

# Preventing fraud for businesses by securing card processing machines (PDQs)

Working with businesses to put preventative measures in place to reduce card processing machine fraud.

First published

26 February 2024

## Key details

<b>Does it work?</b>	Promising
<b>Focus</b>	Prevention
<b>Topic</b>	Crime prevention Intelligence and investigation Vulnerability and safeguarding Digital
<b>Organisation</b>	<a href="#">North Wales Police</a>
<b>Contact</b>	Rob Rands
<b>Email address</b>	<a href="mailto:robert.rands@northwales.police.uk">robert.rands@northwales.police.uk</a>
<b>Region</b>	Wales
<b>Partners</b>	Police Business and commerce Private sector
<b>Stage of practice</b>	The practice is implemented.

## Key details

<b>Scale of initiative</b>	Local
<b>Target group</b>	Communities General public Offenders Victims

## Aim

This initiative addresses the vulnerability of card processing machines (PDQs). In particular, it aims to:

- provide crime prevention education by ensuring potential victims are aware of the vulnerability linked to these machines
- reduce opportunity for fraud through a rolling programme that replaces default PINs with unique pins
- take away the offender's ability to identify vulnerable property
- increase the risk of offenders being caught by providing a method to help operators to identify this fraud

This project won a Tilley Award in 2022 for the Police Now and student officers' category.

## Intended outcome

The intended outcome of the initiative is:

- a reduction of future victims of fraud relating to card processing machines
- an increased identification of fraud relating to card processing machines
- a reduction in fraud relating to card processing machines

## Description

An investigation into a theft at a hotel led to the discovery of a weakness in card processing machines (PDQs). Offenders were accessing PDQ devices and issuing high-value refunds. The investigation found that businesses were primarily targeted at night.

Organised crime groups were exploiting the weakness to defraud businesses out of large sums of money. Groups travelled long distances to commit offences as the rewards were large and the risks were low. In North Wales, clusters of offences were committed within a short timescale. Offences were often unreported, suggesting that this could be a big problem throughout the UK.

North Wales Police looked at the factors and combination of conditions of the problem. They examined the features and relationships between the offender, location and victim to inform their response. This examination revealed:

- victims tended to be independent, family run hotels (but any business that accepted card payments could be vulnerable to this crime)
- businesses tended to be targeted at night when staffing levels were lower
- offenders tended to be transient, use hire/ lease vehicles, and were largely known to the police
- offenders tended to travel great distances to commit the crime suggesting their targets are not random or due to chance

By breaking down the problem in this way, it allowed North Wales police to see a national vulnerability with PDQ PINs. This could be exploited by a motivated group of offenders taking advantage of victim's inability to protect their businesses to steal large sums of money.

## Response

North Wales Police took a multi-faceted approach to the response. Locally, this involved investigation into the reported thefts. The force engaged with local partners to inform and educate businesses of the dangers and the steps required to protect themselves. This was done via the [Pub Watch scheme](#). Additionally, offenders were restricted through their bail conditions.

The force also engaged the support of a super controller to open channels of communication with the banking industry and the City of London Police. The super controller was the Deputy Chief Constable who spoke with National Police Chiefs' Council leads (their super controllers) for business crime, banking crime and fraud to secure their support and provide points of contact.

Multiple changes were made to prevent vulnerability, provide better security, and increase the risk of being caught. This involved:

- a working group of North Wales Police, UK Finance, City of London and Barclaycard providing advice to businesses to limit the number of staff who knew the password
- keeping PDQ machines out of reach, for example locked away in an office
- advising businesses to link the PDQ machine to the business computer system to provide additional security
- extending guardianship, including educating staff on recognising when they are potentially being targeted
- encouraging premises and area management to set their own additional pins

In the short term, the COVID-19 lockdown worked to the project's advantage as many businesses were forced to close, denying the offenders the opportunity to commit the offences. The force used this time to work with the banking industry to provide sustainable solutions to prevent this crime from occurring in the future.

These solutions included:

- any new or replaced PDQ machines would be assigned an individual pin (sent separately to the business)
- the setting of refund limits so businesses are alerted of unusual activity for example, a café dealing in small transactions of £5-£20, a refund request for £5000 should trigger an alert

## Overall impact

Many businesses accepted this crime as part of operation losses, or feared their business would be seen as vulnerable by reporting it. This means that previous crime data was not a true reflection of the scale of the problem. Therefore, it is hard to know the national effects of this initiative.

In 2022 North Wales Police surveyed 24 independent hotels that were situated on Anglesey to investigate whether the initiative had been effective. This survey revealed:

- all hotels except one location had set a unique pin following receiving guidance and advice
- 50% of hotels 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 house, with re-sited CCTV as an additional security measure

Overall, this survey provided reassurance that the advice has been followed and the vulnerability would be harder to exploit.

Within North Wales Police force there have been no further crimes of this type reported. Additionally, surveying similar premises on Anglesey revealed a greater degree of awareness.

## Learning

Asking businesses to limit the number of staff who knew the password posed problems to businesses who operate on a rota. It also has the potential to place increased demand on shift or service managers.

North Wales Police are unable to say their work is solely responsible for the reduction in demand caused by the problem since March 2020 as the national lockdown is likely to have played a role in this reduction. However, the lockdown provided time for the force to reflect on the problem and implement further strategies to prevent it.

## Copyright

The copyright in this shared practice example is not owned or managed by the College of Policing and is therefore not available for re-use under the terms of the Non-Commercial College Licence. You will need to seek permission from the copyright owner to reproduce their works.

## Legal disclaimer

Disclaimer: The views, information or opinions expressed in this shared practice example are the author's own and do not necessarily reflect the official policy or views of the College of Policing or the organisations involved.

## Tags

Crime reduction   Neighbourhood policing   Knowledge sharing