Scams: Real cases, real consequences

A collection of case studies and lessons for consumers

November 2025

CCPC

Coimisiún um Iomaíocht agus Cosaint Tomhaltóirí

Competition and Consumer Protection Commission

Contents

Introduction 4

About this research 4
Structure of report 4
Goods intentionally not provided 6
Overview 6
Case studies 6
Services intentionally not provided 9
Overview 9
Case studies 9
Rental accommodation scam 11
Overview 11
Case studies 11
Fake employment offers 13
Overview 13
Case studies 13
Phishing and vishing 15
Overview 15
Case studies 15
Cryptocurrency scams 17
Overview 17
Case studies 17
Hacked accounts 20
Overview 20
Case studies 20
Other types of fraud 22
Overview 22
Case studies 22
Lessons for consumers 23

Summaries of fraud cases 24

Type of fraud 24
Where fraud was encountered 24
When consumers suspected they had been defrauded 24
Financial loss 24

Contents

Summaries of fraud cases contd.

Payment methods 24
Payment methods across all cases 24
Payment methods by type of fraud 24
Money recovery success 25
Success by type of payment 25
Demographic details 25
Experiences of fraud by age 25
Experiences of fraud by education level 25
Conclusions 25
APPENDIX 1: Fraud survey 26

Introduction

The CCPC's remit includes providing information to consumers on their rights when buying goods and services, both through our website, ccpc.ie, and our helpline. To better understand the impact of our information services, we have undertaken research with consumers to learn about the eventual outcome to their issue (i.e., whether they got an appropriate resolution) after they contacted the CCPC helpline for advice.

One strand of this research relates to consumers' experiences of fraud or scams. This is an area of increasing importance to the CCPC due to our financial education remit and the overlap between fraud issues and consumer protection. Our research into consumers' experiences of fraud also aligns with our commitment to report on financial issues, including fraud cases, under Ireland's National Financial Literacy Strategy.

About this research

In 2024, the CCPC helpline received almost 45,000 contacts with queries on a range of consumer rights and personal finance issues. Of these contacts, less than 1 per cent (441) reported a suspected fraud or scam.

To learn more about consumers' experiences of fraud or scams, we called back a small sample of consumers (30 people) who had contacted the CCPC helpline between May and August 2025 about a suspected fraud experience. The fraud experiences they shared with the CCPC occurred from November 2024 to August 2025.

The follow-up call used a semi-structured interview to survey consumers on their experience and what resolution, if any, they had obtained after first contacting the CCPC. As it can be difficult to revisit an experience of fraud, we kept questions in the follow-up call to a minimum. A copy of the interview questions is in Appendix 1.

These 30 cases involved financial losses of between €41.90 and €20,000. A total of almost €60,000 was lost across all 30 fraud incidents. Of this, less than €5,000 had been recovered at the time of the phone interviews.

Structure of report

This report features a series of brief case studies of people's experiences of fraud or scams, organised by the following categories:

- Goods or services intentionally not provided

- Rental accommodation scams

- Fake employment offers

- Email phishing and fake calls

- Investment scams

- Hacked accounts

- Other scams

Each category starts with an overview of key features, followed by the individual case studies. The case studies combine details recorded during both the consumers' first call to the CCPC and their follow-up interview by phone.

The report also contains a summary of notable patterns across all fraud categories, such as where frauds were encountered, payment methods, amount of money lost and consumers' success in recovering any money before and/or after contacting the CCPC.

The final section of the report provides some overarching findings and recommendations for consumers.

We are publishing these case studies as part of our remit to inform and support consumers so that they may more easily identify and avoid potential scams. We thank all the consumers who agreed to share their experiences with us.

> Although consumers named specific businesses when sharing their experiences, we have removed all business names from this report. We have also made minor adjustments to inconsequential details in some of the case studies (for example the type of item purchased) to further protect consumers' anonymity.

Goods intentionally not provided

Overview

Origin of fraud

- Social media ads link to cloned or fraudulent sites that imitate well known retailers
- Professional design, AI-created visuals and influencer references boost false credibility

Payment patterns

- Purchases made with debit/credit cards; values from €30–€320 common
- In several cases, extra unauthorised charges followed the first transaction.

Resolution attempts and outcomes

- Chargeback: Most effective path but inconsistent and sometimes slow; in one case payment initially reversed but then re-charged; in other cases, chargeback took approx. 2–3 weeks.
- Impersonated retailers: Sympathetic but typically unable to assist
- Social platforms: Routinely declined to intervene or deemed traders genuine
- Authorities (An Garda Síochána): Cases logged; limited follow up when consumers were interviewed
- Small claims procedure: Not applicable when the business is illegitimate

Case studies

Armchair purchased from a cloned website

A consumer paid €125 by debit card for an armchair after clicking through an ad on a leading social media platform to what he thought was the website of a popular furniture retailer.

He started to become suspicious when the furniture didn't arrive a few days later. When he contacted the actual retailer, the shop told him that there was no record of his order and the table was not part of chain's catalogue. It was then clear that he had shopped from a cloned website.

The consumer contacted the social media platform but said it didn't offer any assistance on the matter. After contacting the CCPC for advice, he contacted his bank and reported the scam to An Garda Síochána. His bank reversed the debit card transaction and he recovered the full €125.

He is now more likely to verify transactions on his bank statements and is more suspicious of content on social media.

Chainsaw purchased via ad on social media

A consumer paid €50 by debit card for a chainsaw he had ordered through an ad he had found on social media.

When the chainsaw hadn't arrived a week later, the consumer became suspicious and contacted his bank to request a chargeback to reverse the debit card transaction. His bank told him the chargeback request would take 21 days to review.

After contacting the CCPC, the consumer's bank confirmed that the debit charge transaction was reversed and it had refunded all money. However, the payment was subsequently returned to the trader.

The consumer reported the issue to the social media platform, which did not consider it a scam. The consumer's attempts to contact the seller directly were unsuccessful.

At the time of the follow-up interview, no money had been recovered. The consumer was frustrated with the lack of support from his bank and from the social media platform.

Shelving purchased via social media

A consumer paid €320 by debit card for shelving from a furniture business he found on social media, believing that the page appeared professional.

However, the shelving was not delivered within the promised two-week period and the business failed to respond to any of the consumer's messages. The consumer later discovered online reviews from others who had similar experiences with the same business.

The consumer attempted to resolve the issue through the small claims procedure, but his application was rejected because the business was deemed illegitimate. He then contacted his bank, which requested he first submit a final complaint in writing to the scam company.

After contacting the CCPC, the consumer reported the business to the social media platform, but he was told it couldn't help because it considered the seller to be genuine. The consumer also reported the incident to An Garda Síochána, who logged the case. At the of the interview, the consumer was awaiting follow-up contact from the Gardaí. However, when the consumer got back in touch with his bank, the debit card transaction was reversed and he recovered the full €320.

In hindsight, the consumer said he might have suspected a scam sooner if he had checked the online reviews before he made the transaction. Otherwise, the page looked very convincing. He assumed that the social media platform would have vetted any company that it was advertising.

Dog bed purchased from cloned website

A consumer wanted to buy a large bed for her dog. She was searching online for a cheaper alternative to her usual grocery store's delivery service when she found what appeared to be a legitimate website from an established grocery chain and a listing for a bed that was available for delivery.

She paid €52 for the bed by debit card but realised the offer was a scam by the next day when she still had not received an order confirmation email. When she contacted the grocery chain, it confirmed that it doesn't sell goods online. Though it was sorry for what happened, it said it couldn't offer any help.

After contacting the CCPC, the consumer contacted her bank and reported the scam to An Garda Síochána. About two weeks after she contacted her bank, she received a full refund via a chargeback on her debit card.

On reflection the consumer noted that the website was convincingly cloned, with no obvious signs of fraud. When she went looking through the legitimate website, she was still unable to spot any difference.

Car tools purchased via fake ad

A consumer clicked through a fake grocery store ad on social media to a fraudulent website claiming to sell discounted goods. He ordered jump leads and an emergency breakdown kit, paying €98 by credit card, and received an email shortly afterwards confirming that the items had been shipped.

However, when the items did not arrive in the following weeks, he contacted the grocery store, which confirmed that the ad was fraudulent. It also confirmed that it was aware that others had been targeted.

The consumer also contacted his bank, which had traced the scam to an operator outside the EU. The consumer received a full refund by chargeback from his credit card provider and had his credit card cancelled to prevent further transactions.

Despite being able to recover his own money, the consumer noted that the ad was still active and was frustrated by the lack of accountability from the grocery store and the social media platform.

Supplements purchased via social media ad

A consumer's grandparents clicked an ad on social media for supplements that featured two social media influencers. The ad led them to a website that resembled that of a legitimate wellness brand.

The couple paid €41.90 by debit card for supplements but became suspicious after a few days when they hadn't received any confirmation email.

The consumer's grandmother contacted the bank for a chargeback but, at the time of the phone interview, had not been able to recover the money. However, the bank was able to block the business from taking further payments from the debit card.

To try to protect others from the same scam, the consumer also alerted the genuine website to her experience but received no reply. She also alerted the influencers. One of the influencers replied to say that she would follow up on it.

The consumer's grandparents had believed the site to be trustworthy as it claimed to be based in Ireland. However, upon checking the site, the consumer could see that the brand photos were AI-generated and the influencers were photoshopped to be holding the product.

Fake trader and card misuse

A consumer ordered a shoulder brace online, paying €30 by debit card. He realised the transaction was a scam about five days later when the brace hadn't arrived and his bank notified him that the same business took a further €46.15 from his account. The bank blocked the card to prevent further transactions.

After contacting the CCPC, the consumer reported the scam to An Garda Síochána but was still awaiting a response at the time of the phone interview. He also contacted his bank, which reversed the second deduction (€46.15), knowing the consumer hadn't authorised it. At the time of the interview, he had not received a refund of the first €30.

On reflection, the consumer suspected that the website and photos didn't look quite right. After the second payment was taken from his card, he found online reviews from others who had the same experience. He said that he would have known the offer was a scam if he had checked the reviews first.

Garden tool purchase from fake website

A consumer ordered a garden strimmer online from what he thought was a legitimate website of a grocery chain. He paid by debit card after his attempt via PayPal was declined.

He received a pop-up message that his order was confirmed. He found it strange that he didn't get any email confirmation but didn't think much of it. However, he realised the transaction was a scam about six days later when he saw four unauthorised New York-based payments from his bank account totalling €86.

When the consumer contacted the grocery chain, he was advised that it doesn't offer a delivery service. Though it was sorry to hear about the issue, it said it couldn't do anything. The consumer also contacted his bank, which cancelled the card. After an internal review, it did a chargeback on his debit card to refund the total amount he had lost.

On reflection, the consumer hadn't noticed any signs that he had bought from a fraudulent website. The only thing he would have changed about his actions was to have contacted the bank more quickly after failing to get an order confirmation email. Despite recovering the full amount of money, the consumer reported a loss of confidence in online shopping after the incident and no longer uses his email address.

Services intentionally not provided

Overview

Origin of fraud

- Sponsored links and social media pages leading to fake service providers
- Increased vulnerability due to emotional investment (adopting a pet, securing a loan, booking a holiday)
- Initial overlooking of poor-quality websites and spelling errors
- In some cases, escalating demands and intimidation (e.g., threats of legal action)

Payment patterns

- Upfront payments via bank transfer, online-only banking app or debit card
- Amounts ranged from €300 to €11,000, often in multiple instalments

Resolution attempts and outcomes

- Banks: Chargebacks possible for card payments but slow; bank transfers rarely recoverable
- Authorities: Cases logged by An Garda Síochána but limited follow-up at time of interview
- Platforms: Social media and sponsored link hosts offered minimal accountability
- Legal routes: In some cases, consumers exploring litigation or cross-border recovery

Case studies

Fake dog adoption offer

A consumer and his wife were looking to adopt a dog when they found a page on social media named *Irish Dogs and Pups*. The person offering the dog for adoption claimed the animal was free but asked the consumer to pay €300 for registration and vaccinations.

After the consumer made the first payment via an online-only banking app, he and his wife were given a tracking number from a suspicious site and pressured to pay a further €500 for a cage. At this point, he recognised it was a scam.

He reported the fraud to An Garda Síochána, his bank and the social media platform, but all had told him that they were unable to help. At the time of the phone interview, he had not recovered the €300 payment.

The consumer reported emotional distress over the situation and expressed concern over ongoing scam attempts.

Loan release scam

A consumer's elderly mother was looking to take out a loan when she searched online for loan providers and found a company through a sponsored link. Her loan was approved, but she was told to pay €500 upfront for the funds to be released.

After the consumer's mother paid the initial sum, the scammer demanded another €500 a week later and began threatening her with legal action and accusations of tax evasion. At this point, she told her son, who took control of communications and reported the issue to An Garda Síochána. At the time of the phone interview, they were awaiting follow up contact from the Gardaí.

After contacting the CCPC for advice, the consumer contacted the bank on behalf of his mother. He was told that it was unable to help because she had authorised the first payment. At the time of the phone interview, no money had been recovered.

On reflection, the consumer felt the scam was obvious since neither he nor his mother had heard of the lender previously and the extremely low interest rate sounded too good to be true. He now manages his mother's financial and online activity.

Holiday rental via fake travel agency

A consumer booked a holiday in France through a travel website. After he paid €11,000 via bank transfer, the travel agency ceased communication. The website disappeared a few days later.

Before contacting the CCPC, the consumer contacted An Garda Síochána, the Central Bank of Ireland and his bank. The bank attempted to reverse the bank transfer but was unsuccessful. The consumer was advised that the receiving bank in Spain may bear liability. At the time of the phone interview, he was exploring legal options to recover the funds from that bank.

The consumer noted feelings of frustration and uncertainty after the incident, and a loss of trust in online travel services.

Fake immigration service

A consumer found a sponsored link for an immigration service while searching online for assistance to obtain a permanent visa for the United States. She paid a fee of €330 by debit card, provided her passport details and received login details for an online account.

However, she realised the transaction was a scam the next day when she tried the login and was informed her account did not exist. When she contacted the service, there was no response.

The consumer reported the scam to An Garda Síochána, her bank and the Passport Office. At the time of the phone interview, about six weeks after contacting her bank, she was still waiting for confirmation that the transaction would be reversed via chargeback.

In hindsight, the consumer acknowledged that the visa service didn't seem genuine because of the constant spelling errors in its correspondence to her and the poor quality of its website.

Rental accommodation scam

Overview

Origin of fraud

- Fake listings on reputable property sites and social media groups
- Fraudsters posing as landlords, using convincing tenancy agreements and staged viewings
- Emotional urgency (need for housing) exploited to demand upfront payments

Payment methods

- Upfront payments via bank transfer
- Amounts ranged from €250 to nearly €1,800
- Refusal to provide Irish banking details; foreign bank accounts used (Malta, Lithuania)

Resolution attempts and outcomes

- Authorities (An Garda Síochána, RTB): Cases logged and ongoing; Gardaí advised legal action but otherwise limited follow-up at time of interview
- Banks: Recovery rare; cross-border transfers complicated and often time-barred
- Platforms: Limited evidence of accountability for listings

Case studies

Fake listing on property listing site

A renter lost a deposit and one month's rent after responding to a fake rental accommodation listing on a leading property listing website. The fraudster had posed as a private landlord, arranged a viewing, provided a tenancy agreement and requested payment of a deposit and the first month's rent.

The renter visited the property in person, signed the tenancy agreement and made a payment of almost €1,800 by bank transfer. But when he arrived on move-in day a few days later, the property was already occupied – likely used for short-term rentals – and the 'landlord' couldn't be reached.

Before contacting the CCPC, the renter contacted the landlord, An Garda Síochána, the Residential Tenancies Board (RTB) and his own bank in France. The fraud was traced to a bank account in Malta. After contacting the CCPC, the renter continued to engage with the RTB and his own bank.

At the time of the follow-up phone interview, the consumer had yet to recover any money. The Garda investigation was ongoing and the RTB case remained open. The consumer's bank in France advised that the claim window had passed, but it was still pursuing the matter.

The experience left the renter more cautious and aware of online rental fraud. On reflection, he thought it out of place that the receiving bank account was in Malta. He said online platforms should take more responsibility for the listings they post.

Social media rental accommodation scam

A consumer posted in a social media group seeking rental accommodation. She received a response from someone who said they had accommodation but required payment before letting the consumer view the property.

The consumer paid €250 by bank transfer and signed what she thought was a genuine rental agreement. When the fraudster demanded a further payment a few days later, the consumer refused, realising it was a scam. This led to the fraudster becoming abusive and threatening.

The consumer contacted An Garda Síochána and her bank, reporting that neither were able to assist. An Garda Síochána advised the consumer to seek legal advice because she had already signed what was presented as a rental agreement.

At the time of the phone interview, the consumer had not recovered any money. She said she was distressed due to the threats and abusive messages she had received.

On reflection, the consumer noticed that the fraudster used multiple bank accounts outside Ireland and refused to provide Irish banking details. In addition, she found it suspicious that the same property was listed on a leading property website for €2,000.

Fake employment offers

Overview

Origin of fraud

- Ads on gaming sites and online platforms promising easy work or high pay
- Falsely branded job offers (e.g., department store)
- Emotional triggers: urgency to earn money or trust in a known brand

Payment methods

- Initial small payments escalating to large sums (e.g., €29 → €10,000)
- Payments via credit card, online-only banking app and bank transfers
- In some cases, unauthorised deductions after initial transactions

Resolution attempts and outcomes

- Banks: Chargebacks possible for card payments but reversals refused for "authorised" transactions
- Authorities (An Garda Síochána): Logged cases but little follow-up at time of interview
- Consumers: Gave up hope of a resolution and/or faced ongoing financial stress and emotional strain

Case studies

Ad on gaming website

A consumer was playing an online game on his phone when he saw an ad offering work to check security codes for major global tech companies.

He responded to the ad and worked at the job briefly but was told he would need to pay €29 to release his earnings. He made a payment by credit card but suspected a few hours later that it was a scam. His suspicion was confirmed when his earnings were never released and a second €29 payment was taken from his account a short time later without authorisation.

The consumer contacted his bank to block further transactions and request a chargeback but, at the time of the phone interview, had not recovered the total of €58 from the two transactions.

After contacting the CCPC, the consumer reported the scam to a global tech company, the Data Protection Commission and An Garda Síochána. The Data Protection Commission said the scam fell outside its remit. The consumer said An Garda Síochána logged the issue, but she was awaiting follow-up contact at the time of the interview.

In hindsight, the consumer noted that it seemed too good to be true to be paid for such a simple job and acknowledged that being asked to pay to release earnings was a red flag.

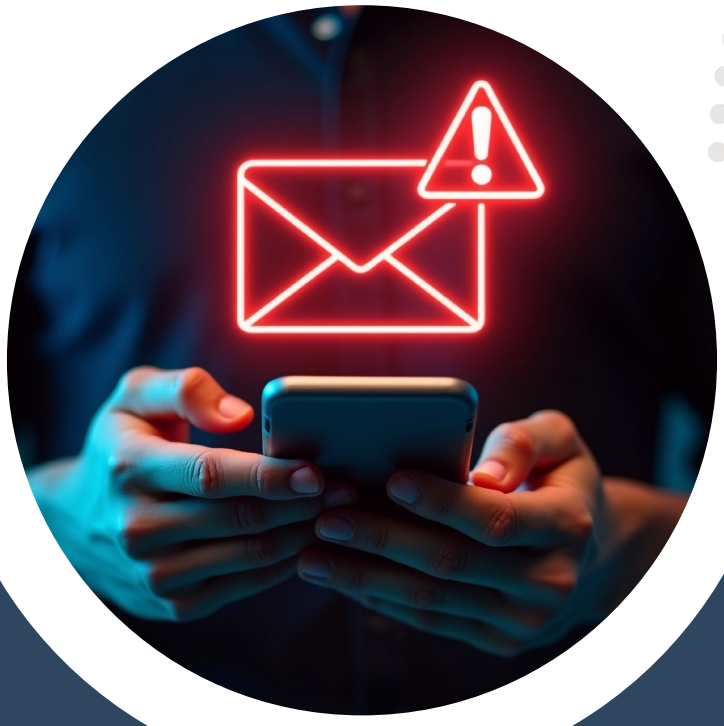
Falsely branded online employment ad

A consumer was looking for work when she found an ad online, falsely branded as a leading department store chain, promising remote work reviewing products with earnings of up to €350 a day. The work involved completing almost 40 tasks a day with a bonus available if the consumer sent cryptocurrency.

Initially, the consumer paid small amounts through her online-only banking app and with her credit card. However, over time, she made €7,500 in payments without receiving any 'earnings' in return. By this point, she knew she was being defrauded but made a final payment of €2,500 in hopes that it would unlock all the money owed to her. This did not happen.

She contacted both the bank and An Garda Síochána about the fraud, but both advised that they were unable to assist because she had authorised the transactions. At the time of the phone interview, she had not recovered any money.

The consumer continues to face financial pressure, with her husband helping pay off the steep credit card bill that arose from the transactions. She reported a great deal of stress and regret over the situation and increased caution and awareness of online scams.



Phishing and vishing

Phishing refers to fraudulent contact by email. Vishing (short for voice phishing) is fraudulent contact by phone.

Overview

Origin of fraud

- Emails: Highly convincing, mimicking hotels and booking platforms complete with real reservation details
- Fake calls: Fraudsters impersonating bank or fraud support using local phone numbers for credibility
- Platform compromise: Messages sent via legitimate apps after account hacks

Payment methods

- Email scams: Payments of €399 and €405 via debit/credit card
- Fake calls: Single withdrawal of €1,000 and multiple withdrawals totalling €3,300 from bank and online-only bank accounts
- In some cases, payments authorised by consumers, making recovery harder

Resolution attempts and outcomes

- Banks: Initial refusals; chargebacks possible only after persistent follow-up
- Platforms: Booking website refunded one case; hotels offered partial goodwill gestures; limited evidence of accountability
- Authorities (An Garda Síochána): Logged cases but limited follow-up at time of interview

Case studies

Hacked hotel account

A consumer was targeted by an email phishing scam after booking a stay in a hotel. The consumer received an email appearing to be from the hotel, complete with accurate reservation details. The email demanded a deposit to secure the booking, threatening cancellation within 24 hours.

After making the payment of €399 by debit card through a link in the email, the consumer contacted the hotel and was told the email was not legitimate. The hotel later confirmed its systems had been hacked.

The consumer contacted both the hotel and her bank for a refund, both of which refused at first. When the consumer contacted the hotel again, it offered her a €150 discount, which she declined.

After contacting the CCPC, the consumer contacted her bank again and reported the matter to An Garda Síochána. After persistent follow-up with her bank, she eventually received the full refund of €399.

The consumer hadn't seen any signs that she was being targeted by a scam because the email was highly convincing. She felt that the hotel was partly liable by not warning customers that its systems had been hacked and was frustrated that there was little accountability or support.

Compromised account on a leading travel website

A consumer's wife booked hotel accommodation on a leading travel website. Soon after, she received a message, seemingly from the hotel, requesting payment. She paid €405 by credit card but was notified by the travel agency a few hours later that the hotel's account had been hacked and the message was a scam.

The consumer's bank refused to process a chargeback to reverse the credit card transaction, stating that the payment to the hotel was authorised. However, he and his wife pursued the travel agency and got a full refund.

The consumer is usually very cautious of scams due to his line of work but said there was no way of knowing that the email was fraudulent because it seemed to come directly from the hotel through the travel agency's app. He believed that the issue stemmed from the travel agency's lack of two-factor authentication for the companies it lists, making it easy for scammers to hack the site.

App download encouraged by fake bank employee

A consumer received a phone call from someone claiming to work for an online-only bank who persuaded her to download an app. The app gave the scammer remote access to the consumer's bank account, leading to the withdrawal of about €1,000 right away.

The consumer noticed the scam immediately and contacted the online-only bank, her bank based in Ireland and An Garda Síochána. The online-only bank traced the scam to India but said it could not assist with the problem. The Ireland-based bank also declined to help, telling her that she was responsible for having downloaded the app.

After contacting the CCPC, the consumer again contacted her bank, the online-only bank and An Garda Síochána, as well as the Central Bank of Ireland and a consumer rights organisation in India. However, at the time of the interview, no money had been recovered.

Because of the loss of funds, the consumer had to borrow money from family to cover her rent and a car loan. She said that, on reflection, she should not have answered an unknown phone number or downloaded the app without getting proper confirmation that the caller was an employee of the online-only bank.

Phone call from fake online retailer fraud support

A consumer reported that her brother and niece were scammed by someone claiming to be from the fraud department of a global retailer. The person had called her brother to tell him that over €9,000 worth of mobile phones appeared in his basket on the company's website.

Soon after, about €3,300 was withdrawn from both her brother's and niece's accounts in multiple transactions. The caller said she didn't know how the fraudster accessed their accounts but suspected it was 'through the internet', as they hadn't shared any personal information.

Her brother and niece discovered the withdrawals within hours when a notification on his banking app showed how much had been debited from his account. After some initial shock, they contacted the CCPC and then their banks and the retailer. However, she felt that the banks and the retailer were redirecting them to each other. At the time of the phone interview, no money had been recovered.

On reflection, the scam appeared legitimate because the caller had used a Dublin phone number and was described as convincing and helpful. The consumer said her family were confused and distressed over how the scam occurred because no personal details had been shared with the caller.

Cryptocurrency scams

Overview

Origin of fraud

- Crypto schemes advertised via websites, social media, TV ads and messaging apps
- Potential vulnerability due to emotional triggers such as desire for financial security and trust in professional presentation
- Use of pressure tactics and fake account dashboards showing inflated returns

Payment methods

- Upfront investments via bank transfer, online-only banking app or debit card
- Amounts ranged from €250 to €20,000, often escalating after initial 'success'
- Additional demands for "taxes" or "release fees" to access funds

Resolution attempts and outcomes

- Banks: Chargebacks rarely possible for transfers; occasional refunds after persistent follow-up
- Authorities (An Garda Síochána, ECCI, foreign regulators): Cases logged but limited recovery of funds at time of interview
- Platforms: No evidence of accountability; one scam linked to a business with an expired operating licence
- Consumers: Psychological and financial impact – distress, sleeplessness and inability to keep up with loan repayments, impacting credit history

Case studies

Locked assets on Malta-based platform

A consumer invested in cryptocurrency through a platform based in Malta, transferring 2,650 USD through his online-only bank account.

He realised the investment was a scam a few weeks after the transfer when the platform displayed his assets but didn't offer any option to withdraw money. It was also requiring him to send more money to be able to release his assets. The consumer communicated with the platform through a messaging app but did not receive any response.

He reported the scam to An Garda Síochána and contacted his bank but, at the time of the phone interview, had not recovered any money and was continuing to engage with the Gardaí.

Since losing the investment, he is unable to keep up with personal loan repayments, which has affected his credit history.

Empty crypto wallet after investment through bank transfer

A consumer who was working two jobs wanted to invest in crypto and found a company online that claimed to offer cryptocurrency investment services. He sent a total of €20,000 by bank transfer to the trader.

The consumer realised the company was fraudulent within a few days when he couldn't see any funds in the crypto wallet that had been set up for him. In addition, the account manager told him he would need to pay taxes to be able to access the funds.

In hindsight, the consumer noted it was a fraud when the 'account manager' would only communicate with the consumer through a messaging app and insisted on bank transfer as the method of payment. The consumer also noted that the company was previously listed by the Financial Conduct Authority (FCA) in the UK but had not renewed its licence, which the consumer thought was for cost reasons.

Despite reporting the incident to his own bank as well as the Central Bank of Ireland, no money had been recovered at the time of the phone interview.

The consumer was initially doubtful that the crypto investment was a fraud because the fraudster was still active on the messaging app and had not disappeared. At the time of the survey, however, he reported a great deal of distress, sleeplessness and regret over the incident and was continuing to seek assistance and explore options.

Inaccessible account and suspicious recovery offer

A consumer came across a cryptocurrency scheme online and invested €500 by debit card. Despite being told by the company that an account had been created, he was unable to log in. Follow-up attempts to contact the company were unsuccessful and the consumer's number was blocked.

After the initial loss, someone claiming to be from the Financial Ombudsman in Switzerland contacted the consumer, offering help to recover the funds. The caller was unsure of their legitimacy and had previously been targeted by similar frauds via social media. After contacting the CCPC, the consumer contacted An Garda Síochána and the Federal Department of Finance in Switzerland.

The consumer had also contacted his bank about the fraud, both before and after contacting the CCPC, but, at the time of the interview, had yet to recover any money. He said his bank did not explain why it could not reverse the debit card transaction.

On reflection, the consumer said there were no initial signs that the crypto investment was fraudulent, as it did not appear any different to past crypto schemes in which he had invested. However, having experienced multiple frauds in the past, the consumer felt that this incident was the final straw. He now is extremely careful with sharing personal information and refuses to answer unknown phone numbers.

Crypto opportunity seen on TV

A consumer came across a company claiming to offer cryptocurrency investment services through a TV ad and made several bank transfers.

The consumer first invested €250 and had regular contact with financial managers and advisors, who showed her promising returns on the platform. When she saw that her initial investment of €250 showed a return of approximately €700, she invested an additional €961 after some pressure from the company. The platform then displayed a balance of €2,700.

Shortly after the second transfer, however, the platform became inaccessible, and the account manager ceased communication. When the consumer tried to contact the trader, she got automated responses and a message that her email was not associated with any account on the platform.

The consumer concluded the platform was a fraud and reported the incident to her bank, while planning to report the incident to An Garda Síochána. Though the payment was not eligible for a chargeback because it was made by bank transfer, her bank refunded the full amount of €1,211. The consumer attributed this to her ongoing persistence until the money was recovered.

On reflection, the consumer felt the TV ad gave the scam an air of legitimacy and described feeling deceived and much more cautious about future online interactions.

Crypto investment offer through social media

A consumer's elderly mother was contacted on social media by a stranger who claimed they advised people on crypto investments. She invested €4,000 from her pension by bank transfer, believing it was a legitimate opportunity.

The consumer learned of the scam about a week later when her mother told her that she was being repeatedly contacted from different phone numbers with demands for further payments and threats of jail time for tax evasion. The consumer then took control of her mother's financial activities and social media accounts to prevent further harm.

The consumer's family contacted the mother's bank, which was unable to assist with a refund. After contacting the CCPC, the family also reported the scam to An Garda Síochána and contacted the European Consumer Centre Ireland.

At the time of the phone interview, no money had been recovered. The consumer's mother had lost most of her remaining pension through the incident.

Hacked accounts

Overview

Origin of fraud

- Account compromise: Hacked gaming accounts; pop-ups triggering unauthorised withdrawals; multiple charges to unknown websites without consumer consent

Payment methods

- Losses ranged from €80 to €1,000 in single incidents and up to €464 through repeat withdrawals
- Payments processed via debit card, digital wallet and online-only banking app
- Transactions often classified as "authorised" by banks, complicating recovery

Resolution attempt and outcomes

- Banks: Chargebacks possible only after persistence; no refund from online-only bank as transaction considered authorised
- Authorities (An Garda Síochána, Central Bank of Ireland and Financial Services and Pensions Ombudsman): Logged cases but insufficient evidence or beyond their remit to follow up
- Money recovered in most cases

Case studies

Unauthorised subscription charges

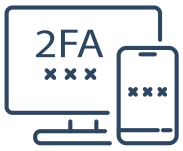
A consumer noticed multiple unauthorised payments on her debit card to companies and websites she did not recognise. One of the sites led to a dating platform while another appeared to sell supplements.

In total, €464 was taken from the consumer's debit card. The consumer did not receive any confirmation emails for these transactions and was unaware of having authorised them.

When she contacted her bank, she was told that the transactions were authenticated through her phone and were classified as subscriptions. She was told she needed to contact the companies to dispute the payments before the bank could consider reversing them through a chargeback.

Eventually, the consumer recovered all her money through her bank, which classified the payments as disputed transactions. She said she had to cancel her debit card twice and get new cards issued and did not know how the scammer got her details.

Funds withdrawal via gaming account

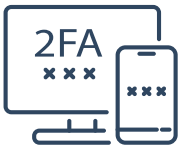


A consumer used her online-only bank card to pay for a game on the website of a large video gaming brand. Shortly after this authorised purchase, her video gaming account was hacked and €80 was withdrawn from her online-only bank account.

The consumer immediately reported the issue to the online-only bank, which froze her account. She also contacted the gaming brand, which acknowledged the hacking and said it would refund the money. The consumer contacted the CCPC while waiting for the refund from the gaming brand and later contacted An Garda Síochána, who logged the issue.

At the time of the phone interview, the video gaming platform had refunded the money to the consumer. She reported that, on reflection, there was no way of spotting the fraud because the hacking happened so quickly and was outside her control.

Online-only bank account withdrawal via digital wallet transaction



A consumer received a suspicious pop-up on her online-only banking app asking if she wanted to accept a payment. Though she declined and blocked the contact, about €175 was still withdrawn from her account and sent to the blocked contact through a digital wallet transaction.

The consumer contacted the online-only bank directly, which said it was unable to do a chargeback and regarded the digital wallet transaction as an authorised payment. After contacting the CCPC, she contacted the Central Bank of Ireland, which logged the issue but said it could not help. She also reported the scam to An Garda Síochána and the Financial Services and Pensions Ombudsman, with the latter telling her that there was insufficient evidence to take further action. At the time of the phone interview, no money was recovered.

The consumer felt there was no way she could have identified the fraud because she had not interacted with the scammer. She reported a loss of trust in digital banking platforms.

Other types of fraud

Overview

Origin of fraud

- Preceded by legitimate online purchase or trust in branded product and seller
- No suspicion of fraud or sense of agency to avoid it

Payment methods

- Pattern: Use of debit card or online-only banking app
- Card skimming via small charges that escalated to larger amounts in quick succession

Resolution attempts and outcomes

- Consumer: Mixed efforts – persistence from one, no reporting from another
- Bank: Card replacement; eventual chargeback after initially requiring consumer to contact the seller
- Authorities (An Garda Síochána): Logged counterfeit goods issue but noted no physical harm
- No money recovered in the case of counterfeit goods

Case studies

Counterfeit items

A consumer bought what she thought were genuine branded earbuds from an old school friend on social media, paying €180 through an online-only banking app. However, the earbuds were not working when she received them.

She realised she had been defrauded less than a week later when she took the faulty earbuds to the manufacturer and was told they were fake. The consumer then noticed that the seller had blocked her on the social media platform to prevent further contact.

The consumer reported the incident to An Garda Síochána, who she said declined to assist because no physical harm had been done. Because of this, she gave up hope of resolving the issue and failed to report anything to the social media platform or her own bank.

At the time of the phone interview, the consumer had not recovered the payment for the earbuds. She said that she had no reason to believe they were counterfeit because a friend had sold them. The experience has left her disappointed and distrustful of online marketplaces.

Card skimming

A consumer checked his bank account online and noticed about seven withdrawals from his account in the space of an hour. The first few transactions were small (between €2.50 and €5) but were then followed by a €45 charge and three charges of €81.90. The total withdrawals came to €303.

He contacted his bank right away but was told to complain to the business before the bank would consider a chargeback.

After contacting the CCPC, he followed up with his bank, telling it that the company had not responded to his complaint. His bank refunded all the unauthorised transactions, cancelled his compromised card and issued a replacement.

He is not sure how the scam occurred. He suspected his card details were skimmed during a previous online purchase, as he had never engaged with the business before.

Lessons for consumers

1. Do not buy through ad links. Navigate to the retailer's official site/app and find the item there.
2. Treat visual trust cues with scepticism: logos, "about us" pages and imagery can be fabricated.
3. If ordering goods, follow up with the seller or your bank immediately if no order confirmation arrives.
4. Check business details online, including independent reviews, and/or contact the business directly to verify any requests for payment, employment offers or goods or services for sale.
5. Pay by debit or credit card where possible (stronger chargeback protections).
6. Monitor banking statements regularly and report any unusual transactions immediately.
7. Never pay upfront for something that would typically be free of charge, for example viewing a letting or accessing employment earnings.
8. Be vigilant against unsolicited requests by phone or email. Delete any suspicious pop-ups or messages.
9. Treat urgent requests or 'too good to be true' offers or investment returns with extreme caution.
10. Check that any investment exchanges or financial providers are regulated in Ireland before investing.

Summaries of fraud cases

Type of fraud

In nine of the 30 case studies, the fraud related to the intentional non-delivery of goods, for example using fraudulent online ads or cloned websites. The least common – just one incident each – were counterfeit goods and card skimming to extract unauthorised payments.

Where fraud was encountered

In 10 cases, people encountered the fraud through an online ad, a cloned website or a sponsored but fraudulent search result. Social media platforms were the source of nine cases. Of these, seven originated from a single social media platform.

When consumers suspected they had been defrauded

The length of time it took to suspect that a transaction or experience was fraudulent depended on the type of scam.

A total of 21 cases were suspected anywhere from right away to within a few days. The scams that were caught right away or within a few hours related to card skimming, hacking (either the consumer's bank account or a website) and non-delivery of goods. However, in two cases – both related to cryptocurrency – fraud was not suspected until up to three months later.

Financial loss

The total amount lost through all 30 case studies came to almost €60,000, with the average loss totalling €1,985.43. A review of the case studies shows a stark variation in the amount of money lost per scam, ranging from €41.90 to €20,000.

- Fake cryptocurrency schemes were responsible for the greatest monetary loss, totalling over €28,000. A single cryptocurrency scam resulted in a €20,000 loss.
- Frauds related to the intentional non-delivery of a service accounted for almost €12,000 in monetary loss. Again, a single case – involving a fake holiday rental – accounted for the largest share within this category, with €11,000 lost.
- A single case within the category of fake employment offers accounted for €10,000 of the total €10,058 lost through this type of scam.

Payment methods

Payment methods across all cases

A debit card was used in 12 cases of fraud, whether through the consumer using their card to pay for an item or service that was never delivered or, in one case, having their card skimmed. Nine cases of fraud involved transfers through an online-only banking app, while other bank transfers were used in seven reported fraud cases.

Payment methods by type of fraud

The types of fraud were achieved through a number of payment channels. Scams involving non-delivery of goods were most likely to be paid for with debit cards. Scams involving fake rental accommodation or cryptocurrency offers were achieved most often through bank transfers. Out of five cases involving a hacked bank account, three occurred with customers of an online-only bank.

Two cases of fraud involved more than one payment method: a transfer through an online-only banking app and either a credit card transaction or regular bank transfer.

Money recovery success

Money was fully recovered in 14 of the 30 cases and partly recovered in one case.

Of the total loss of €59,562.90, over €55,000 had not been recovered at the time of the phone interviews.

Success by type of payment

Across all cases of fraud, consumers were most likely to recover their money if they had paid by debit card. This was particularly true for the use of debit card in cases involving the non-delivery of goods; banks reversed the payments when they acknowledged the transactions were not genuine.

Payments by bank transfer (including through an online-only bank app) were least likely to be recovered because the financial institutions regarded the transactions as authorised. As noted above, bank transfers (including through online-only banks) were used for higher value scams, including those involving fake cryptocurrency or employment offers.

Demographic details

Experiences of fraud by age

Of the 30 consumers who took part in the survey, 25 volunteered their age range. Of these, almost 12 consumers were in the 25-34 year and 45-54 year age range. Only five were aged 55 or over. This suggests that consumers can be vulnerable to scams regardless of age if fraudsters catch them at an opportune time.

Experiences of fraud by education level

Of the 30 consumers who took part in the survey, 20 volunteered details of their education level. Of these, 10 consumers had a Leaving Certificate or equivalent level of education.

The remaining 10 had completed either third level or post-graduate education. This suggests that the sophistication of some frauds, particularly those involving cloning or hacking, makes them harder to detect and avoid regardless of education level.

Conclusions

Based on the small sample of fraud cases, the variety of techniques to target or exploit consumers becomes clear.

In frauds involving the non-delivery of goods and services and cryptocurrency in particular, slick branding and professional presentation created a false air of legitimacy, which can cause consumers to bypass verification, for instance checking online reviews, before committing to a purchase.

Another evident practice was exploitation of immediate needs (such as housing, income) in frauds related to the non-delivery of services and fake employment and rental accommodation offers. Demands for advance payments through payment methods with a less positive recovery rate (such as bank transfers) were common in these types of scams.

The creation of a false sense of urgency was especially evident in phishing, vishing and cryptocurrency scams. The urgency was created in different ways, for example with the threat of a cancelled hotel booking or the promise of rapid investment growth.

Lastly, an underlying theme across all fraud cases was an exploitation of trust, whether in personal networks in the case of counterfeit sales, authority in the cases of vishing or brands in scams involving cloned websites or ads.

It is also noteworthy that fraud was encountered across age groups and education levels. The use of sophisticated but manipulative techniques to exploit trust and personal circumstances can sometimes catch even the most alert consumer off guard.

Appendix 1:
Fraud survey

Agent introduction

Hi, am I speaking to [consumer's name]?

Good morning/afternoon/evening, my name is [name of agent] and I am calling from the CCPC. You recently contacted us about a scam or fraud you experienced. We're following up to learn more about your experience and see if the information we provided was useful. Would you be willing to answer some questions about your experience? It should take about 12 minutes.

Thank you. As you recently contacted the CCPC about a scam or fraudulent activity you experienced, the following questions will focus on that specific incident to help us better understand these types of issues.

[Issue confirmation – agent recaps details of fraud as reported by consumer when they first contacted the CCPC.]

Are these details correct?

[Confidentiality & consent]

Everything you share is confidential. If you don't want to answer a question or want to end the interview at any point, just let us know.

Section 1: Fraud questions

Q.F1 What type of scam or fraud did you experience?

(Provide examples of below if consumer unsure.)

MULTICODE
PROBE TO PRECODE

- Goods or services were intentionally never delivered or provided (e.g. the seller/provider was fake) 1
- Receiving counterfeit or fake goods or services 2
- Pyramid scheme 3
- Investment scam 4
- Cryptocurrency 5
- Cloned website of a well-known brand 6
- Bank account / banking app was hacked 7
- Rental accommodation 8
- Money mule 9
- Music/sport event ticket related 10
- Payment card skimmed 11
- Text scam (smishing) 12
- Romance scam 13
- Other (specify) 14
- Don't know/can't recall 15

7,11,12 – Skip question F4

Q.F2 How did you pay for this?

Note: reference product or service mentioned by consumer if possible.

MULTICODE

- Cash 1
- Debit card 2
- Credit card 3
- Bank transfer (including cheque) 5
- [Online-only bank] transfer (e.g., Revolut) 6
- Voucher/ gift card 7
- Payment intermediary (e.g. PayPal) 8
- Buy now, pay later {CLARIFICATION: "A credit agreement generally with a third party such as Humm or Klarna. The consumer owns the product from the point of purchase but makes repayment to the third party over a short term."} 9
- Other, specify: _____. 10

Q.F3 How long after you paid did you realise that it (the product/service on offer) was a fraud or scam?

SINGLE CODE
PROBE TO PRECODE

- Straight away 1
- Hours 2
- Within a few days 3
- Longer than a few days 4
- Other (specify) 5
- Don't know/can't recall 6

Q.F4 How did you come across the scam?

MULTICODE
PROBE TO PRECODE

- In-store premises 1
- Off-site premises (CLARIFICATION: "For example, a booth at a trade show or shopping centre or a talk or sales event) 2
- Online (website or app) 3
- Over the phone 4
- Online, on a third-party marketplace, website or app {CLARIFICATION: "For example Amazon or Deliveroo."} 5
- Online, on a website where private individuals sell to each other, such as Adverts.ie or Airbnb 6
- In-person 7
- WhatsApp or other messaging platform 8
- Social media platform (e.g. Facebook, Instagram, BlueSky, TikTok) 9
- Text message 10
- Doorstep/ Called to my house 11
- Other 13
- Don't know/ can't recall 14

Q.F5 In addition to contacting the CCPC, can you please tell me who else you contacted?

Note – probe to find out if before or after.

MULTICODE. DO NOT READ OUT

Who contacted	Before CCPC	After CCPC
Family/ friends	1	1
The trader (who sold the good or service)	2	2
The manufacturer of the product	3	3
Another regulator or consumer organisation	4	4
An Garda Síochána	5	5
Solicitor/barrister	6	6
Your bank	7	7
Instant payment provider (e.g. Revolut or PayPal)	8	8
Debit or credit provider (e.g. Visa, Mastercard, Amex)	9	9
Other (specify)	10	10
Don't know	11	
Did not contact anyone else	12	

ASK ALL

Q.F6 Did you experience any financial loss and if so, can you tell me how much?

SINGLE CODE

- ENTER NUMBER EUR: 1
- Don't know/can't remember 2

Ans 2 – Skip QF 7,8,9

Q.F7 What steps have you taken to try to get your money back/resolve the issue?

MULTICODE

- Reported the fraud/scam to An Garda Síochána 1
- Reported the fraud/scam to another regulator (e.g. Central Bank of Ireland, ComReg, Coimisiún na Meán) 2
- Reported the fraud/scam to another consumer organisation 3
- Reported the fraud/scam to a social media platform 4
- Started a claim through the small claims procedure (in the District Court) 5
- Reported the fraud/scam to a trader that was impersonated by the fraudster 6
- Contacted bank or credit/debit card issuer (e.g. to block account, restrict access to online banking or mobile banking, block card to prevent further transactions) 7
- Contacted bank or credit/debit card issuer to get payment reversed through chargeback 8
- Other (specify) 9
- Don't know/can't recall 10

Q.F8 Did you get any money back? If so how much?

SINGLE CODE

-Yes - ENTER NUMBER EUR: ..... 1 **GO TO Q.F9**
-No ..... 2 **GO TO Q.F10**
-Don't know/can't remember ..... 3 **GO TO Q.F10**

ASK ALL >€0 @ Q.F8

Q.F9 And who did you receive this from?

OPEN END

-Don't know/can't remember 1

ASK ALL

Q.F10 What impact, if any, did the fraud/scam have on your credit history?

To be inserted following clarification on question.

ASK ALL

Q.F11 Looking back now on the fraud or scam, were there any signs that could have indicated that this was a fraud or scam?

OPEN END

ASK ALL

Q.F12 On a scale of 1 to 5, where 1 means 'strongly disagree' and 5 means 'strongly agree', to what extent do you agree with the following statements based on your experience of the fraud or scam?

Note: Only read out examples where required.

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree	Don't Know
I am more aware of suspicious content/communications when on social media and/or websites.						
I am more aware of suspicious content/communications received by phone or email.						
I check fraud and scam warnings issued by financial service providers.						
I regularly change passwords on my devices.						
I take steps to protect my personal information when interacting online or on calls (e.g. thinking carefully about posting personal information online, only providing personal information on calls I have made).						

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree	Don't Know
I check and verify the transactions on my bank statements.						
I take steps to verify if a suspicious oral or written communication from an organisation or company is genuine. (e.g., a doorstep visit, a phone call, an email),						
I am more vigilant when contacts request sensitive information.						

ASK ALL

Q.F13 In the past year, can you recall seeing an advertisement, campaign and/or warning to inform you about fraud or scams?

SINGLE CODE

- Yes ..... 1 **GO TO Q.F14**
- No ..... 2 **GO TO CCPC QUESTIONS**

IF ANSWERED 'YES' to Q.F13, OTHERWISE CONTINUE TO CCPC QUESTIONS

Q.F14 Who provided this information?

MULTICODE
PROBE TO PRECODE

- A financial services provider (e.g. your bank) 1
- Central Bank of Ireland 2
- Competition and Consumer Protection Commission 3
- An Garda Síochána 4
- FraudSMART 5
- Social media platform 6
- Other regulator (specify) 7
- Other (specify) 8

ASK Qs RE CCPC, DEMOGRAPHICS SECTION

Thank you so much for answering those questions, I am now going to ask you a few questions about your experience with the CCPC.

Section 2: CCPC questions

ASK ALL >€0 @ Q.F8

Q.C1 How useful was the information provided by the CCPC in helping you get any money back? Would you say it was...?

SINGLE CODE

- Not useful at all 1
- Somewhat useful 2
- Very useful 3

ASK ALL

Q.C2 Could the CCPC have done anything differently to better support you to resolve your issue?

SINGLE CODE

- Yes 1
- No 2
- Don't know 3

IF ANSWERED 'YES' AT Q.C2

Q.C3 Please explain your answer.

OPEN END

Thank you, finally I have a couple of questions about yourself.

Section 3: Demographic questions

Age:

Q.D1 Which of the following age groups do you belong to?

SINGLE CODE

- 18-24 1
- 25-34 2
- 5-44 3
- 45-54 4
- 55-64 5
- 65-74 6
- 75+ 7
- Prefer not to say 8

Gender:

Q.D2 Which of the following words best describes your gender?

SINGLE CODE [READ OUT]

- Male (or man) 1
- Female (or woman) 2
- Other 3
- Or prefer not to say 4

Education:

Q.D3 What is the highest level of education or training you have finished?

SINGLE CODE. DO NOT READ OUT

No formal education or training	1
Primary education	2
Junior cert or equivalent	3
Leaving Cert. or equivalent	4
Third level qualification	5
Postgraduate qualification	6
Don't know	7
Refused	8

Location:

Q.D4 Which of the following best describes where you live?

SINGLE CODE

- City 1
- Suburban 2
- Small/medium town 3
- Rural 4
- Remote 5
- Prefer not to say 6

CCPC

Coimisiún um Iomaíocht agus Cosaint Tomhaltóirí

Competition and Consumer Protection Commission

Competition and Consumer Protection Commission

Bloom House, Railway Street, Dublin 1, D01 C576.

Tel +353 (0)1 402 5500
Consumer Helpline 01 402 5555

www.ccpc.ie