Bringing Ingenuity to Life.
paconsulting.com

Tackling the rising incidence of financial sexual extortion

Takeaways from a cross-sector innovation forum

Foreword

As evidenced in the 2023 Global Threat Assessment of child sexual exploitation and abuse online, the volume of child sexual abuse material detected has increased by 87% from 2019. One concerning trend contributing to the sustained increase in the incidence of child sexual exploitation online is an explosion in Financial Sexual Extortion (FSE), with the number of reports of this crime having increased by 7200% between 2021 and 2022.

The impact and trauma experienced by victims of FSE cannot be overstated. Due to the intense shame felt by victims, we have seen a continued rise in suicide rates in young male victims (~91% of sextortion reports are male victims, and ~60% are 16-17 years old). In the six-month period from October 2022 to March 2023, the FBI and US Homeland Security Investigations received over 13,000 reports of financial sexual extortion of children online. The sexual extortion involved at least 12,600 victims and led to at least 20 suicides. Since running the cross-sector innovation event, we have seen reports of another very unfortunate case, where the father of Dinal De Alwis is warning others on the social media dangers after an inquest heard how the 16-year-old teenager killed himself after being asked to pay £100 in return for embarrassing nude images on Snapchat.

The cross-sector innovation forum took place in January 2024 and convened experts from across the child sexual exploitation and fraud eco-systems, who work tirelessly to prevent these pervasive harms, to discuss current and future opportunities for stimulating cross-system collaboration to tackle and prevent the alarming and growing trend of FSE.

The forum had three goals;

1. Help to raise awareness of the alarming growth of FSE and the devastating impact it causes
2. Understand what is currently being done to combat the threat, and what the challenges are
3. Discuss what needs to happen to combat this growing crime.

It is recognised that similar forums are also looking at this threat area. For example, the Tech Coalition held its Second Biennial Multi-Stakeholder Forum in June 2023 which focused on 'Combating Online Financial Sextortion of Children', and the UK Safer Internet Centre, who have run roundtables on this topic.

This report intends to contribute towards the effort of these forums by summarising the rich debate of the cross-sector innovation forum on what more can be done at a whole-system level to prevent FSE.

Two important caveats to the discussions captured in this report summary. Firstly, it is recognised that there may already be solutions in place or in development that address some of the discussion points raised during the event, Secondly, no market assessment has been undertaken on the effectiveness of any potential solutions raised.

At PA we believe in the power of ingenuity to build a positive human future. As strategies, technologies, and innovation collide, we create opportunity from complexity. Whilst FSE is a relatively simple crime to commit, it is complex in its nature to identify, disrupt, and investigate (spanning both fraud and child sexual abuse and exploitation online), which will require a whole-of-society approach to prevent. Governments, regulators, law enforcement, third sector and charities, the technology sector, educators, parents, and carers all have an important part to play in proactively preventing the crime by building a greater understanding of the harm and applying solutions that can help with early intervention, helping to shift the emphasis from cure to prevention.

We welcome the opportunity to continue collaborating with those wishing to help prevent FSE and all forms of online harms.

Patrick Cronin
Vulnerabilities & Online Safety Lead
Partner at PA Consulting

Contents

Introduction

The fight against financial sexual extortion requires collaboration, technological awareness, legislative support, adaptive strategies, and a comprehensive understanding of the challenges faced to protect victims and prevent harm.

On 31 January 2024 CEOs from social media giants Meta (the parent company of Facebook and Instagram), X, Snapchat, Discord, and TikTok faced a US Senate Committee hearing where they were questioned over their platforms' efforts to protect young people from online abuse, including sexual exploitation. As the CEOs testified in front of the US Senate, PA Consulting (PA) held a cross-sector innovation forum co-facilitated with Plexal to explore some of the challenges and opportunities for tackling and preventing the alarming, growing abuse trend of financially motivated sexual extortion.

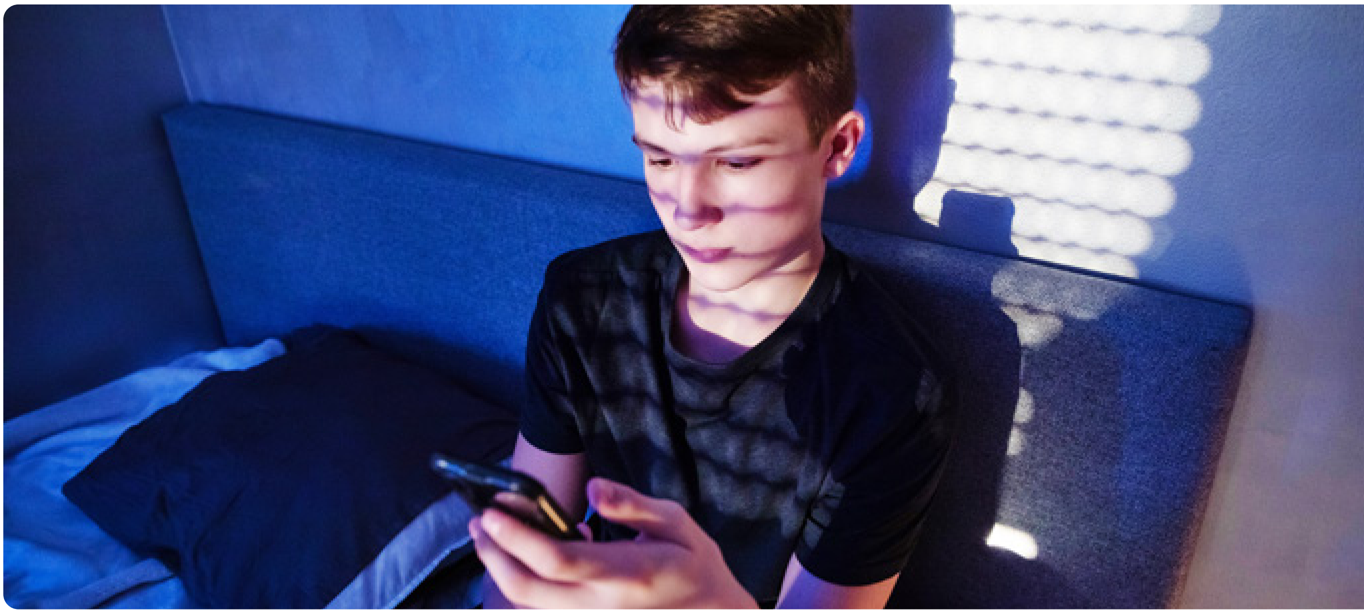
The forum included opening addresses from sector experts Iain Drennan (WeProtect Global Alliance), Simon Bailey (representing Child Rescue Coalition), Ian Critchley QPM (National Police Chiefs' Council), Julie Dawson (Yoti), and Saj Huq (Plexal), who set out the challenges faced in today's digital age, and observations on the current response to FSE.

Attendees then took part in facilitated workshops to explore a typical 'victim-perpetrator pathway', and an open group discussion to consider challenges and opportunities for early intervention.

The workshop discussions focussed primarily around three areas for intervention, within which specific challenges and opportunities were identified:

1. PREVENT – how to *prevent* people from engaging in FSE (stopping the problem at source)
2. PROTECT – how to *protect* individuals from FSE (building high levels of defence and resilience)
3. PURSUE – how to *pursue* offenders through prosecution and disruption (relentless disruption and targeted action)

The group discussion emphasised the shift required from cure to prevention, and how the ecosystem can maximise the use of innovation from small and medium-sized enterprises (SMEs).



Financial sexual extortion and coercion of children

Statistics from the National Centre for Missing and Exploited Children (NCMEC) point to an 87% volume increase in child sexual abuse material since 2019. A significant increase in new tactics by perpetrators, including through FSE, are a large part of this growth. This category of harm bridges crime types and techniques, and therefore requires a collective, cross-threat whole-system response to reduce the disastrous impact on vulnerable children.

Reported cases of the coercion, extortion, or blackmail of a child by technological means, and using sexual images and/or videos depicting that child for the purposes of financial gain, have increased dramatically in the past year. In 2022, NCMEC received over 10,000 reports of financial sexual extortion of a child (compared to 139 reports in 2021), and the FBI issued a public safety alert about an 'explosion' of financial sexual extortion and coercion schemes targeting children and teens.

Children are particularly vulnerable; in a survey of over 1,500 victim-survivors, 46% were children. Financially motivated sexual extortion and coercion is highly traumatic for victims and has led to tens of children taking their own lives.

These criminals deceive and extort children into producing and sharing 'self-generated' sexual content for monetary gain. Many extorters pose as young girls online and predominantly approach boys aged between 15-17 years via social media, proposing the exchange of sexually explicit imagery. Internet Watch Foundation (IWF) data also suggests that boys are more likely to be targeted, although the organisation cautions that they have identified female victim-survivors too. The Canadian Centre for Child Protection (C3P) analysis of 6,500+ public posts by sexual extortion victim-survivors in 2022 revealed many extorters use similar strategies. Once sexually explicit imagery is sent, the extorter threatens to send the imagery to the child's friends and family, blackmailing them for money. They make threats appear credible by sending screenshots of the child's social media contacts.

The landscape of sexual extortion has undergone a significant transformation

The landscape of sexual extortion has undergone a significant transformation in recent years. Historically, sexual gratification has been identified as the primary motive for sexual extortion. However, as seen with the rising cases of FSE over the last two years, there has been a significant emergence of financially motivated perpetrators committing this crime type.

Note: Financial incentives are still the minority motive in known cases of sexual extortion against children.

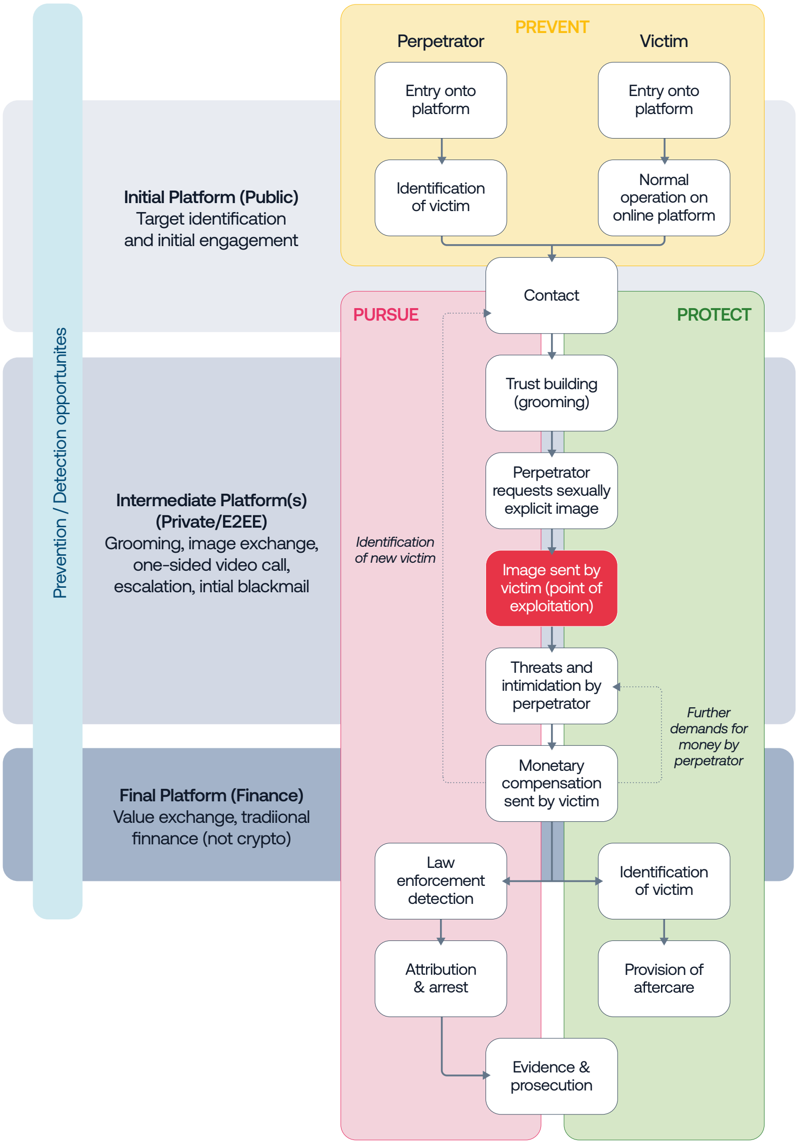
During the opening remarks from the expert panel, several key themes emerged regarding the rise in FSE:

- **Starting from the victim's perspective:** To combat FSE effectively, it is crucial to comprehend the victim's world and recognise FSE as a pervasive societal issue. Particularly concerning is the blurred line between online and real-world experiences, especially for children. The impact and trauma experienced by victims of FSE cannot be overstated. The unique challenges faced by those abused online are only now becoming clearer. Ensuring appropriate support and responses for victims and parents reporting incidents is essential.
- **Scale:** FSE operates on a massive scale and minimal participation is needed to sustain a successful criminal enterprise. As technology evolves, FSE is expected to become more intricate. Urgent efforts are required to catch up and address this growing issue comprehensively.
- **Prevention and Safety by Design:** There is a significant opportunity to safeguard children by embedding Safety by Design and age-appropriate design principles into the development of technologies, whether that be for social media platforms, gaming platforms, or other applications and services used by children. By exploring the creation of a robust safety ecosystem for online child safety and leveraging tangential technologies, emerging threats can be more effectively counted and prevented. Additionally, building victims' confidence to come forward to talk about their experience as well as normalising conversations around FSE, is paramount to prevention by de-stigmatising the experience of abuse and raising awareness and knowledge of the harm and how to keep safe online.
- **Cross-cutting environment and collaboration:** FSE transcends traditional boundaries (fraud and online child sexual exploitation and abuse), necessitating collaboration across various domains. Learning from subject matter experts in fraud prevention and other forms of extortion will ensure best practice solutions and approaches are adopted and implemented, rather than inventing the wheel or starting from scratch. Existing criminal entities don't operate in a static way as they are constantly evolving their revenue streams and are adept at adapting without needing to form new entities or formations. Collaboration between players already working within the ecosystem is therefore critical to identify opportunities for innovation, develop adaptable and agile technologies that respond to shifting threats, and rapidly scale up effective solutions to tackle the evolving threat posed by these criminal entities.
- **Technologies and tactics used by perpetrators:** The varied tactics and methods employed by perpetrators to conduct FSE pose a formidable challenge for law enforcement and investigators. The offense can occur within seconds, particularly in gaming contexts with brief average interaction times, and perpetrators are continuing to shift to encrypted platforms which complicates investigations. Technology facilitates blackmail tactics, often with little regard for the trauma inflicted on victims. Understanding the intricate intersection of technology and FSE is imperative. Perpetrators exploit emerging technologies such as deep fakes, emphasising the need for an AI lens to detect and prevent activities before their full unfolding.
- **Victim payment and material release:** Disturbingly, instances exist where victims comply with extortion demands, yet compromising material is still released. Harassment and abuse often escalate after this critical moment and has often led to tragic outcomes for victims, including suicide. This underscores the urgency to inform victims of the methods of perpetrators and in technology platforms intervening before any monetary funds are sent.
- **Learning from experts and a whole system approach:** There is an urgent need to view FSE as a whole system challenge. The connection with databases like the Child Abuse Image Database (CAID) and forensic technology is crucial for a comprehensive response.
- **Regulation:** Leveraging the UK's Online Safety Act is crucial to enhance platform safety, especially where abuse occurs.

Opportunities for intervention across the victim-perpetrator pathway

A typical victim-perpetrator pathway was used to help frame the workshop discussions, where groups stepped through each stage of the pathway, discussing both challenges and opportunities for intervention. This pathway was set in the context that many cases of FSE initially begin on a platform which is public (where a target is identified and there is initial engagement), and then progresses onto an intermediate private platform (where the threat escalates through grooming, image exchange, and initial blackmail), before moving onto the financial platform (where there is value exchange).

Whilst opportunities for intervention and possible solutions were identified during the discussion, it should be noted that there is a possibility that some of these may already be in use by an organisation. The intention is not to duplicate effort, but instead, ensure action is being taken across the ecosystem and to maximise opportunities for earlier upstream intervention.

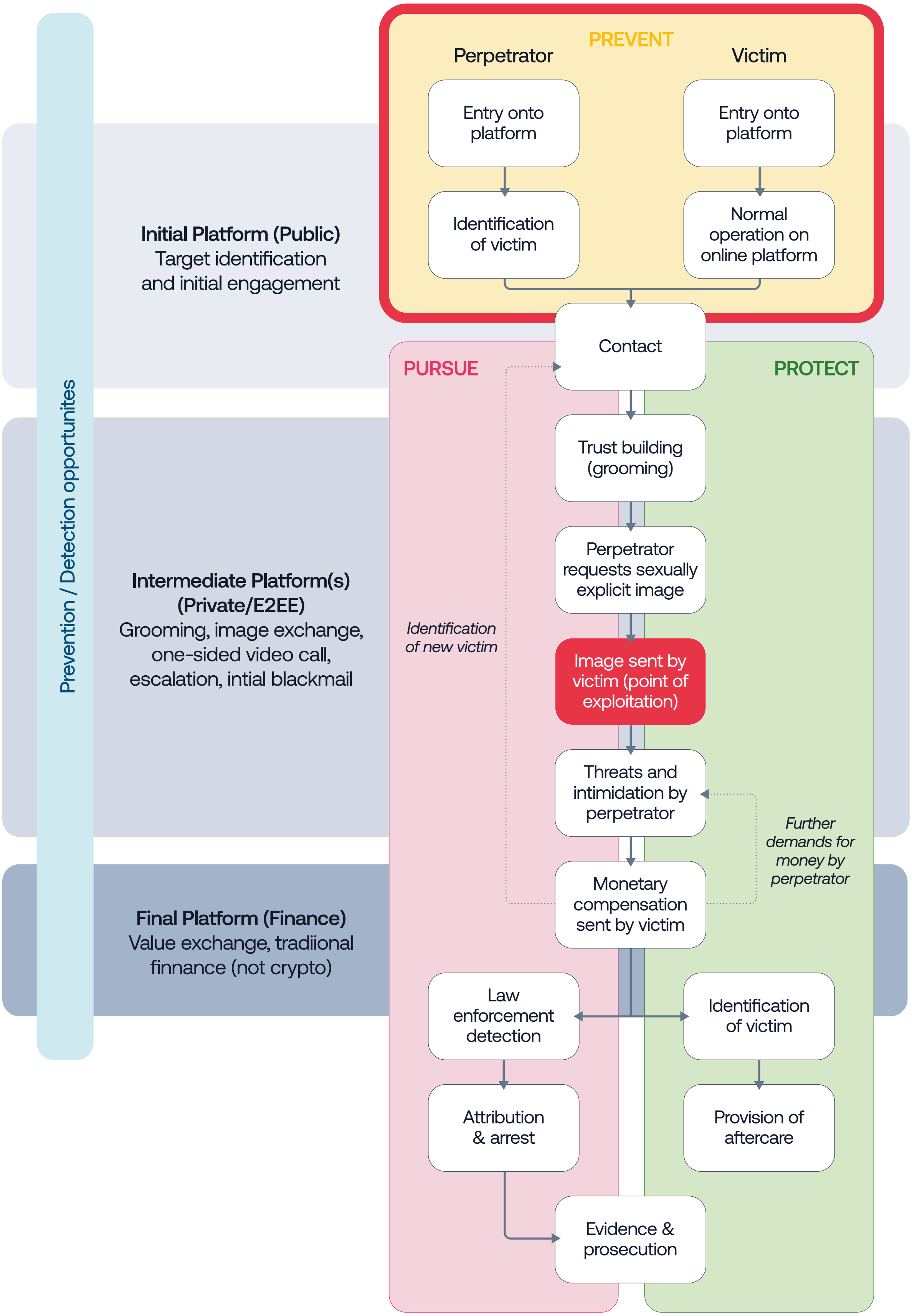

Prevention / Detection opportunites
PREVENT
Perpetrator
Victim
Entry onto platform
Entry onto platform
Identification of victim
Normal operation on online platform
Initial Platform (Public)
Target identification and initial engagement
Contact
PURSUE
PROTECT
Trust building (grooming)
Perpetrator requests sexually explicit image
Intermediate Platform(s) (Private/E2EE)
Grooming, image exchange, one-sided video call, escalation, intial blackmail
Identification of new victim
Image sent by victim (point of exploitation)
Threats and intimidation by perpetrator
Further demands for money by perpetrator
Monetary compensation sent by victim
Final Platform (Finance)
Value exchange, tradiional finnance (not crypto)
Law enforcement detection
Identification of victim
Attribution & arrest
Provision of aftercare
Evidence & prosecution

'Victim-perpetrator pathway' used to facilitate the syndicate workshops

1. PREVENT | Prevention is better than cure

There is unanimous agreement that intervening early to stop the problem at source is the best strategy to protect children.

The UK Home Office's Tackling Child Sexual Abuse Strategy 2021 sets out the Government's ambition to prevent, tackle and respond to all forms of child sexual abuse. The Strategy states the Government's goal of stopping the problem at source, identifying and supporting those at risk of engaging in criminality.



Prevention / Detection opportunites

Initial Platform (Public)
Target identification
and initial engagement

Intermediate Platform(s) (Private/E2EE)
Grooming, image exchange, one-sided video call, escalation, intial blackmail

Final Platform (Finance)
Value exchange, tradiional finnance (not crypto)

PREVENT

Perpetrator

Entry onto platform

Identification of victim

Victim

Entry onto platform

Normal operation on online platform

Contact

PURSUE

PROTECT

Trust building (grooming)

Perpetrator requests sexually explicit image

Image sent by victim (point of exploitation)

Threats and intimidation by perpetrator

Monetary compensation sent by victim

Identification of new victim

Further demands for money by perpetrator

Law enforcement detection

Attribution & arrest

Evidence & prosecution

Identification of victim

Provision of aftercare

Challenges identified that will need to be overcome:

Awareness with potential victims

- Increased peer pressure in society to share nude images, and it becoming 'the norm' for teenagers, without fully realising the potential risks
- Difficulty "getting through" to minors in their language and a tendency for a lack of trust in adults
- Education and awareness interventions happening too late in the pathway
- Limited public awareness, including awareness of parents and carers.

Ease of committing the offence

- Ability to easily identify a child's profile on the public platforms
- Anonymity of predators who typically work across multiple platforms, often moving victims into private (typically end-to-end encrypted) environments
- Increased abuse of AI which significantly impacts ease and scale (e.g. increased use of deep fakes negating the need for an actual image to be sent)
- Grooming can be effective even after a few minutes.

Complexity and existing approaches

- Issue is "full stack", involving both hardware and software/platforms
- Lack of visibility of existing interventions
- Lack of coordination between platforms and lack of detection mechanisms.

Possible solutions that should be explored:

Awareness

- Run a public safety awareness campaign highlighting the risks of the crime
- Run awareness conferences in and out of schools
- Increase traditional awareness raising (e.g. posters)
- Define peer ambassadors/evangelists and social media influencers to run campaigns for primary and secondary schools (e.g. like the IWF campaigns)
- Engage with children to raise awareness on what law enforcement can actually do to help
- Leverage targeted ad networks and marketing algorithms on social media to alert potential victims and target prevention activities and messaging to the demographic most affected/ vulnerable groups
- Utilise sports networks.

Barriers to entry/safeguards

- Strengthen verification checks on platforms (e.g. face match, user and age verification)
- Introduce watermarking to help identify AI generated content
- Block outbound nude image sharing on devices
- Increase on-device protection and embedded features
- Use AI through chatbots to send deterrent messages
- Introduce “safety essentials” before firms can provide services.

Intelligence picture

- Leverage known data, e.g. trend of predators targeting people with more information on social media profiles
- Leverage Regulation of Investigatory Powers Act (RIPA) 2000
- Understand what makes children look more vulnerable (e.g. from their public profiles)
- Use behaviour analysis to understand more about users
- Engage in psychological/behavioural work for young males.

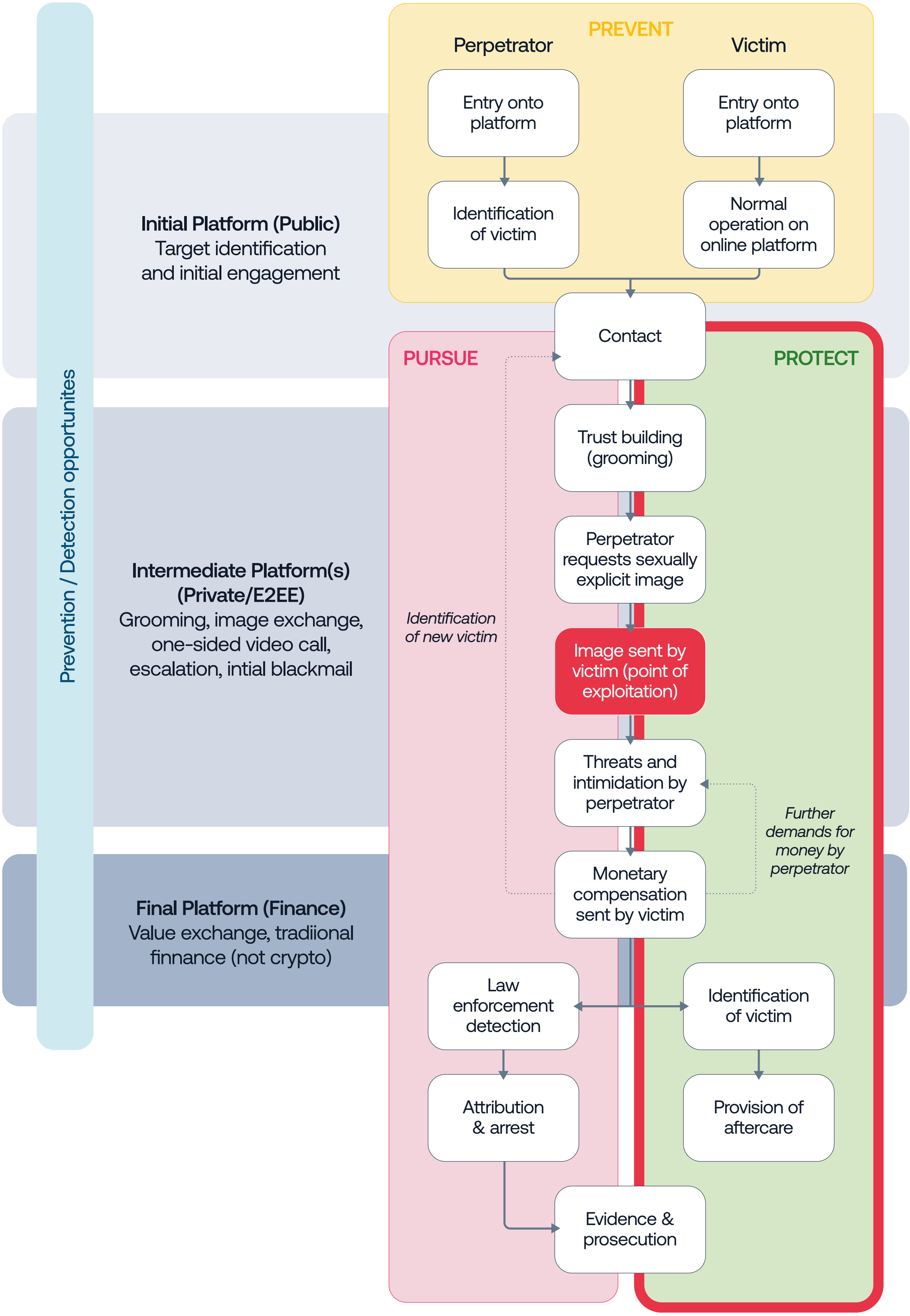
Collaboration across the ecosystem

- Leverage diplomatic networks with international partners to identify lessons learnt
- Increase data sharing across partners across the ecosystem (including platforms and government)
- Conduct horizon scanning and industry research to understand best practices and what good looks like for the industry
- Publish statistics of platforms involved to impact reputation and force action.

2. PROTECT | Protecting those most vulnerable

The emphasis should not be on children to protect themselves online, but instead focus on those who are better able to put in place the highest levels of defence and resilience to the threat.

A key component of protecting children from FSE is ensuring that the online platforms and communities where they spend their time are safe. Improve multi-agency working and cross-sector collaboration is needed to provide targeted support for those most at-risk to stop perpetrators from taking advantage of them.


Prevention / Detection opportunites
Initial Platform (Public)
Target identification
and initial engagement
Intermediate Platform(s)
(Private/E2EE)
Grooming, image exchange,
one-sided video call,
escalation, intial blackmail
Final Platform (Finance)
Value exchange, tradiional
finnance (not crypto)
PREVENT
Perpetrator
Victim
Entry onto platform
Identification of victim
Entry onto platform
Normal operation on online platform
Contact
PURSUE
PROTECT
Trust building (grooming)
Perpetrator requests sexually explicit image
Image sent by victim (point of exploitation)
Threats and intimidation by perpetrator
Monetary compensation sent by victim
Identification of new victim
Further demands for money by perpetrator
Law enforcement detection
Attribution & arrest
Evidence & prosecution
Identification of victim
Provision of aftercare

Challenges identified that will need to be overcome:

- Feeling of shame by affected children which disincentivises engagement
- Lack of reporting and understanding the true scale of the crime.

Possible solutions that should be explored:

Victim's approach

- Provide mental health support for victims
- Ensure long-term links with a victim's digital footprint
- Support victims' families as well as the victims (e.g. siblings)
- Signpost support for victims' parents
- Approach affected person as a victim, not a child
- Take away the element of shame from the victim
- Create a #MeToo moment.

Collaboration across the ecosystem

- Connect globally to leverage intelligence and data across the ecosystem
- Act on learnings quickly
- Collaborate cross-sector, cross-policing, and cross-government and join up across platforms
- Work with global finance providers regarding access and signals on platforms.

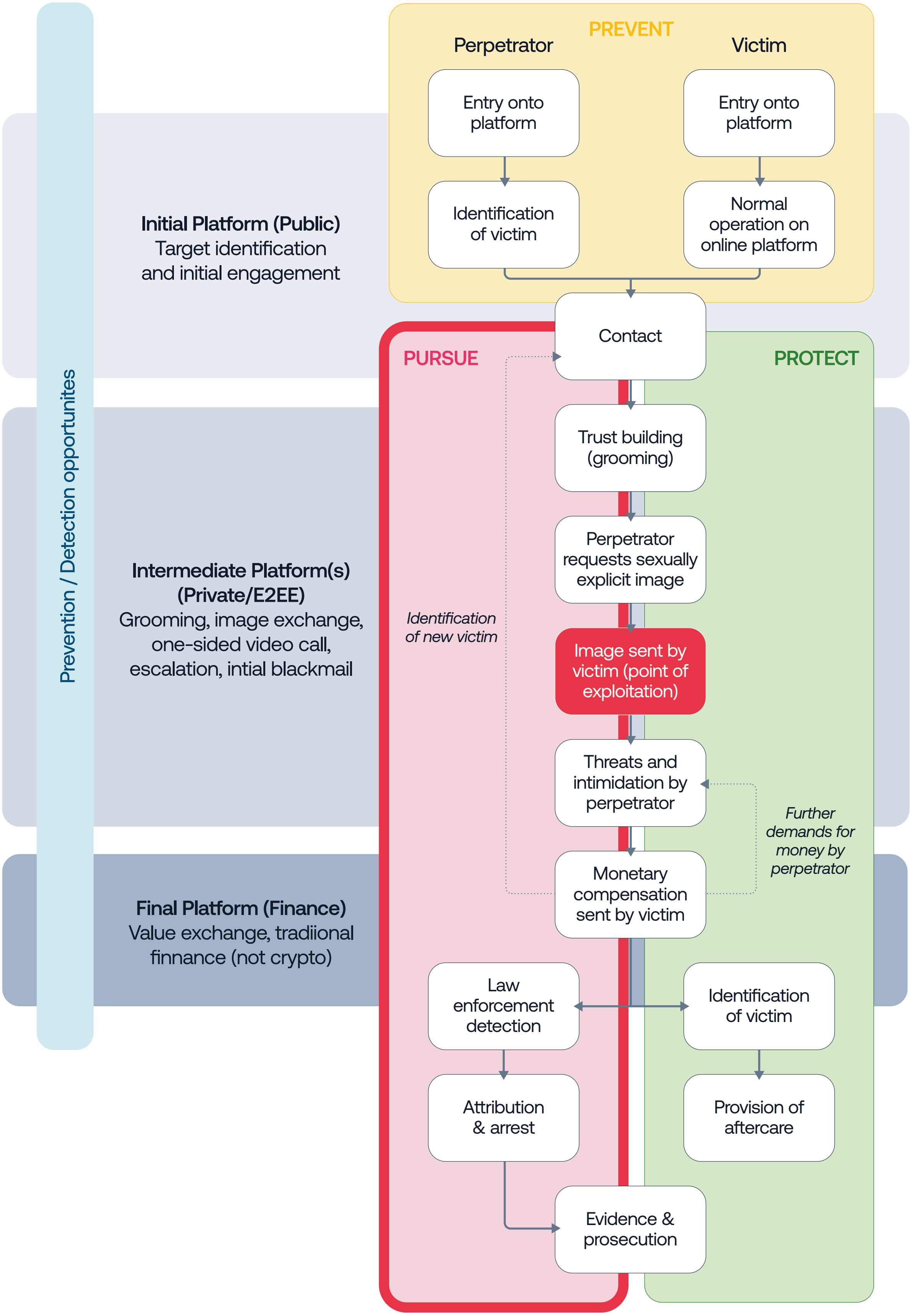
Technology platforms

- Block predators and victims' nude images
- Prevent further resharing/revictimisation of uploaded image(s)
- Identify adults speaking 'child-like', and therefore, masquerading as a child online
- Automate messaging to potentially vulnerable individuals to highlight risk and provide guidance
- Publicise the association of FSE and certain platforms (e.g. platforms with highest risk of harm).
- Generate a banned list/watch list on platforms to deter predators

3. PURSUE | Relentlessly disrupting perpetrators

Urgent action is required to proactively target, pursue and dismantle perpetrators through to prosecution and disruption, bringing the collective powers and tools from across industry and government to bear.

The ecosystem needs to better utilise the full capabilities of the combined safety and security apparatus to better identify, assess and pursue those individuals who are determined to exploit children through FSE.


Prevention / Detection opportunites
Initial Platform (Public)
Target identification
and initial engagement
Intermediate Platform(s)
(Private/E2EE)
Grooming, image exchange,
one-sided video call,
escalation, intial blackmail
Final Platform (Finance)
Value exchange, tradiional
finnance (not crypto)
PREVENT
Perpetrator
Victim
Entry onto platform
Entry onto platform
Identification of victim
Normal operation on online platform
Contact
PURSUE
PROTECT
Trust building (grooming)
Perpetrator requests sexually explicit image
Identification of new victim
Image sent by victim (point of exploitation)
Threats and intimidation by perpetrator
Further demands for money by perpetrator
Monetary compensation sent by victim
Law enforcement detection
Identification of victim
Attribution & arrest
Provision of aftercare
Evidence & prosecution

Challenges identified that will need to be overcome:

Reporting

- Lack of awareness of where/how to report instances of FSE
- Investigations are dependent on the quality of reporting
- Dealing with reports in sites and not escalating threat to law enforcement.

Collaboration

- Silos across the ecosystem and ways of working across partners (including platforms, finance, and public protection teams).

Capability

- Lack of adequate investigatory skills and capability.

Scale

- Content is shared at scale making its removal significantly challenging
- Increased use of crypto as a means to "cashing out".

Possible solutions that should be explored:

Collaboration across the ecosystem

- Join up the approach between industry platforms and law enforcement
- Work with partners to map offenders' financial network as one individual is often behind many accounts
- Share offence related data with partners to strengthen the intelligence picture.

Capability

- Equip law enforcement officers with the right tools (e.g. AI)
- Leverage the use of digital forensics
- Define what technological innovation is needed to successfully intercept and intervene
- Standardise reporting and coordination approach.

Next steps

There is clear evidence from the rising incidence of reports of financial sexual extortion and the devastating impact it has on victims that now is the time to step up the UK and global approach to tackling this alarming, growing abuse trend.

The following next steps will be taken:

- Share the output from this cross-sector collaboration event with attendees and consider options for further dissemination (e.g. at the NPCC Prevent Board).
- Consider if there is value in running a series of cross-sector collaboration forums around the topic of tackling FSE (consider it from a campaign perspective and taking an activist approach, with a focus on innovation and better utilisation of SMEs capabilities).
- Consider how to shape awareness campaigns and communications to technology platforms, focusing on the fact that by tackling FSE, they are tackling many more issues.
- Consider what capabilities are currently missing from across the ecosystem that could better help tackle FSE, and thereby, helping to set out what the opportunities are for SMEs and others to build new capabilities to fill any perceived gaps.

Together, we can work to prevent the threat of FSE, ensuring children are able to enjoy the benefits of social media and other online platforms.

Acknowledgements

PA would like to thank Plexal for hosting the event, and the expert panel for providing the opening address and helping to set the context for the event:

- Iain Drennan, Executive Director, WeProtect Global Alliance
- Simon Bailey QPM, Director, Child Rescue Coalition
- Ian Critchley QPM, Child Protection Lead, NPCC
- Julie Dawson, Chief Policy & Regulatory Officer, Yoti
- Saj Huq, Chief Innovation and Commercial Officer, Plexal

Additionally, PA would like to thank all those who attended the event for their ideas and contributions:

Accenture

Actica Consulting

Breck Foundation

Child Rescue Coalition

Government Communications Headquarters

UK Home Office

Internet Watch Foundation

National Crime Agency

National Police Chiefs' Council

Policing Institute for the Eastern Region

Playroom

Plexal

UK Safer Internet Centre

WeProtect Global Alliance

Yoti

About PA

We believe in the power of ingenuity
to build a positive human future.

As strategies, technologies, and innovation collide,
we create opportunity from complexity.

Our diverse teams of experts combine innovative thinking and breakthrough technologies to progress further, faster. Our clients adapt and transform, and together we achieve enduring results.

We are over 4,000 strategists, innovators, designers, consultants, digital experts, scientists, engineers, and technologists. And we have deep expertise in consumer and manufacturing, defence and security, energy and utilities, financial services, government and public services, health and life sciences, and transport.

Our teams operate globally from offices across the UK, Ireland, US, Nordics, and Netherlands.

Discover more at paconsulting.com and
connect with PA on LinkedIn and Twitter.

PA. Bringing Ingenuity to Life.

Corporate Headquarters

PA Consulting
10 Bressenden Place
London SW1E 5DN
United Kingdom

+44 20 7730 9000

paconsulting.com

This document has been prepared by PA. The contents of this document do not constitute any form of commitment or recommendation on the part of PA at the date of their preparation.

Produced by Design Studio at PA
3_376700 March 2024.