Science & Technology in Policing

CASE STUDY

FRAUD EXPERIENCED BY CHILDREN AND YOUNG PEOPLE: PROTECTING THE DIGITAL GENERATION

Understanding and addressing fraud against children and young people (CYP), and developing an effective policing and policy response to it, is an emerging operational priority. To understand how science and technology is part of the solution, we spoke to a Senior Intelligence Analyst of City of London Police, Beth Mooney (Head of Research, Crest Advisory) and Madeline Rolfe (Strategy and Insight Manager, Crest Advisory) who have been working together to tackle youth-targeted fraud by developing an action plan setting out clear actions for partners involved in the response.

Understanding the threat

Fraud is commonly associated with older or vulnerable adults – a perception echoed by many young people during the interviews conducted as part of this study. This project, funded by the 24-25 Police STAR Fund and led by the City of London Police in collaboration with Crest Advisory, challenges that assumption. It is the first police-led initiative to examine fraud experienced by CYP in depth, combining national survey data, police intelligence, and qualitative interviews to build a comprehensive evidence base.

To understand the scale, nature and impact of fraud among CYP, the research team conducted interviews with over 50 young people aged 11–21 across England. They also ran two nationally representative surveys: one with 1,000 CYP aged 13–21, and another with 999 parents and guardians of children aged 10–21, both across England and Wales.

The project analysed National Fraud Intelligence Bureau data on all fraud reports from CYP aged 10–21 during 2023, and engaged fraud experts from financial institutions, technology companies, police forces and voluntary organisations. Running from April 2024 to early 2025, the research triangulated these multiple data sources to build a comprehensive picture of the problem.

The team's research revealed:

88% of young people aged 13–21 reported encountering suspected fraudulent content online in the past year.

Nearly one in three (29%) had been a victim of fraud.

Only 1% said they had never seen a scam attempt.

These figures reveal a widespread but under-recognised threat. Young people are not only at risk, they are being actively targeted.

A senior representative of City of London Police reflects on why fraud against CYP has remained under-recognised despite its scale.

"Initiatives to safeguard CYP against other crime typologies perpetrated online such as sexual exploitation, terrorism and radicalisation, bullying and hate crime have been more vocal and have moved at greater paces. Whilst these threats are quite rightly priorities, it is critical that efforts to protect CYP financial safety whilst online don't fall behind."

The research also uncovered a significant perception gap. Many young people did not recognise fraud as a crime, as Beth Mooney explained:

"When we asked young people about fraud, they didn't know what it was. When we told them what it was, they didn't understand that it was a criminal offence."

It also transpires that they don't consider it something worth reporting.

> ***"I thought fraud happened only to people who didn't understand the internet, not someone my age."*** 17-year-old participant

This normalisation of scams as part of online life contributes to under-reporting and a lack of support for victims.

How fraudsters operate

The study identified clear patterns in how fraudsters target young people. Rather than relying on complex cyber-attacks, scammers exploit everyday digital behaviours. Social media platforms, messaging apps, gaming environments and online marketplaces are the primary vectors. Madeline Rolfe explained that, often, professional-looking and familiar sites such as TikTok shop or Facebook Marketplace can ***"confer a sense of legitimacy, which can make young people more susceptible to falling for the fraud and scams."***

Common tactics include impersonation via direct messages, phishing links disguised as delivery notifications or login prompts, and fake storefronts selling popular items. Instagram and TikTok were frequently cited as platforms where fraudulent sellers appeared legitimate due to high engagement metrics. Discord and Roblox were mentioned in relation to in-game scams, while Facebook Marketplace was a hotspot for various kinds of fraud.

The impact on victims

Fraud against CYP is not a victimless crime. The emotional and behavioural consequences are significant. Victims reported feelings of shame, anxiety and isolation. Some withdrew from social activities or changed their online habits.

> ***"It broke me for a while – I stopped going out with friends because I had no money and I felt dumb about what happened."*** 18-year-old who lost £600 in a cryptocurrency scam

Madeline Rolfe spoke to several young people with different stories, explaining that: ***"There was a huge list of harms. They lost money. That was clear, but the emotional impact – feelings of fear, and doubting their own safety online were quite significant - and there was nothing set up to support young people with those harms."***

Despite this, 60% of victims did not report the incident to any official channel. Reasons included not knowing how to report, believing nothing would be done, and feeling personally responsible. This silence means victims miss out on support, and the true scale of youth fraud remains hidden from law enforcement and policymakers.

Developing the response

To address these challenges, the project team developed a five-point Action Plan. It is designed to be practical, scalable and rooted in evidence.

1. Make youth fraud prevention a national policy focus

The team's findings have been presented to government, and the team have recommended that the upcoming National Fraud Strategy includes children and young people as a priority group.

2. Education must be strengthened

Schools should integrate fraud awareness into the curriculum, alongside cyberbullying and online safety. Young people need to understand what fraud is, how it works, and how to respond.

Madeline Rolfe spoke of the conversations she had with young people to help develop recommendations shaped by youth voices: ***"We went back and spoke to many of the same young people who we had interviewed and some additional young people who were just interested in the topic, and facilitated questions based on that to help arrive at some feasible recommendations."***

3. Industry must design out fraud opportunities

Social media platforms should identify and remove fraudulent material. Banks and payment apps should implement safeguards for young users, such as transaction alerts and verification steps for large payments – as Alexander Hides recognised, as fraud methodology moves quickly, response to it also needs to.

Beth Mooney explained that banks are already working to out-design fraud, stating that there's now ***"legislation that means the banks, in some cases, are responsible for reimbursing people when they've been a victim of fraud...even just having that level of responsibility on banks is likely mobilising them."***

It is also important to remember that fraudsters shift methodology quickly, so fast adaptation is just as crucial as the innovation of mechanisms to disrupt them.

4. Reporting and support systems must be tailored to the audience

The City of London Police will replace Action Fraud with a new service, Report Fraud, launching in December 2025. This service will make reporting fraud and cyber crime easier and faster for everyone, reduce the burden on victims, and keep them informed about their case. Victims will also be notified when their report helps protect others.

5. Data collection must improve

Age-tagging of fraud reports is inconsistent, making it difficult to track trends and measure progress. The Action Plan proposes a Youth Fraud Index to monitor prevalence, financial losses and outcomes annually.