



Date XX April 2018

Michael Lane  
Police and Crime Commissioner for  
Hampshire  
(by email)

*Elizabeth II Court, The Castle  
Winchester, SO23 8UJ*

Telephone: 01962 846693

Fax: 01962 867273

E-mail: [members.services@hants.gov.uk](mailto:members.services@hants.gov.uk)

<http://www3.hants.gov.uk/hampshire-pcp>

Dear Mr Lane,

### **Hampshire Police and Crime Panel's Proactive Scrutiny of Cyber Crime**

At the 26 January meeting, Members of the Hampshire Police and Crime Panel reviewed the evidence received from yourself and other organisations in relation to cyber crime within the Hampshire policing area.

This review aimed to scrutinise and support you in your role as Police and Crime Commissioner (PCC) in your intention to keep the residents and communities of Hampshire and the Isle of Wight safer, through preventing cyber fraud. This scrutiny considered how well you have worked with partners to identify and prevent these crimes, and reviewed how effectively you have held the Chief Constable to account for ensuring that operational policing plans are reflective of the strategic priority placed upon tackling cyber fraud. Further this scrutiny looked at how the residents Hampshire and the Isle of Wight have been educated and informed to recognise and protect themselves from cyber-enabled fraud.

The review looked at the following key questions:

- How well has the PCC, through holding the Chief Constable to account, ensured that operational policing plans are sufficiently robust to meet the strategic threat posed by cyber-enabled fraud?
- How effective have the PCC and his office been in engaging with appropriate partners to ensure a joined-up approach to identifying and tackling cyber-enabled fraud?
- What efforts have been made by the PCC to educate and inform the residents of Hampshire and the Isle of Wight to recognise and protect themselves from cyber-enabled fraud?
- What are the key priorities which need to be considered by the PCC to reduce the threat posed to the residents of Hampshire and the Isle of Wight through cyber-enabled fraud?

- What best practice exists which could also be considered by the PCC in his approach to preventing and tackling cyber-enabled fraud?

Following a review of the evidence received, the Panel have outlined their findings below for your consideration.

### *Findings*

Through this evidence it was noted that:

- Cybercrime activity is growing and evolving at a fast pace, becoming both more aggressive and more technically proficient. As a result organisations seeking to prevent cyber fraud needed to evolve rapidly to keep up with those looking to cause harm.
- Recognising this, Hampshire Constabulary was one of the first forces to implement digital strategies at force level and was in the process of creating a Digital Investigation Team (DIT), to be operational during the first quarter of 2018. Whilst recognised as an expensive resource, in terms of regular training and access to the latest technology, it was considered an essential component of the Constabulary's approach to tackling cyber crime.
- Hampshire were also the first Force in South East region to have a 24/7 Digital Medium Investigators (DMIs) response, to provide tactical advice if responding to a major investigation.
- It was understood, that with the growing shift away from traditional crime types, that cybercrimes would, in the future, need to be mainstreamed within the Constabulary and that the Chief Constable faced a significant challenge, along with forces across the country, to equip Hampshire Constabulary to meet the changing criminal landscape.
- Current figures suggest that approximately 1000 reports are made each month within Hampshire and the Isle of Wight (IOW) by victims of fraud. Of this 39% were made by individuals and the remainder being reported by businesses and organisations. It was recognised that a significant proportion of this defrauding had occurred online, and that cyber fraud was an area that was considerably under reported and therefore the true figures were likely to be much higher.
- Compared with national figures, Hampshire and the IOW had seen a higher than average take up for victim support, with the greatest area of uptake being in relation to online shopping fraud. It was heard that the OPCC were working alongside Hampshire and IOW Neighbourhood Watch (NHW) to identify opportunities to further encourage uptake of the support available by victims.

Whilst it is recognised that general cyber awareness is improving across the UK, a lack of understanding and recognition of cyber fraud still exists. Members of the Panel noted that evidence received has strongly suggested a need for greater

engagement by the PCC with both residents and partner organisations, in raising awareness of the profile of cyber fraud and sharing prevention messages:

- A number of town and parish councils responded to the Panel's request for information, stating that they felt unable to provide a response due to lack of engagement from the PCC around cyber fraud. Those who provided a response also highlighted this as a concern. Many town and parish councils, who responded to the Panel's request for information, further suggested that they would be happy to disseminate information from the PCC within their local communities.
- AgeUK IOW also stated that they don't receive any communication from local police regarding cyber crimes and have identified an opportunity for the PCC to work with them through their Digital Inclusion Project. Doing so would enable key messages from the PCC and Constabulary to be relayed to vulnerable older residents across the island.
- A number of those responding to the review highlighted that they had not seen any evidence of the PCC communicating directly with residents around the topics of online safety and cyber fraud.
- It has been suggested that improvements could be made to the PCC's website, in particular through incorporating links to other service providers who can provide additional support. It was also suggested that cyber crime should feature more prominently within the Constabulary's homepage.

The Panel were, however, also provided with a number of examples demonstrating how the PCC and his office are working with and supporting partners to prevent cyber fraud, as well as seeking to enhance engagement with residents:

- The OPCC are jointly working with Hampshire Constabulary and Hampshire and Isle of Wight Neighbourhood Watch (NHW) to support the public launch of Operation Signature in April 2018. Hampshire is one of six forces who have adopted the scheme, initially developed by Sussex Police, which aims to identify and support vulnerable victims of fraud across the two counties.
- The OPCC are a partner in the Safer Hampshire Business Partnership, led by the Constabulary, which focusses upon encouraging and enabling businesses to protect themselves from crime, including cyber fraud.
- Isle of Wight Council Trading Standards received funding from the OPCC, to support the establishment of the Isle of Wight Against Scams Partnership (IWASP). This partnership brings together Police, Fire, Citizens Advice Bureau and other organisations to provide prevention advice, encourage the reporting of concerns and help victims' access appropriate support.
- Southampton City Council stated the OPCC have worked closely with the Safe City Partnership to prevent online sexual exploitation. In particular they highlighted that Hampshire Constabulary's Sextortion awareness campaign had been viewed by at least 238,000 people online and their related radio advert was listened to by over 27,000 people. They have also highlighted their

strong relationship with Hampshire Constabulary, particularly in safeguarding supporting victims of financial abuse.

- Hampshire and Isle of Wight NHW had raised concern within their initial evidence over lack of engagement from the PCC, however through oral evidence it was heard that this had significantly improved since November 2017 and that engagement between the organisations had been very active since this time.
- The OPCC provided examples demonstrating how they have sought to increase engagement with residents around the topics of fraud and cyber safety through attendance at older driver awareness events, visiting secondary schools and early years settings. They also highlighted that, in collaboration with Hampshire Constabulary, they would be holding their first cyber protect and young persons conference in January 2018.

Further, the evidence suggested the following should be considered within the PCC's priorities:

- Romance fraud is a growing area of concern, with dating and sexting both being used as methods of exploitation. One example was given in which an individual was defrauded of £130,000 as a result of a romance fraud.
- Other areas of increasing concern were mandate fraud, which had been targeted towards both individuals and business within Hampshire and the IOW, and crypto currency fraud.
- The profile of those vulnerable to cyber fraud is wide, with nobody immune from being targeted. Therefore communications on cyber safety should be targeted to the widest possible audience, be available through online and offline media sources and give consideration to keeping both individuals and businesses safer. Hampshire Constabulary highlighted, within their evidence, that they were undertaking enhanced engagement with small to medium sized businesses to share advice on how to better protect themselves and how to manage a fraudulent incident should one occur.
- The sharing of best practice between partners and enhancing education of the public in relation to cyber fraud were both considered to be vital, as it was recognised most cyber fraud offences were preventable if businesses and residents are well informed on spotting the signs of potentially fraudulent activity.

## *Recommendations*

In reviewing the evidence received, Members brought forth a number of recommendations, which they wish to raise for your consideration:

- a. The PCC and his office should seek to enhance their engagement with the residents of Hampshire and the IOW in relation to cyber safety and cyber fraud. Consideration should be given to how messages can be targeted to reach the widest possible audience, with a focus on educating the public and local businesses upon how to keep themselves safe from the risk of cyber fraud and encourage the reporting of fraudulent activity.
- b. Further the PCC and his office should also consider how they might better engage with Town and Parish Councils, to raise the PCC's profile in relation to cyber fraud. Consideration should be given to whether Town and Parish Councils might be willing to support the PCC in his intention to keep communities safer through the dissemination of information within local communities. The evidence would suggest that sharing information in this way may better enable the PCC to access those residents harder to reach through other mediums, and who may therefore be particularly vulnerable to cyber fraud.
- c. In his role to support and empower partners, the PCC should continue to encourage and facilitate the sharing of best practice between partners. Through greater sharing of information the PCC should encourage partners to deliver consistent messages Hampshire and IOW wide regarding the approach to tackling cyber fraud and urge members of the public to come forward to report concerns.
- d. Through his responsibility to hold the Chief Constable to account, the PCC should regularly review the force's strategic provision for cyber fraud, and assure himself that the Chief Constable's strategic direction will enable Hampshire Constabulary to meet future demand in tackling cyber fraud.
- e. The PCC and his office should review the information currently available within the Commissioner's website for those seeking advice and guidance in relation to staying safer online and/or reporting concerns. This review should also consult Hampshire Constabulary upon the relevance of the information contained within their webpages and consider whether sufficient links are available to enable self referral to partner organisations.
- f. That the results of the PCC's cyber survey should be shared with the PCP, in due course, highlighting how the PCC intends to incorporate the findings within the strategic priorities of his Police and Crime Plan.

We look forward to receiving, in due course, your response to the recommendations outlined above, including consideration as to how the recommendations made will be incorporated into related activities within your Delivery Plan.

Yours Sincerely,

A handwritten signature in black ink, appearing to read 'David Stewart', with a stylized flourish at the end.

**Councillor David Stewart**  
**Chair, Hampshire Police and Crime Panel**

DRAFT