns material misrepresentations made by or on behalf of MBs in respect of applications for loans, credit, or grants. In this example, MBs can perpetrate and facilitate fraud by evading the controls and regulation supervising bank-to-MB or government-to-MB lending. The second example concerns instances where MBs facilitate fraud due to failings in their ability to mitigate against, for example, phishing scams or email compromise, causing loss to third parties. The third example concerns MBs as ‘money mules’ who, knowingly or not, allow their business account to be used by fraudsters for money-laundering purposes.

These examples expose deficiencies in the law’s approach to MBs. MBs all too often fall outside the scope of legislative and regulatory provisions designed to mitigate against fraud. Despite the increasing prevalence of MB fraud, new proposals by the UK Government to combat economic crime omit MBs from their scope. This is unfortunate. While it is important that ‘red tape’ does not stifle the ability of MBs to conduct business, excluding them entirely enables economic harm.

4.1. MB Lending Fraud

In MB lending fraud, MBs (or individuals purporting to be MBs) make loan applications which materially misrepresent the purpose of the loan and/or the identity and nature of the business. According to a recent report, the average year-on-year increase in MB lending fraud is 14.5%, compared to 6.9% in 2021, and is estimated to represent up to 15% of overall losses sustained by lenders.²¹ Two factors have

¹⁹ Experian (2009) *Identifying Small-Business Fraud* (An Experian White Paper) p 2.

²⁰ *ibid.*

²¹ LexisNexis Risk Solutions, *The State of Small Business Lending Fraud* (2023: LexisNexis).

driven this increase in fraud in recent years: first, the uptake in and emergency provision of loans as a result of recent crises (including the pandemic and cost of living), and second, the uptake in applications being made via remote channels (such as online or over the phone) as opposed to in-person.

The rise in MB lending fraud has a clear, causal relationship to the onset of the pandemic and the associated economic crisis. In the UK and Australia, reports suggest that MBs engaged in dishonest attempts to obtain government economic stimulus funding during the pandemic.²² In Australia, the pandemic led to a substantial increase in government-support payments being made to small and MBs. The Coronavirus Economic Response Package Omnibus Act 2020 contained 16 schedules of support payments enabling MBs to claim between \$20,000 and \$100,000 as a cash flow boost to help them maintain operations during the pandemic.²³ Similarly, in the UK, stimulus programmes included the Bounce Back Loan Scheme. Under the scheme, eligible businesses could apply for a 100 percent, government-backed loan of up to £50,000 per business, with no interest charged or repayments during the first 12 months. By August 2020, more than 1.5 million businesses had borrowed up to £50,000 each, worth a total of £35bn.²⁴

It is now believed that a proportion of these loans were provided to MBs in the UK and Australia who had dishonestly made claims outside the strict eligibility requirements.²⁵ According to the National Audit Office, around 11 per cent of the loans granted under the UK's Bounce Back Loan Scheme were fraudulent – equating to some £4.9 billion.²⁶ The scale of the fraud remains unknown.²⁷ The limited literature has so far identified three ways in which the material misrepresentations were perpetrated by or on behalf of MBs: MBs inflated their turnover or other requirements in order to fit the eligibility criteria and/or receive more funds; MBs made a loan application through the business and then, upon receipt, declared the company insolvent; and MBs applied to multiple lenders for a loan.

The speed and urgency with which the schemes were introduced, which led to insubstantial due diligence and regulations for approving applications, has been the primary rationale provided for this type of fraud. This appears to be only part of the problem. The inadequacy of the current law in identifying and combating fraud perpetrated by and through MBs undermines efforts to diminish the risk of economic harm. Legislative measures, both prior to and following the pandemic,

²² *ibid.*

²³ Australian Treasury, Annual Report 2020–21. Available at: <https://treasury.gov.au/sites/default/files/2021-10/p2021-216241-tsy-annual-report-2020-21.pdf> (last accessed 30 May 2023).

²⁴ HM Treasury, Annual Report and Accounts 2020–21. Available at: www.gov.uk/government/publications/hm-treasury-annual-report-and-accounts-2020-to-2021 (last accessed 30 May 2023).

²⁵ S Browning, *Coronavirus: Business loans schemes* (House of Commons Library, 21 March 2023).

²⁶ *ibid* p 37.

²⁷ Browning, *Coronavirus: Business loans schemes* (n 25). See also HMRC, *Error and Fraud in the COVID-19 Schemes: methodology and approach (an update for 2022)*, (18 July 2022). Available at: www.gov.uk/government/publications/measuring-error-and-fraud-in-the-covid-19-schemes/error-and-fraud-in-the-covid-19-schemes-methodology-and-approach-an-update-for-2022 (last accessed 30 May 2023).

either entirely omit MBs from their scope in preventing fraud or fail to adequately recognise the part MBs play in perpetrating and facilitating fraud.

A failure to consider the role of MBs in perpetrating fraud is illustrated by the Rating (Coronavirus) and Directors Disqualification (Dissolved Companies) Act 2021 ('CDDA'), introduced in December 2021. The CDDA was introduced to prevent directors (whether naively or deliberately) dissolving their company to avoid repaying debts owed to the Bounce Back Loan Scheme. The legislation extends the Insolvency Service's powers to investigate and disqualify company directors who abuse the company dissolution process. In announcing the changes, the government emphasised that the measures would specifically 'tackle directors dissolving companies to avoid repaying Government backed loans put in place to support business during the Coronavirus pandemic'.²⁸ Nonetheless, the enforceability of the Insolvency Service's new measures are unlikely to have any substantive effect on MBs. Under the CDDA, s 6, the court is obliged to disqualify a director where they are found to be unfit. Although, given the company will not have become insolvent (within the meaning of the CDDA) prior to dissolution, there will be no office holder responsible for reporting on the conduct of its directors prior to dissolution. It appears, therefore, that the Insolvency Service will be heavily reliant on the creditors of a dissolved company to raise concerns regarding its directors' conduct in order to initiate their investigations. While a creditor may be able to benefit personally from any resulting compensation order, providing an incentive to participate, it is far from clear such incentives will exist for creditors of MBs – who may consider the size and limited means of the business, and the costs associated with any enforcement measures, to outweigh the value of the loan itself. In any event, the Insolvency Service's guidance 'Dissolved Company Investigations', makes clear that the primary purpose of any investigation is to protect the public or the business community, not the repayment or recovery of assets for creditors and, before it will consider bringing a case, the Insolvency Service must be satisfied the expense is justified.²⁹

The pandemic also accelerated the development of, and changes in, the methods by which loan applications are made. Post-pandemic, nearly three-quarters of all loan applications are made online or by mobile. It is estimated that some 19 per cent of MB lending fraud losses are attributed to these changes, and presented further difficulties in verifying the truth of the statements made. While such fraud is clearly a result of inadequate internal controls and fraud prevention mechanisms by lenders – indeed most fraud is not caught until *after* the point

²⁸ HM Government, 'Crackdown on directors who dissolve companies to evade debts' (16 December 2021). Available at: www.gov.uk/government/news/crackdown-on-directors-who-dissolve-companies-to-evade-debts#:~:text=Rogue%20directors%20who%20dissolve%20their,disqualified%20from%20being%20a%20director.&text=The%20Insolvency%20Service%20has%20been,to%20avoid%20paying%20their%20liabilities (last accessed 30 May 2023).

²⁹ Insolvency Service, 'Dissolved Company Investigations' (16 December 2021). Available at: www.gov.uk/government/publications/dissolved-company-investigations/dissolved-company-investigations (last accessed 30 May 2023).

of account origination (some 68 per cent of MB lending fraud),³⁰ it is concerning that, despite such growing practices by MBs, legislative measures nonetheless propose to *exclude* MBs from anti-fraud legislation. According to recent reports, Ministers are planning to exclude small UK businesses from measures targeting liability for businesses who ‘fail to prevent fraud’ contained in the Economic Crime and Corporate Transparency Bill.³¹ The UK’s Home Office stated that ‘the offence will only apply to large companies, to avoid disproportionate burdens on SMEs and support economic growth.’³² As discussed below, the inadequacies in the law’s response reveals a key misunderstanding about the role MBs can play in perpetrating and facilitating fraud, at the expense of both consumers, businesses and the broader economy.³³

4.2. Business Email Compromise

The current law further provides limited protection in instances where MBs *facilitate* fraud as a result of their inexperience, negligence and/or recklessness. A key concern is the rise of ‘Business Email Compromise’ or ‘phishing’ scams whereby fraudsters can infiltrate an MB’s email system and impersonate the MB, directing fraudulent payments to be made. While this form of fraud arises in all businesses, MBs are prime targets due to the (often) inadequate systems in place to detect fraud and prevent cyber-security attacks. According to the Cyber Security Breaches Survey, 39 per cent of the UK’s small and MBs were subject to a cyber-attack in 2022, with an average cost per attack from loss of money or data of £4,200.³⁴

For example, the Western Australian farmer discussed in section 2 above, was a victim of Business Email Compromise, when their business partners paid nearly AUD \$1 million to scammers who issued fake invoices as opposed to the farmer who owed the money. The current law in England, Australia and Singapore provides little guidance on who is to bear the responsibility for such fraud – the business or consumer who made the payment to the wrong account, or the MB whose email account was hacked? This presents key challenges to those transacting with MBs – particularly in relation to consumers who, like MBs, often also lack the sophistication to detect and prevent cyber-attacks. Thus far, three responses to

³⁰ LexisNexis Risk Solutions, *The State of Small Business Lending Fraud* (2023: LexisNexis).

³¹ See, eg, ‘Small UK companies set to be excluded from anti-fraud legislation’ (13 March 2023). Available at: www.ft.com/content/ddbbe258-e0d2-40ad-bfd5-23b9b91cf51d (last accessed 30 May 2023).

³² HM Government, ‘Factsheet: failure to prevent fraud offence’ (11 April 2023). Available at: www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/factsheet-failure-to-prevent-fraud-offence (last accessed 30 May 2023).

³³ See also the recent comment from Cifas, the UK’s leading fraud prevention service, which expressed concern at MBs’ exclusion from the ‘failure to prevent’ fraud legislation. Available at: www.cifas.org.uk/newsroom/economic-crime-plan (last accessed 18 October 2023).

³⁴ HM Government, ‘Cyber Security Breaches Survey 2022’ (11 July 2022). Available at: www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022 (last accessed 30 May 2023).

determining liability have been posited and will be discussed in more detail below, but none adequately assist MBs in detecting and preventing such attacks, nor do they adequately mitigate against the harms incurred.

The first response is to consider the contractual position governing the parties. It is common ground that one of the primary purposes of a contract is the allocation of risk between contracting parties. Accordingly, in circumstances where one party has sustained a loss, any relief to be obtained may be provided for in such a contract. This response rests on two assumptions: first, that the parties have entered into a binding agreement; and second, that such an agreement contained an express or implied term allocating responsibility for the loss presented by Business Email Compromise. Finding that the parties have entered into a binding agreement is unlikely to be contentious – even for MBs and consumers, who lack the sophistication of larger commercial parties, it is common practice for contracts of goods or services to be entered into. More difficult is identifying a precise term that allocates responsibility for the loss caused by Business Email Compromise (or similar such frauds). At present, no such legislation exists which gives authority for such terms to be readily implied or incorporated. Further, it is rare for an MB contract to expressly allocate the risk arising from Business Email Compromise.

Another response the law may adopt is to determine whether the MB owes the consumer or other transacting party a duty of care to ensure that payment instructions are not altered by reason of the MB's negligence. Although such a duty is not established under the current law, parallels have been drawn with case law on cheque fraud, which state that a duty is owed by a customer to a bank when drawing on a cheque which was intercepted by a third-party fraudster. For example, in *Young v Grote*,³⁵ the plaintiff was a customer of the defendant bankers; on leaving home he entrusted to his wife several blank forms of cheques signed by himself desiring her to have them filled up according to the exigencies of his business. Mrs Young subsequently, for the purpose of the business, required the sum of £50 2s. 3d. and she delivered one of the cheques so signed by her husband, the plaintiff, to a clerk of the plaintiff, and asked him to fill it up with such sum. The clerk subsequently altered the cheque so it was drawn in the sum of £350 2s. 3d., presented it at the bank and absconded with the proceeds. It was held that a customer drawing a cheque owes a duty of care to the bank to take care that it cannot be altered and that, by reason of Young's negligence, he was liable for the loss suffered.

The House of Lords in *London Joint Stock Bank v Macmillan*³⁶ cited the duty of care established in *Young v Grote* with approval. Lord Finlay LC noted at p 810:

'The ground on which *Young v Grote* proceeded was, according to my judgment of three out of the four judges, simply this, that if a customer in drawing a cheque neglects reasonable precautions against forgery and forgery ensues, he is liable to make good the loss to the banker and the fact that a crime intervenes to cause the loss does not make it too remote ... No one can be certain of preventing forgery, but it is a very simple thing

³⁵ *Young v Grote* (1827) 4 Bing 253.

³⁶ *London Joint Stock Bank v Macmillan* [1918] AC 777.

in drawing a cheque to take reasonable and ordinary precautions against forgery. If owing to the neglect of such precautions it is put in the power of any dishonest person to increase the amount by forgery, the customer must bear the loss as between himself and the banker.’

In *Macmillan*, the respondents’ firm, which had an account at the appellant bank, entrusted to a clerk the duty of filling in the cheques for signature. The clerk presented to one of the partners of the firm for signature a cheque drawn in favour of the firm or bearer. There was no sum in words written in the space provided for the writing, and there were the figures ‘2.0.0’ in the space intended for figures. The partner signed the cheque. The clerk subsequently added the words ‘one hundred and twenty pounds’ in the space left for the words and wrote the figures ‘1’ and ‘0’ respectively on each side of the figure ‘2’. The clerk presented the cheque for payment and obtained the funds out of the firm’s account. It was held by the House of Lords that the bank was entitled to debit the firm’s account with the full amount of the cheque.

There are, of course, differences with MBs. Most obviously, the cases concern a relationship between customer and bank, as opposed to the position between an MB and its customer. Further, it is by no means clear a court will find there to be sufficient proximity and foreseeability in an instance of Business Email Compromise, such that an MB would be deemed liable for any failure to prevent such fraud. Indeed, the law of tort has been averse to finding that omissions give rise to liability unless there is some ‘special relationship’ between the parties. It is not altogether certain that a relationship of MB and customer will give rise to such a relationship.

It must also be queried whether recognising such a duty will have the effect of ‘opening the floodgates’, and therefore be deemed undesirable. Lord Scarman in *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd*³⁷ rejected the notion that a duty to take reasonable care in drawing a cheque extends to a common law duty to organise one’s business in such a way as to prevent fraud. In *Tai Hing*, a bookkeeper perpetrated a series of frauds on his employers. In some cases, he tricked them into signing blank or incomplete cheques which he converted and completed. There was no attempt by the company to check his activities and his frauds went undetected from approximately six years. The employers accepted responsibility for all cheques which carried genuine signatures but demanded that the three banks recredit the firm’s respective accounts with the amounts paid out against the forged cheques. The bank’s defence was, principally, that the frauds were occasioned by the firm’s negligence in the way it conducted its business. Reversing the Hong Kong Court of Appeal’s decision in favour of the banks, Lord Scarman emphasised that a customer’s duty of care was confined to what could:

‘... be seen to be plainly necessary incidents of the relationship. Offered such a [current account] service, a customer must obviously take care in the way he draws his cheque, and must obviously warn his bank as soon as he knows that a forger is operating his account.’³⁸

³⁷ *Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank Ltd* [1986] AC 80.

³⁸ *ibid* 106D.

His Lordship however rejected the view that the customer's duty at common law went further than this. Accordingly, unless it can be established that there are certain '*incidents of the relationship*' which give rise to a duty of care, the courts are unlikely to hold that an MB owed its customer any duty of care to prevent the fraud.

That no duty of care is owed in such circumstances was affirmed by the English Court in *Sell Your Car with Us Ltd v Sareen* [2019] BCC 1211. Mr Sareen had sold a Maserati Levante car through the company and, under the terms of the contract, the company was obliged to pay him £51,800. A third party fraudulently intercepted the email exchanges between the company and Mr Sareen. The third party, impersonating Mr Sareen over email and telephone, induced the company to wrongly divert £30,000 to a different bank account under the control of the fraudster. The company refused to pay up and Mr Sareen served a statutory demand. The company issued an injunction to restrain the presentation of a winding-up petition. The company argued that they had a genuine counterclaim against Mr Sareen equal to the debt on the basis that: first, there was an implied term in the contract that Mr Sareen would take reasonable care over the security of his email communication which he had failed to do; secondly, there was an implied representation by Mr Sareen that he had reasonable control over the security of his emails. If he did not, it amounted to a negligent misrepresentation. The Court rejected both arguments. It held that there was no basis to imply a term as it was neither necessary nor obvious that such a term should be implied. Further, the mere agreement by Mr Sareen to accept communications by email did not imply any representation about the security of his email account or control he exercised. It represented no more than that he was contactable at that address. Even if supplying his email address did amount to a representation, there was no evidence that the company had relied upon any such representation or that any alleged representation was false at the time it was given.

The result is that MBs are not only perpetrators of but, increasingly, facilitators of cyber fraud by virtue of their flawed IT systems and/or failings to adequately prevent such attacks. The current law has no clear means by which customers of MBs can be adequately protected from such harms. Nor has the law provided clarity on how such losses should be allocated.

4.3. Money Muling

Another example of MBs facilitating fraud is the practice of 'money muling', which involves a fraudster using a third party's bank account for money laundering purposes. It takes various forms but, in the MB context, typically involves the fraudster claiming to be interested in 'investing' in the MB. Funds are paid by the fraudster into the MB's account and, over time, the MB is persuaded to transfer the funds into another (fraudulent) account. Often, MBs are unaware of their role in such money-laundering activities. For example, one former MB owner

interviewed by the National Fraud Intelligence Bureau noted that they were unaware of why they had been targeted:

‘I had a small engineering company which I was trying to get off the ground. The first contact I had was by email from an investment company in the Middle East. They said they wanted to invest some capital into my company and they had other business interests in the UK. They only transferred a few thousand pounds at a time so the bank never questioned it.’³⁹

According to the National Fraud Database, in 2021 some 79,000 cases of fraud demonstrated a misuse of banking facilities, nearly three-quarters of which (72%) showed behaviours indicative of money mule activity.⁴⁰ As with loan misrepresentations and business email compromise, money muling activities have grown in prevalence since the COVID-19 pandemic and the cost-of-living crises whereby fraudsters have been known to more readily prey on an MBs’ need for investment.⁴¹

The current law’s response to money muling is a contradiction. On the one hand, MBs are portrayed as innocent victims unaware of having committed a crime and ‘tricked’ by a fraudsters’ fake investment offer.⁴² On the other hand, MB owners can face criminal sanctions for facilitating (even unwittingly) such activities.⁴³ At present, there appears to be no clear civil or commercial response to money muling by MBs. This is an area in urgent need of reform, as it is important to have clear guidelines on the approach to regulating these activities, specifically whether intent is necessary to be held liable for money muling.

5. Back in (Micro)Business: Levelling the Playing Field

The above sections highlight the commercial law’s deficiencies in responding to the specific issues presented by MBs as victims, perpetrators, and facilitators of fraud. The law has adopted an ‘all or nothing’ approach: either an MB is a ‘business’ and bound to follow the same rules as applied to medium and large businesses, which are significantly greater in both size and sophistication, or; it

³⁹ Action Fraud, ‘Alert: Small businesses tricked into laundering money’ (18 May 2016). Available at: www.actionfraud.police.uk/alert/alert-small-businesses-tricked-into-laundering-money (last accessed 18 October 2023).

⁴⁰ Cifas, ‘UK businesses under increasing attack by criminals as latest Cifas data reveals reported cases of fraud up 16%’ (28 April 2022). Available at: www.cifas.org.uk/newsroom/fraudscape-2022 (last accessed 18 October 2023).

⁴¹ See, eg. BBC, ‘Money launderers ‘prey on generation Covid’ (10 March 2021). Available at: www.bbc.co.uk/news/business-56334862 (last accessed 18 October 2023).

⁴² See, eg. Cifas ‘Latest fraud statistics reveal middle-aged mules targeted by online money laundering gangs’ (3 June 2021). Available at: www.cifas.org.uk/newsroom/middle-aged-mules (last accessed 22 October 2023).

⁴³ Such criminal sanctions are beyond the scope of this chapter. By way of a broad overview, money mules have been convicted for money-laundering offences under Part 7 of the Proceeds of Crime Act 2002 for prison sentences of up to 14 years. Available at: www.lloydsbankinggroup.com/media/press-releases/2022/lloyds-bank/money-mules-are-getting-older.html (last accessed 18 October 2023).

has opted to exclude MBs entirely from the scope of protective measures (such as anti-money laundering and economic crime legislation) in fear that this would overly-burden MBs with 'red tape'. Neither approach addresses the needs of, or risks posed by, MBs. In this final section, we provide recommendations for 'leveling the playing field'. Our recommendations are guided by two aims: the first is to provide MBs with more protection to mitigate against fraud; the second is to ensure MBs are also made accountable for their role in perpetrating and/or facilitating fraud.

5.1. Providing Additional Protection to MBs

The first recommendation is to afford MBs the same level of protection as consumers. This has already occurred in Australia with little controversy and significant popularity, but there does not seem to be the political appetite in either the UK or Singapore. The starting point is to recognise that MBs often have the same levels of knowledge, power, and resources as individual consumers. There is therefore a strong argument that they should be treated as consumers in terms of regulatory protection available. As outlined by Experian:

'Among fraud topics, small-business fraud and the challenges organizations face in identifying and mitigating these losses frequently are overlooked and are not well-understood. Small-business fraud is not as visible as consumer fraud because businesses often are not seen as victims in the way that consumers are. With no legislation requiring fraud to be reported and no national bodies to collate information, there is a dearth of information on which to base statistics.'⁴⁴

As has been proposed by the Law Commission in 2005⁴⁵ and in debates surrounding the passage of the CRA,⁴⁶ MBs should be included in the statutory definition of 'consumer' under the CRA (or, in Singapore, the Consumer Protection (Fair Trading) Act).

The primary objection to such an amendment is 'floodgate concerns' – that is, a substantial increase in the number of claims regarding unfair terms.⁴⁷ This can be easily dismissed. A sufficiently tight definition of MBs should be adopted. Such a definition already exists in the Companies Act 2006, s 364A which defines an MB as consisting of not more than 10 employees and having no more than £632,000

⁴⁴ Experian (2009) *Identifying Small-Business Fraud* (An Experian White Paper) p 1.

⁴⁵ The Law Commission and the Scottish Law Commission (Law Com no 292), 'Unfair terms in contracts: Report on a reference under section 3(1)(e) of the Law Commissions Act 1965 (Cm 6464 SE/2005/13).

⁴⁶ See, eg, Department of Business, Innovation and Skills, 'Protection of small businesses when purchasing goods and services: call for evidence' (March 2015). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/433139/bis-15-209-protection-of-small-businesses-when-purchasing-goods-and-services-call-for-evidence.pdf (last accessed 16 September 2021).

⁴⁷ *ibid.*

in turnover. This would translate to around 4.5 million MBs in the UK⁴⁸ and fewer than 300,000 in Singapore.⁴⁹ If this was considered to be too broad and increased the scope of protection beyond acceptable levels (something with which neither of the authors agree), the definition used by the Australian Bureau of Statistics – as a small business with 0–4 employees – could be utilised instead.

Regardless of which definition is used, the number of MBs will pale in comparison to the number of consumers, some 67 million in the UK⁵⁰ and 5.5 million in Singapore,⁵¹ for whom substantial protection has already been afforded. The significant detriment to the livelihood of MBs, and in turn the economy, as well as the adoption of unfair practices by larger corporations therefore cannot be justified by ‘floodgate’ arguments.

Amendments to the CRA can take inspiration from the success of reforms implemented in Australia, where MBs have been recognised as deserving the same protection as consumers. The Treasury Legislation Amendment (Small Businesses and Unfair Contract Terms) Act 2015 (Cth) amended the Australian Securities and Investments Commission Act 2001 and the Competition and Consumer Act 2010 to allow smaller businesses to be included in the Australian definition of consumer. Australian MBs thereby gain access to the greater protections of consumer law when contracting on account of their weaker bargaining power. Adopting a precise definition of when a small business can rely on consumer protections, Section 12BF provides that contracts with small businesses with an upfront contract price of AUD\$300,000 or less, or AUD\$1 million or less⁵² where the term of the contract is for more than 12 months are covered under the Act. Resultantly, small businesses benefit from enhanced protections, including a fairness test for the courts to apply to strike out unfair terms. Further, Australian law more adequately reflects the realities of B2MB contracting. It is notable that the reforms have received almost universal praise.⁵³

⁴⁸ Department for Business, Energy and Industrial Strategy, ‘Business Population Estimates for the UK and the Regions 2020’ (8 October 2020). Available at: [\(www.gov.uk/government/statistics/business-population-estimates-2020/business-population-estimates-for-the-uk-and-regions-2020-statistical-release-html#:~:text=Composition%20of%20the%202020%20business%20population,-The%20UK%20private&text=there%20were%20estimated%20to%20be,aside%20from%20the%20owner\(s\)\)](http://www.gov.uk/government/statistics/business-population-estimates-2020/business-population-estimates-for-the-uk-and-regions-2020-statistical-release-html#:~:text=Composition%20of%20the%202020%20business%20population,-The%20UK%20private&text=there%20were%20estimated%20to%20be,aside%20from%20the%20owner(s)) (last accessed 30 May 2023).

⁴⁹ The exact numbers in Singapore are not known, however there were estimated to be 291,000 SMEs in Singapore in 2021; the definition of MB will be significantly more restricted than that of an SME, therefore the numbers will be notably lower than the total number of SMEs.

⁵⁰ Based on the number of adults in the UK. Office of National Statistics: ‘Overview of the UK population: January 2021’ (14 January 2021). Available at: [\(www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/overviewoftheukpopulation/january2021\)](http://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/overviewoftheukpopulation/january2021) (last accessed 30 May 2023).

⁵¹ Based on the number of adults in Singapore: Statista, ‘Number of adults in Singapore from 2012 to 2021’. Available at: [\(www.statista.com/statistics/667768/number-of-adults-in-singapore-by-country/#:~:text=In%202021%2C%20there%20were%20approximately,the%20age%20of%2018%20years\)](http://www.statista.com/statistics/667768/number-of-adults-in-singapore-by-country/#:~:text=In%202021%2C%20there%20were%20approximately,the%20age%20of%2018%20years) (last accessed 21 August 2023).

⁵² Around £160,000 and £530,000 respectively.

⁵³ Debate has centred around whether protections for small businesses should be enhanced further, not whether they should have been introduced in the first place. See, eg, the Consumer Affairs Forum,

Such a reform would have numerous benefits. In economic terms, minimising opportunity and bargaining costs will allow MBs to grow through reduced difficulties caused by poor bargaining power. Additionally, by instilling a more ‘level playing field’, reform would incentivise larger businesses to be more efficient and innovative, driving productivity and GDP-per-capita.⁵⁴ In legal terms, the law will better reflect the nuances and realities of the business landscape and fulfil its stated aim of protecting against unfair terms. The reform also has the moral benefit of protecting against the increased commercialisation of individuals who, through self-employment structures such as the gig-economy, are more frequently being used as a ‘means to an end’⁵⁵ and for whom the UK Supreme Court has deemed it important to protect.⁵⁶ It would also put bigger businesses and – most importantly – financial institutions ‘on notice’ when contracting with MBs, ensuring that they are provided with the same level of protection as individuals. This places the risk on larger institutions, which are more likely to have the safety protocols, knowledge, and resources to have protections in place preventing fraud from occurring in the first place.

As MBs are both victims and perpetrators of fraud, it could be argued that providing them with ‘consumer’ status is too much of a risk, as it could allow them to facilitate fraud more easily. This, we argue, is using a sledgehammer to crack a nut. As will be discussed below in section 5.3, different mechanisms can be implemented to restrict MBs ability to perpetrate fraud and to hold them to account when this occurs. We believe that, instead of removing additional protection from all MBs, an approach that aims to hold the rogue businesses to account creates a much more equitable approach. It would be inappropriate and unfair to stop all MBs receiving additional protection because of a handful of bad apples who can be dealt with by other means.

5.2. Empower MBs to Protect Themselves

The second recommendation is to empower MBs, so that they can protect themselves from fraud. One of the most significant barriers associated with this is the cost of implementing fraud protection processes. It is therefore important to both increase the resources available to MBs for fraud protection and identify ways to create ‘economies of scale’ for fraud prevention for MBs.⁵⁷ This should include

‘Regulation Impact Statement for Decision’ (2020). Available at: <https://treasury.gov.au/publication/p2020-125938> (last accessed 30 May 2023).

⁵⁴ A. Fletcher, A. Karatzas and A. Kreutzmann-Gallasch, ‘Small Businesses as Consumers: Are they Sufficiently Well Protected?’ (Centre for Competition Policy, 2014).

⁵⁵ For an excellent exploration of this see J Prassl, *Humans as a Service: The Promise and Perils of Work in the Gig Economy* (Oxford University Press, 2018).

⁵⁶ *Uber BV and others v Aslam and others* [2021] UKSC 5.

⁵⁷ Luis A Aguilar, ‘The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses’, 19 October 2015. Available at: www.sec.gov/news/statement/cybersecurity-challenges-small-midsize-businesses (last accessed 30 May 2023).

encouraging businesses to work together to identify repeat fraud offenders and to share resources for developing fraud protection processes.⁵⁸

It is accepted that this is a difficult ask. A balance must be struck between what is realistically achievable for MBs in terms of protecting and monitoring for fraud, and what protection is necessary to ensure customers of MBs do not become victims. A starting point is to issue detailed government guidance to MBs on the standards they are expected to meet in respect of cyber-security. Government-issued 'best practices' or regulatory guidance can assist in signalling to MBs the extent of the risks faced, the actions that should be taken, and the resources available to them to consult. Unlike larger businesses, MBs often lack the expertise on how their business can be targeted. Educating MBs and providing resources to assist in bolstering their protection will help to ensure MBs can detect and prevent fraud. There are significant resources available for advising consumers on how not to avoid being victims of fraud, and similar advice and assistance should be provided specifically for MBs.

As outlined above, one of the main reasons that MBs are so frequently victims of fraud is that they lack the funds to create bespoke, tailored fraud prevention strategies in their business. Considering the growing reliance on MBs in the economic development across a number of countries *and* the devastating impact of fraudulent activities on MBs, it is important to think imaginatively about potential solutions. Creating systems where similar MBs can work together to develop and implement a fraud protection system that would be appropriate for all the businesses, but share the costs associated with its development.

5.3. Holding MBs Accountable

The third recommendation recognises that a balance needs to be struck. Where MBs are known to be perpetrators and/or facilitators of fraud, they must be held accountable. A significant weakness in anti-fraud legislation is its failure to include MBs within its scope. An oft-cited concern is burdening MBs with 'red tape'. MBs are likely to find it more difficult than larger businesses to comply with, for example, the reporting and compliance standards imposed by such legislation. This is not a reason to exclude MBs entirely from its scope. Parliament and policymakers must consider how such legislation can be tailored to the size and sophistication of the business. For example, by tempering, where necessary, the monitoring and reporting requirements for anti-money laundering and fraud legislation, or the level of sanctions for failing to comply.

To reduce and mitigate against the economic harms caused by Business Email Compromise, policymakers should consider introducing a legislative duty of care. This requires careful consideration: it would be unwelcome and cumbersome for the law to recognise a general duty of care to prevent fraud. Nonetheless, where

⁵⁸ Experian (2009) *Identifying Small-Business Fraud* (An Experian White Paper) p 2.

MBs transact with consumers and/or businesses via email and require those individuals or businesses to make payment in accordance with instructions provided by email, MBs should have a duty of care to ensure that those instructions are not intercepted by a fraudster due to the failure by the MB to detect and prevent against cyber-attacks.

Finally, lenders should strengthen internal controls when verifying loan applications made by MBs. This is particularly so where applications are made online and remotely – as has become increasingly frequent following the pandemic. Policymakers should consider regulating the checks lenders need to make in respect of customer due diligence and, where necessary, enhanced customer due diligence, before loans are granted.

6. Conclusion

Fraud is on the rise – particularly amongst MBs. This chapter has called for an increased focus on the inherent risks associated with operating as, or contracting with, MBs. The lack of focus by policymakers and academics on the relationship between fraud and MBs has created a range of risks for MBs themselves and those transacting with them. On the one hand, MBs are increasingly victim to fraud. As this chapter has shown, MBs are among the most targeted for cyber-fraud and are often ill-equipped to mitigate against such harms. Despite this, law enforcement has shown a decreasing interest in investigating and prosecuting such fraud – particularly among MBs where the losses sustained by MBs as victims of fraud are often small.

On the other hand, for certain types of fraud – such as loan fraud and Business Email Compromise – the MB population is among the main perpetrators or facilitators. The legislative and regulatory response has been the same: to exclude MBs from the scope of anti-fraud legislation and initiatives. Fears that MBs will become overburdened by ‘red tape’ are too simplistic. Policymakers need to adopt a more nuanced approach to anti-fraud controls, which are tailored to the size and sophistication of the business. Without this, further economic harms are inevitable.

