Title: Secure your PDQ

Agency: North Wales Police

1. Project Summary

Scanning

The investigation of a fraud at a Hotel led to the discovery of a major weakness in the card processing machines used by businesses throughout the United Kingdom. Organised Crime Groups were exploiting that weakness to defraud businesses out of large sums of money. Groups were prepared to travel long distances to commit offences as the rewards could be large and the risk low. In North Wales a series of offences were identified that showed clusters were committed within a short timescale. Under reporting of offences suggested that this could be a big problem nationally.

Analysis

By working through the features of the offence we focused on the factors which enabled the problem to persist as well as the combination of conditions that produced the problem.

Using the Problem Analysis Triangle we examined the features and relationships between the offender, location and victim to inform our responses. By breaking down the problem in this way we could see a national vulnerability in card processing machines being set with a default PIN when sent to businesses. This can be exploited by a motivated group of offenders taking advantage of victim's inability to protect their businesses to steal large sums of money. This analysis would inform our responses.

Response

We took a multi-faceted approach to the response and referred to the situational Crime Prevention techniques to focus our attention on appropriate responses. Locally this involved the investigation into the reported thefts, but with a national focus on prevention. We engaged the support of a Super-controller to open channels of communication with the banking industry, national regulators and the City of London Police. Multiple changes were made that would prevent the vulnerability in many cases, provide better security as well as increase the risk of being caught.

Assessment

The Coronavirus lockdown worked to our advantage as many businesses were forced to close denying the offenders the opportunity to commit the offences. We were able to effectively utilize this time to work with the banking industry to provide sustainable solutions to prevent this crime from occurring in the future. Within our own force there have been no crimes of this type reported. Surveying our own similar premises on Anglesey we have found a greater degree of security awareness and no devices set with default PIN numbers.

Word Count: 383

2. Description

A. Scanning:

The nature of crime has changed. In the UK, since 1995, whilst 'traditional' crime has fallen by 75% and has "been replaced by new forms of crime and harm" (Police Foundation, 2022:9). The internet has been related with a 47% increase in fraud, with an 89% increase in offences contravening the computer misuse act (CMA) between 2020 and 2021 (ONS, 2022)[1]. Of the 30,467 CMA offences recorded (year ending March 2021), only 0.2% (71) resulted in a charge and/or summons, with 27.3% (8,328) faced with evidential difficulties and/or an inability to identify a suspect [2] (Home Office, 2021b). Sadly, the proliferation of fraud offences and those responsible are often invisible to the police.

In 2020 a form of computer-based fraud came to the attention of North Wales Police, a territorial police force responsible for policing North Wales. The force has approximately 1,600 officers and is responsible for policing a largely rural area containing epic landscapes popular with tourists and outdoors enthusiasts. At 3.14am on the 20th of March 2020 three males engaged with the night porter at Tre-Ysgawen Hall, a rural spa hotel close to Llangefni. Whilst two served to distract him the third was seen by a guest to take the PDQ (Process Data Quickly), machine from behind the counter, before being observed to return it a short while later. All three then left in a taxi, explaining they were going out to get food,

[1] https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2020-to-2021/crime-outcomes-in-england-and-wales-2020-to-2021#experimental-statistics-outcomes-assigned-to-fraud-and-computer-misuse-act-cma-offences

[2] "These data are Experimental Statistics, which means that caution should be taken when interpreting the figures" (see Home Office, 2021).

which enabled the guest to inform the night porter what had occurred. The police were called and fortunately the attending police officer had experience of the hotel trade. She advised the night porter to run a “z” report. This showed the man who had momentarily taken the PDQ machine had used it to request a £18,000 refund in two transactions onto two different cards. The hotel was able to immediately stop the transactions and prevent the loss.

When the description of the men was circulated to other patrols, another officer explained that he had recently spoken to the occupants (who had been stationary in a car park 14 miles away), who explained they were on their way back to London. They were driving a luxury Mercedes C200 sport and soon identified travelling at more than 100 mph. The vehicle, containing four males was pursued and eventually stopped.

Further enquiries revealed this type of fraud had already been conducted locally. Two offences occurred on the same night in different areas of the force utilizing the same modus operandi. A further six offences had occurred in North Wales hotels, using the same modus operandi, a few months earlier:

4/12/19 – 3 Hotels

6/12/19 – 2 Hotels

9/12/19 – 1 Hotel

The sum from these offences was approximately £52,000. The modus operandi was similar in that the hotel was entered late at night and lone staff members were distracted. On each occasion one of the males took possession of the hotel’s PDQ machine and performed

multiple refund transactions onto a bank card, which went to a foreign account in the Netherlands. On each occasion the offenders replaced the PDQ and left the hotel and often the offence went unnoticed at the time.

This problem had the potential to affect every business that accepted card payments. Due to the lack of reporting to the police further enquiries were conducted using open-source research. Offences had been reported all over the UK, including the north and south of Scotland, middle and southern England. We discovered in 9 months reported losses of £150,000+ for this type of fraud which contributed towards the UK £620.6 million lost due to fraud in 2019 (see data table 1). This modus operandi appeared to have commenced from late 2019/early 2020 and was becoming increasingly common. UK Finance (Trade association of the UK Banking and Card Processing Sector) would categorise this type of fraud as Card fraud face to face and 2018 and 2019 data show it peaking at £69.8 million lost to UK businesses in 2018 (see data table 2).

These enquiries also established the national figure for this type of offence is difficult to establish and is artificially low, for a number of reasons. First the offences are not generally reported to the police but the banks, with refunds not being issued to business it was commonly not reported. Secondly, there is underreporting as businesses are often unaware, they have been targeted. Third, the figure supplied by UK Finance does not differentiate between individual crime types but provides generic crime types such as face to face, cardholder not present or courier frauds. They do not hold data regards PDQ involvement and generally would categorise as face to face but could not provide specific data.

Unlike card fraud offences where individuals are reimbursed by the banks for any fraud they are victim to, in this type of case the financial burden rests with the business. This can generate a disproportionate effect on the business's viability, especially when committed on independent hotels, such as the ones targeted here. Whilst the offenders could be dealt with locally this appeared to be a much bigger problem across the UK. (and possibly internationally), which needed to be tackled. The high value of these refund transactions had the potential to have a significant detrimental effect on the businesses, particularly in the Covid-19 climate whereby the hospitality sector has suffered huge financial loss. With a number of incidents in a short space of time it was clear that the problem was a new emerging threat and needed to be addressed before it caused more victims and organisational demand.

B. Analysis:

Using the Problem Analysis Triangle, the target, offender, and location were considered in sequence.

The Target - PDA vulnerability

The increase in electronic banking has increased the opportunity for fraud and in this type of modus operandi the PDQ machine is central to the offending opportunity and its use has evolved over time to improve user convenience. The PDQ itself is a portable device allowing the customer to pay for a product or service via electronic banking. Initially refunds required a supervisor card to be presented. However, these cards were copied or misused, which generated a change in the process. From 2019 all PDQ machines across the UK were accompanied with a personal identification number (PIN), and the machine could only be used if this code was typed into it. This was thought to provide a robust solution to prevent misuse of the PDQ machine.

Initially a default PIN was issued for each device and a guidance card sent out to each business customer explaining how the code could be changed. However, the financial authorities we contacted explained users found this unduly onerous, and many businesses were put off changing their PIN, leaving the default code (often set as 0000 or 9999) to aid their staff. However, this information had become known outside of the business allowing potential fraudsters to unlock the code by typing in 0000 or 9999. This then allowed them to transfer money to their own account.

Barclaycard are a significant stakeholder. They launched the UK's first credit card and continues to be a major supplier. They confirmed that business customers refuse to reset the generic PIN, mainly due to the security protocols involved in changing the code. Whilst security advice is provided on the Barclaycard monthly invoice, provided to each business customer, they conceded the reader of this message would be in a back-office accounts department rather than engaged in the payment process.

UK finance were able to provide information that demonstrated that operating companies had the ability to identify which locations still used devices with the default pin set. Clearly this vulnerability provided the ability for the operating providers to be exploited and the information shared with those wanting to target such locations. There was also no upper limit set to the amount that could be refunded through a business account, however the larger the amount the more likely it would be to stand out to the business from normal routine activity.

It was evident that the current security procedures surrounding the PDQ made it vulnerable to fraud. However, it was extremely difficult to establish the scale. Digital record would only show as a refund being issued by the device, with correct pin being used records were of no use in identifying a national scale.

Offender

Whilst many offenders involved in this type of crime go undetected, the males involved in the North Wales offences provide some insight. These were aged 19-25 and police records showed them belonging to a Somali Organised Crime Group (OCG), based in London with known links to the south of the UK. Analysis of their phone records shows them to be highly mobile and to travel long distances to commit their offences. Indeed, GPS tracking data from the offenders' vehicle shows they travelled directly from London to North Wales, only stopping once on the M6 motorway (the London to Anglesey distance is 302 miles).

Examination of one of the suspect's phones showed a journey from London to Northern Ireland returning through Scotland in the few days prior to the North Wales offences. This mobility assisted in protecting their anonymity as well as providing a legitimate reason for their location (i.e. tourists looking for a hotel). The rewards were epitomised by their choice to used high-cost, luxury hire/lease vehicles when traveling and the ability to attempt multiple offences in a short space of time. In essence the rewards were potentially large, and the risk of detection was low. The fact that the money transfers were directed to a Netherlands based bank shows the international nature of the fraud.

Location/Victim

The victims were particularly vulnerable. The offences committed in North Wales primarily involved independent, family run hotels or smaller chain hotels which reduced the chance of being warned, as national chains were more likely to pass on information. However, any business using PDQ card processing machines were potentially vulnerable to this type of offence. The hotels were targeted at night when staff levels were low. This enabled staff

members to be more easily distracted, which increased the opportunity of accessing the PDQ machine and also reduced the likelihood of being caught.

Further the victim was unlikely to report these frauds to the police. Many businesses accepted the crimes as part of operating losses or feared they would reveal business vulnerability. In some cases, it was possible that the loss may not have been detected for many weeks or months, if at all. This presented the opportunity for offenders to escape the scene undetected and many other legitimate transactions to take place using the PDQ machine. Further, coronavirus had increased the level of refunds to customers which masked the identification of crimes.

Nationally while some offences had taken place at hotels, others were identified as café and restaurants, either as part of a chain or local smaller businesses as well as other retail premises. Wherever a PDQ machine existed, and refunds made a vulnerability existed. The only common feature of the crime was the PDA functionality.

C. Response:

As this was both a local and national issue it required separate responses. These will be considered in turn.

Local Response

The officer attending the scene on the 20th March 2020 took responsibility for the intervention, supported by her local team and Inspector. She initially sent a message to local business using the 'pubwatch' scheme[3]. They were able to contact all licensee's, including hotels, pubs and restaurants to ensure that they protected their PDQ machines and were aware of the vulnerability. But the effect of a national lockdown meant that all licensed premises closed only 3 days later.

Local detectives completed a further investigation into the offences committed in North Wales and the arrested suspects. Bail conditions were put in place preventing them entering North Wales. Money was seized from their accounts and a wider examination of their mobile telephone data sought to provide links to other offences. This sought to remove the risk of future targets as well as deny them the benefits of crime. The investigation showed that the suspects hired a car in Croydon (South London) and left during the evening. They arrived at 12:15am at Bodysgallen Hall Hotel, Llandudno where they told the night porter they were there for a reservation. When it quickly transpired, they had no reservation they

[3] The pubwatch scheme is a local link that connects premises licensed to sell alcohol to a user group allowi9ng crime prevention information to be shared.

were asked to leave without getting close to a PDQ machine. They drove directly to Tre-Ysgawen Hall in Llangefni where they committed their offence. The account given by the suspect of going for a drive in his uncle's car was discounted by the fact that the vehicle was hired and had a tracker fitted to it. The four suspects were charged with offences of conspiracy to commit fraud , two were sentenced to a combined 33 months, while the other two remain wanted on warrant.

National response

It was discovered this type of fraud was emerging as an increasingly common national problem since the middle of 2019 to May 2020 across the UK. The City of London Police are the national lead for fraud and despite having a Dedicated Fraud and Payment Crime Unit (funded by UK Finance) they did not investigate this type of fraud. No other police force had had taken the national lead on the issue either. The direction of UK finance states "*It is vital that the industry works together with regulators and legislators to improve current payment processes and ensure that new systems have fraud prevention as an intrinsic part of their design.*" (UK Finance, Annual fraud report 2018)

The setting of a default PIN was creating a vulnerability that needed to be addressed. It was difficult to see how North Wales Police could influence the key industry leads such as Barclay card, the largest supplier of PDQ machines to change their operating methods. However, working with the force Problem Solving team we identified the National Police Chief's council (NPCC) leads for the relevant crime areas; banking crime, business crime and

fraud and sought to engage the industry 'super controllers'[4]. By doing this we hoped to gain support to influence the national providers through UK finance, the super controller for the finance industry, to implement a solution. The approach was made through our Deputy Chief Constable who wrote to the National Police Chiefs' Council leads to gain support. It was felt the City of London Police who hold the lead for commercial crime, should be the lead agency and they provided a point of contact of representatives who would help us.

Using the operational name 'Blue Centennial', a number of meetings took place between agencies to establish a solution. Members of the coordinating group involved the City of London Police, Barclay Card, UK Finance and North Wales Police. There were several strands to the work, which took place over several weeks. The meetings considered the 10 principles of crime prevention to consider how each could it at all be achieved. The project delivered short-term and long-term interventions.

Short term interventions

UK Finance stated that they had warned their members several years ago about the dangers of this type of offence and how to prevent it. The group reviewed the guidance material to encourage the securing of their premises and PDQ machines. Letters and booklets were produced by UK finance and distributed to all banks, and PDQ providers for circulation to all businesses with PDQ devices. This was focussed on target hardening and controlling access to their facilities. Within the literature, businesses are encouraged to password protect their

[4] Sampson, R., Eck, J.E., Dunham, J. Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. Security Journal (2010) **23,** 37 – 51. doi: 10.1057/sj.2009.17; published online 12 October 2009

PDQ machines, change any pre-set generic passwords on the PDQ and regularly change their own passwords. These measures if followed would have the effect of removing targets. However, we were mindful that many businesses had ignored similar advice. Specifically the measures included:

- Advice was provided to limit the number of staff with knowledge of the password and who had access to facilities. However, it was apparent this provided operational difficulties and placed increased demand on shift or service managers.
- Keeping PDQ machines out of arms reach, locked away in office etc outside of operation hours conceals targets.
- Linking the PDQ machine to the business computer system provides additional security, requiring four stages of authorisation to issue a refund.
- Extending guardianship involved educating staff to recognise when they are potentially being targeted.

Through trade bodies and social media, we encouraged premises and area management to set their own additional PINs, this was done sensitively in order that the correct audience only see the messages so as not to alert other offenders to this lucrative offence.

Longer term interventions

Following discussions with the Dedicated Card and Payment Crime Unit of the City of London Police we contacted banking organisations regarding future ways to frustrate and disrupt the activities of Organised Crime Groups in their use of this tactic. It was agreed that as part of a rolling programme any new or replaced PDQ machines would have an individual PIN assigned, and the PIN sent to the business separately (much like the security involved in

the issuing of a bank card). It was also agreed that the PDQ operating software would no longer show to the sector whether the default Pin was still active at each location.

PDQ service providers also reviewed the setting of refund limits. For example a café or coffee shop dealing in small transactions of say £5-£20, should alert the business owner if a refund request for £5000 is attempted. Reviewing the system, Uk finance agreed to extent the banking protocol in a way that similar to how unusual credit card transactions trigger an alert, then businesses would be phoned directly if there appeared an anomalous refund. Unusual activity include refunds when business don't normally refund, or where the refund amount is outside of identified normal parameters. This method prevented £60.7 million of fraud in 2021, 34 percent more than in 2020.

These short and long term interventions were based upon the following crime prevention principles:

- Target hardening. By providing crime prevention education we are denying future victims by ensuring that they are aware of the vulnerability and can act themselves to prevent becoming victims.
- Removing the means to commit crime. Reducing opportunity through a rolling program to replace default PIN's with unique pins will prevent future vulnerability. Taking away the ability to identify vulnerable property.
- Increasing the risk of being caught. Identifying unusual activity – By providing a method for operators to improve their ability to identify this method and contact the business to verify the action.

D. Assessment:

It is difficult to assess the efficacy of this project since March 2020. This is because the crime is often invisible as it is rarely reported to the police. Similarly, the coronavirus pandemic had an impact on reducing the opportunity as premises were often closed during this period. Large refunds were common during this period and this prevented offences being identified, many independent chains closed due to business losses which this offence likely contributed to.

Whilst national lockdown has been a considerable factor the period provided time to reflect on the weakness exploited by the offenders and instigate the simple changes to prevent this particular crime and stop businesses from becoming victims in the future. We have been able to work collaboratively with small businesses and their peer groups along with large Banking institutions to prepare responses which can lead to a reduction in harm and demand.

Starting our assessment with North Wales Police, there has not been a similar crime reported since March 2020. To establish whether this could be associated with our interventions during 2022 we surveyed 24 independent hotels that were situated on Anglesey, who had received our advice in 2020. We found all locations had received guidance from their PDQ provider with regards to having unique PIN numbers. All hotels except one location had set a unique pin, and that location stated they would do so after receiving the call. 50% had linked their booking system to their PDQ device, which provided

an extra level of verification for processing refunds. 63% now locked away PDQ devices out of hours and had re-sited their CCTV to observe their PDQ as an additional security measure. The evidence they provided during the calls gave us reassurance that the advice the advice had been followed and that the vulnerability would be far harder if not impossible to exploit.

Nationally it this is much harder to know the effects. As previously stated crime figures were artificially low, often being unreported. The opportunity to commit this crime appears to have been generated by efforts to control the use of the PDQ through the issuing of a PIN number. Conducting open-source research we did not identify any other cases being brought to court following our intervention (a similar approach had discovered such offences prior to our intervention). What we do know is that the opportunity surrounding this offence is very much reduced, and that the likelihood of committing a crime in the same way has been prevented. Consultation with UK finance has revealed that there have been no contact from PDQ providers or investigating agencies to highlight crime clusters of this type. The banking protocol identified an increase in identifying and preventing fraud in 2021 by 34%. This may be largely attributed to the involvement of this work in retail/hospitality refunds, or equally as attributable to variations in type and volumes of offences.

It is difficult to show the cost and benefit of the intervention. In terms of the inputs, these have been negligible and have just involved opportunity costs in terms of the police and banking practitioners. We can show in our Force area the intervention saved £52,000. However, it is likely that losses in larger metropolitan forces were much higher, and potentially more frequent. It should be recognized that North Wales is one of the UK's

smaller forces and is placed in a geographically isolated area. As such it is often one of the last forces to experience crime trends. Using this knowledge we feel that most other forces would suffer higher losses. However, using the North Wales figure of £52,000 and replicating this in the other 43 forces in England and Wales, as well as Police Service of Northern Ireland and Police Scotland, this would generate £2, 236,000 in terms of loss prior to our actions. However, it is a reasonable expectation the loss would be much higher, especially in more urban locations where the availability of targets is much more numerous, potentially equating to the £15.4 million in increased fraud potential through the monitoring provided by the banking protocol.

We feel that the project has made a significant impact on the ever-increasing amount of online fraud, facilitated by electronic banking. The project has been shared with "what works" college of policing platform and as a UK Tilley Award finalist is available to other forces. We see the approach as eminently transferable to anywhere in the world that suffers similar patterns of fraud, as well as through sharing the methodology used to tackle this type of large-scale retail fraud.

Word Count: 3925

3. Agency and Officer Information

Key Project Team Members

Police Inspector 739 Rob Rands
Llangefni Police Station
Industrial Estate Road
Llangefni
Anglesey
North Wales
LL77 7JA
+44 1492 805001
Robert.Rands@northwales.police.uk

Police Constable 3487 Annie Halstead
Llangefni Police Station
Industrial Estate Road
Llangefni
Anglesey
North Wales
LL77 7JA
Annie.Halstead@northwales.police.uk

Project Contact Person

Police Inspector 739 Rob Rands
Llangefni Police Station
Industrial Estate Road
Llangefni
Anglesey
North Wales
LL77 7JA
+44 1492 805001
Robert.Rands@northwales.police.uk

4. Appendices

Data tables regards UK fraud losses (UK Finance, Annual Fraud report 2022)

Fraud Type (£m)	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	% Change 20/21
Remote Purchase (CNP)	£247.3	£301.0	£331.5	£398.4	£432.3	£408.4	£506.4	£470.2	£452.6	£412.5	-9%
Of which e-commerce	£139.6	£140.2	£190.1	£219.1	£261.5	£310.3	£310.4	£360.5	£377.2	£339.2	-10%
Counterfeit	£42.3	£43.3	£47.8	£45.7	£36.9	£24.2	£16.3	£12.8	£8.7	£4.7	-46%
Lost & Stolen	£55.4	£58.9	£59.7	£74.1	£96.3	£92.9	£95.1	£94.8	£78.9	£77.2	-2%
Card ID Theft	£32.6	£36.7	£30.0	£38.2	£40.0	£29.8	£47.3	£37.7	£29.7	£26.3	-12%
Card non-receipt	£12.8	£10.4	£10.1	£11.7	£12.5	£10.2	£6.3	£5.2	£4.4	£3.9	-11%
Total	£390.4	£450.2	£479.0	£568.1	£618.1	£565.4	£671.4	£620.6	£574.2	£524.4	-7%
UK	£288.4	£328.2	£328.7	£379.7	£417.9	£407.5	£496.6	£449.9	£414.5	£384	-7%
Fraud Abroad	£102.0	£122.0	£150.3	£188.4	£200.1	£158.0	£174.8	£170.7	£159.7	£140.5	-12%

Table 1 - Debit, Credit, and other payment card fraud volumes in UK and abroad, 2012 -2021

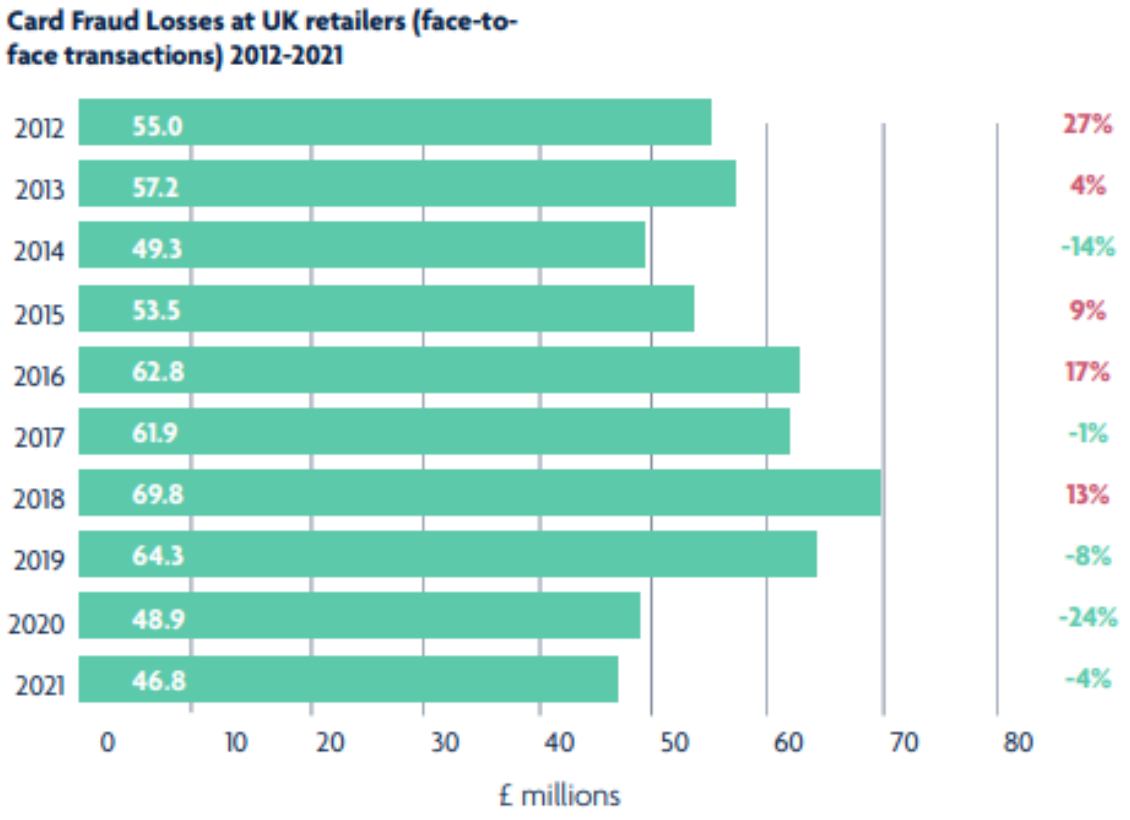

Table 2 – Face to Face, card fraud losses at UK retailers (face-to-face transactions) 2012-2021