Opening Statement by Niamh Davenport, Head of Financial Crime, Banking & Payments Federation Ireland at the Joint Committee on Finance, Public Expenditure and Reform, and Taoiseach

Good afternoon Chairman, Committee members. I am joined today by Richard Walsh, BPFI's Director of Industry Collaboration & Innovation. We welcome the opportunity to appear before you.

In recent years, the fraud landscape in Ireland has evolved significantly. Fraud previously consisted of criminals hacking into bank systems, online scams and even some in-person attempts. Nowadays, fraudsters have found that it is easier to manipulate customers into making transfers rather than trying to impersonate them directly. This type of fraud is known as authorised push payment fraud or APP fraud and is what we are here to discuss today.

In an authorised push payment scam, a criminal will trick the consumer or business into sending money directly from their account to an account which the criminal controls. In most cases the customer fully believes they are making a legitimate payment, even at times when it has been flagged to them by their banking provider that it is high risk. Examples include investment scams such as fake cryptocurrency schemes, romance scams, accommodation scams and for business customers invoice redirection and CEO impersonation scams.

Financial institutions have a clear role to play in preventing fraud, a commitment which the industry takes very seriously through a range of measures both at industry level and within each individual institution. However, it is important to note the first sight a financial provider will have of an authorised push payment fraud is when a transaction has already taken place. The payment occurs at the end of what can often be a long engagement between the criminal and the victim. Therefore, the banks cannot combat this crime alone.

APP fraud losses are driven by the fraudsters abusing online platforms to scam victims. This can include investment scams advertised on search engines and social media, romance scams committed via online dating platforms, and purchase scams promoted through auction websites. Once the victim has authorised the payment and the money has reached the criminal's account, the criminal will quickly transfer the money onwards to numerous other accounts, often abroad, where it is then cashed out.

We know that in the UK almost 80% of these types of scams originate through online advertisements. Critical therefore to tackling and ultimately reducing losses and the impact on consumers, is a greater understanding of where and how these frauds and scams originate and blocking these channels to criminals.

Simply focusing on the payment and reimbursement of payments will fail to reverse the increasing incidents of fraud, will fail to protect consumers and businesses, and will only reward criminals and enable them to fund more serious and lucrative crime. As An Garda Síochána will verify, money stolen through APP scams is used to fund drug trafficking, human trafficking, sexual exploitation and terrorism.

To effectively combat APP fraud Ireland needs a centrally led, 'whole of system' response where social media companies, telecoms, financial services, the State and An Garda Síochána can collaborate to

devise appropriate strategies to better share intelligence, implement protections for consumers and develop barriers to criminals.

Close, cross-sectoral collaboration on intelligence sharing would be a significant game changer in fraud prevention in Ireland. There is currently a very siloed approach between the various industry sectors and agencies in identifying and combating financial crime. Our European and UK colleagues have benefited from national collaboration projects, in particular Shared Fraud Databases, as a key resource in effectively combatting fraud - the UK database, for example, has been operational for over 30 years.

This sentiment was also echoed in the Hamilton Report published by the Department of Justice in December 2020, which encourages greater inter-agency co-ordination, collaboration, and information sharing, and also recommends a clear cross-government financial crime strategy. As the report Summary of Recommendations note:

"Ireland has at present, no national strategy for combating economic crime and corruption. Given the range of agencies involved, the Review Group recommends the development of a multi-annual strategy to combat economic crime and corruption and an accompanying action plan. This will facilitate a joined-up and cohesive approach to combating economic crime and corruption in this jurisdiction and provide a basis for measuring progress."

This collaborative approach is not happening in any significant way in Ireland. Financial institutions have had some good successes in combatting the wave of fraudulent SMS text messages which impersonate genuine bank messages, but to keep pace with the changing landscape we believe a national strategy should be built on three pillars of defence - Cross Sector Collaboration, Education and Awareness, and Information Sharing – pillars on which we have built own industry strategy.

1. **Cross Sector Collaboration:**

- To effectively combat fraud, it is crucial to address the source, and prevent scams from reaching consumers in the first place. Cross sector collaboration will us to target the channels currently used by criminals to contact victims and disrupt fraud at the source.
- BPFI is participating in a ComReg led project to reduce spoof callers, the project has successfully blocked almost 10 million phishing calls since September 2022.
- BPFI coordinates the bimonthly Joint Intelligence Group which brings together financial institutions and An Garda Síochána and which facilitates the sharing of fraud trends and typologies.
- BPFI has worked closely with An Garda Síochána on the Banking Protocol project which trains bank branch staff to identify and assist customers who present at a bank and who may be under coercion or under the influence of a fraudster
- Further cross collaboration work is needed with internet providers and social media companies. They have a significant role to play in blocking fraudulent websites, monitoring network traffic and taking down fake advertisements.
- Collaboration creates a united front against fraud and by leveraging the expertise and resources from across all stakeholders it becomes possible to disrupt the fraud ecosystem and protect consumers from falling victim to scams.

2. **Education and Awareness:**

- In 2017, BPFI launched our FraudSMART programme, which was developed in conjunction with our members, and which aims to raise consumer and business awareness of the latest financial fraud activity and trends and provide simple and impartial advice on how best they can protect themselves and their resources from fraud.
- FraudSMART regularly raises awareness about the authorised push payment fraud scams we are discussing here today among many others. Through a variety of channels including national media, social media, radio advertising, email alerts and in person events, the programme provides information on the tactics fraudsters use and highlights key warning signs and red flags to help consumers become more vigilant and protect themselves from fraud. Over the last six months for example we have focused on raising awareness on investment scams, online scams and invoice redirection and have partnered with Age Friendly Ireland and the Small Firms Association as part of this work.
- Ultimately empowering consumers and businesses through education helps to close the gap that fraudsters exploit when manipulating customers and this is what our FraudSMART programme sets out to achieve.

3. Information Sharing (Shared Fraud Database):

- Shared fraud database schemes seen across Europe and the UK, which support the sharing of information across financial institutions and law enforcement, are critical in the fight against financial crime. Enabling collaboration and sharing of information about known fraudsters, fraud schemes and emerging trends allows the industry to act in real time and prevent the fraud from taking place. The benefit of a shared fraud database extends beyond prevention. It assists law enforcement to investigate and prosecute more effectively. It also protects customers who believe their identities may have been compromised.
- By pooling resources and information through a shared fraud database, banks and law enforcement can enhance fraud prevention efforts and endeavour to stay ahead of evolving fraud techniques.
- BPFI has worked with members to develop an industry shared fraud database which is ready to stand up once legislative amendments currently with the Department of Justice are approved.

Conclusion

The three pillars of Collaboration, Education and Information Sharing provide a solid foundation on which to further build a fraud prevention ecosystem in Ireland. However more work is required and with potential regulation changes making a significant difference and the development of a National Economic Crime Strategy, which brings key stakeholder together, we can ensure that Ireland is not a prospective destination for fraudsters.

BPFI and its members will continue to seek insights and best practices from other jurisdictions along with our own initiatives to prevent fraud. Adopting and improving upon successful strategies employed elsewhere can contribute to the development of a robust anti-fraud framework in Ireland.

The key difference we note with other jurisdictions is their level of intelligence sharing, cross-sector collaboration, and national strategies. By working together, it becomes possible to gather and share intelligence, identify patterns, and proactively address emerging fraud trends.

However, we must look at other jurisdictions as a whole, rather than adopting individual pieces of their fraud strategies in isolation. Each jurisdiction has its unique fraud landscape and challenges. By

examining their fraud ecosystem comprehensively, including the regulatory framework, technology infrastructure, industry collaboration, and consumer education initiatives, it becomes possible to understand the holistic approach they have taken to combat fraud. By studying successful fraud prevention models, we can gain insights into the most effective strategies for identification and for prosecution.

Thank you.