FraudSMART
Informed. Alert. Secure.

FraudSMART Monitor

October 2021

FraudSMART was created by

Banking & Payments Federation Ireland

Impersonation scams on the rise as fraudsters exploit Covid-19 upheaval

The Covid-19 pandemic has caused dramatic changes to daily life and the wider economy.

Against this backdrop, fraudsters continuously update and adapt their tactics and tools. They can quickly identify and exploit scam opportunities presented by evolving consumer and business behaviour as well as the ever-changing economic and social environment.

They have sought to exploit the fallout from the pandemic, preying on worry and fears about the virus, as well as the loneliness and isolation felt by many. They have targeted people who have lost jobs or income and taken advantage of the increase in remote working and online shopping.

SHARP RISE IN FRAUD

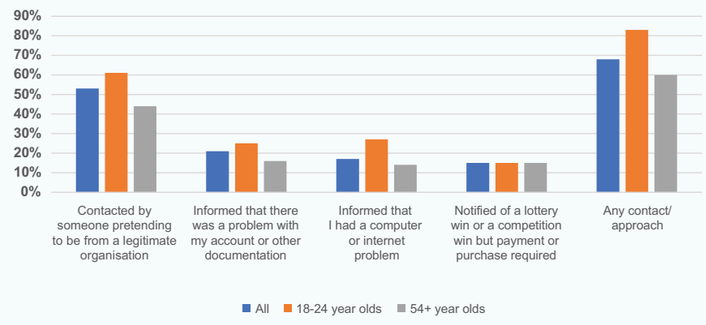
The total losses from unauthorised payment fraud (where a person's account is used without their authorisation or permission) rose by 19.7% year on year in 2020 to more than €41.5 million. Within that, online or card not present (CNP) card fraud losses increased by 21% year on year to €23.1 million, with some 258,000 fraudulent CNP transactions in the year.

Malware (malicious software) campaigns have spread during the pandemic, through which fraudsters aim to steal passwords, bank details and other sensitive information. For example, the FluBot malware, which affects Android phones, is designed to steal personal information including bank details. A common approach is for fraudsters to send text messages claiming to be from a delivery company, that asks user to click a link and install an app to track a package delivery or to pay additional surcharges/customs. The app is actually malware for stealing information from infected devices. Worse still, the malware sends more infected texts to the user's contacts.

2020 saw increasing focus on scams or authorised push payments (APPs) where a consumer or business is tricked by a fraudster to pay them or send them money either by promising a product, services or benefits that isn't delivered or by redirecting a payment intended from someone else to their own account.

APP fraud grew sharply in 2020, with the number of fraudulent transactions jumping by 79% year on year to more than 2,900. Gross losses on APP frauds increased by 51% to almost €15.6 million in 2020.

Impersonation Scams Experienced (Past 12 Months)



Source: Survey of 1,000 adults, July 2021, Coyne Research.

INCREASING PREVALENCE OF IMPERSONATION SCAMS

A key concern in 2021 is the growth of impersonation scams, where the fraudster pretends to be from a legitimate organisation or business to get sensitive information or money from the victim.

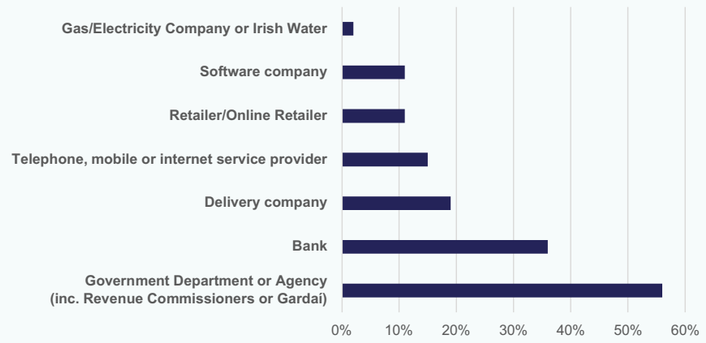
Some 68% of consumers reported being targeted by some form of impersonation scam in the twelve months to July 2021, according to a survey commissioned by BPFI. That proportion was much higher among 18-24 year olds, at 83%. About 53% reported being contacted by someone pretending to be from a legitimate organisation.

When asked who the fraudster was pretending to be, more than half (56%) said a government department or agency including the Revenue Commissioners or Gardaí, while 36% said the fraudster was pretending to be from a bank. Almost one in five said the fraudster pretended to be from a delivery company.

Despite the widespread adoption of online and mobile solutions, most consumers report that fraudsters target potential victims over the phone, with 72% of respondents contacted by fraudsters saying they were contacted by phone, almost twice as many as reported being contacted by email (37%). Some 32% reported being contacted via text message.

Scammers aim to pressure or frighten potential victims into handing over money but it's encouraging that some 70% of respondents to the survey did nothing when contacted. Only 6% clicked on a link in an email, while 3% provide personal or account information and 2% provided bank or credit card details.

Who Fraudsters Claimed to Represent



Source: Survey of 1,000 adults, July 2021, Coyne Research.

It's clear that fraudsters have increased their activity in the past year. Some 83% of consumers report that impersonation scams are more prevalent in 2021 than in 2020, with 68% saying they are a lot more prevalent. They target potential victims through a range of communication channels and in various guises. Some even combined approaches, seeking to communicate through a mixture of emails, cold calls, follow-on calls, voice messages and SMS text messages.

Banks use a range of measures such as encryption and continuous fraud monitoring to protect their customers and ensure every day payments can be made securely but it is important for everyone to protect themselves from fraud by being vigilant.

FraudSmart reminds all consumers to be wary of answering or returning calls or responding to texts from unknown numbers. Always double check before clicking links or attachments in random or unexpected emails or texts. Never give away security details such as PINs or passwords to anyone. If you suspect that you may be a victim of fraud, you should report it to your local Garda station.

We all face the threat of fraud but together, we can stand up to the scammers and stop fraud.

FraudSmart reminds all consumers to be wary of answering or returning calls or responding to texts from unknown numbers.

Fraud Trends in Ireland

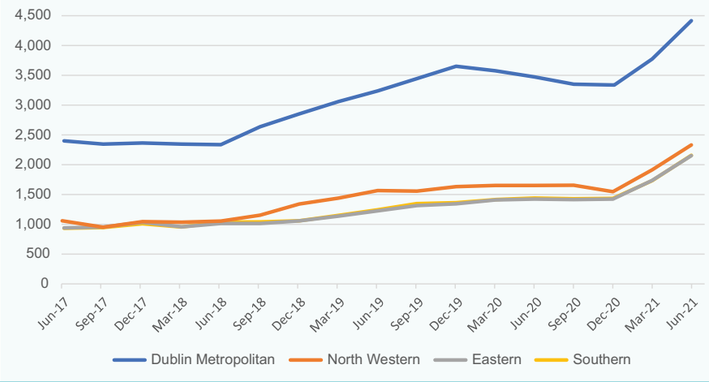
GENERAL FRAUD TRENDS

The number of fraud, deception and related offences recorded by An Garda Síochána jumped in the second quarter of 2021 to 4,044, the highest single-quarter total since the data series began in 2003[1]. According to the Central Statistics Office, the increase primarily related to fraudulent attempts to obtain personal or banking information online or by phone as well as fraudulent use of credit and debit card information.

On an annualised basis, the number of offences also rose to a new high of 11,253 in the twelve months ending June 2021, some 40.6% higher than in the twelve months ending June 2020.

The Dublin Metropolitan Region, which accounted for 39% of fraud-related offences, saw the lowest growth at 26% to 4,407 in the twelve months ending June 2021. Each of the other regions (Eastern, Southern and North Western) saw increases of at least 50%.

Annualised Fraud, Deception and Related Offences



Source: CSO Statistics Under Reservation.

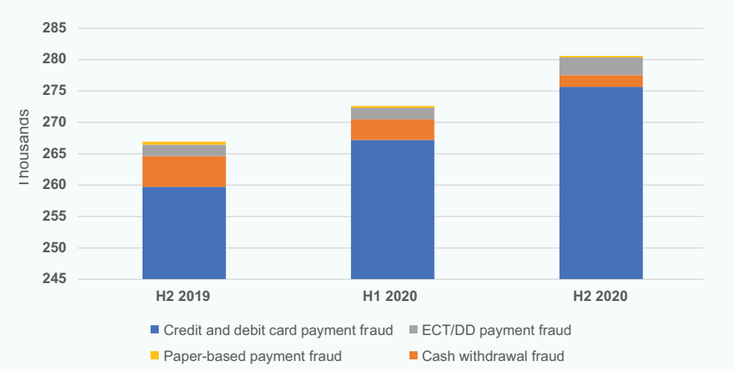
[1] Recorded Crime statistics are produced on a quarterly basis by the Central Statistics Office (CSO) based on information recorded by An Garda Síochána. The CSO categorises the statistics as Under Reservation, which indicates that the quality of these statistics do not meet the standards required of official statistics published by the CSO. These offences include fraud, forgery, counterfeiting (cash and goods), embezzlement and money laundering.

PAYMENT FRAUD TRENDS

The total value of unauthorised payment fraud losses[2] rose by 19.7% year on year in 2020 to more than €41.5 million. The number of fraudulent transactions rose by 5.1% over the same period to amost 281,000.

The growth in fraud activity was driven mainly by a sharp increase in fraud in online card payment fraud and electronc credit transfers (ECTs).

Annualised Payment Fraud Transactions



Source: BPFI. Note: Where possible, payment fraud data includes unauthorised transaction fraud only.

The number of combined ECT and direct debit (DD) fraudulent transactions rose by 55% year on year to 2,800.[3] Gross losses on those payments jumped by 82.8% over the same period to almost €14 million.

ECT payments tend to be relatively high value transactions, with the average ECT/DD payment fraud in H2 2020 at almost €5,000. While ECT/DD payments accounted for only 1% of fraudulent transactions volumes they represented 34% of gross losses in 2020.

Many businesses and consumers adapted to the public health measures to limit the spread of Covid-19 by increasing their use of electronic channels and solutions, especially electronic payments.

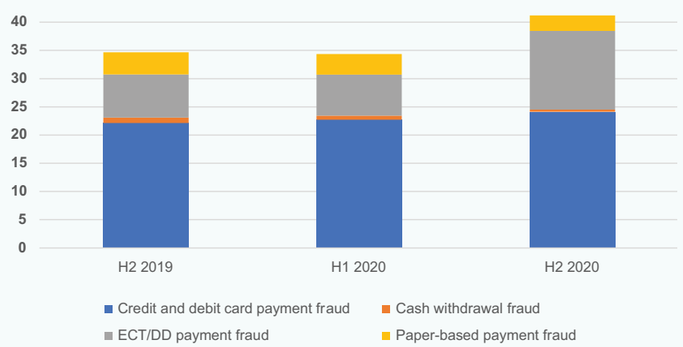
[2] An unauthorised transaction is a payment or cash withdrawal made by another person without the account holder's authorisation or permission and results from the loss, theft or misappropriation of sensitive payment data (such as account numbers and PINs) or a payment instrument (such as a card or cheque).

[3] ECT and DD data are combined due to low DD fraud volumes.

Electronic payments grew significantly in 2020, with the number of ECTs and DDs up by 9.9% and 7%, respectively, according to the Central Bank of Ireland (CBI)[4]. Separate BPFI figures show that online and mobile banking payments grew by 67% between 2016 and 2020 to about 118 million transactions.

Card payment is by the far largest category of fraud payments, a reflection of its dominant place in daily payments. The CBI reported that card payments accounted for 64% of all non-cash payments in 2020. We look at card fraud in more detail in the next section.

Annualised Payment Fraud Gross Losses



Source: BPFI.

As electronic payments grew, cash and paper-based payments declined. Cheque volumes fell by 26% in 2020, according to the CBI, while over-the counter cash transactions in branches fell by 24% and ATM cash withdrawals fell by about 40%.

As usage dropped, so did fraud. The number and value of fraudulent payments with paper-based payments (mainly cheques) fell by 47% and 23%, respectively. There were only 247 fraudulent paper-based payments in 2020 but, with the average paper-based fraud loss at more than €12,300, they caused substantial losses.

By contrast, there were almost 1,900 fraudulent cash withdrawals, down 61.5% year on year but the average loss was much lower at €204.

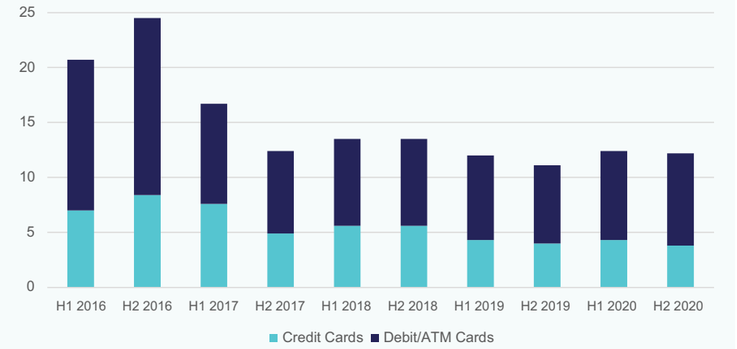
[4] BPFI collects retail payments data on a quarterly basis from six member banks (AIB, Bank of Ireland, Danske Bank, KBC Bank Ireland, permanent tsb and Ulster Bank). The CBI's annual data, as well as its regular payment cards, covers a larger group of payment service providers.

CARD FRAUD

Losses due to unauthorised[5] card fraud (including ATM fraud) increased by 9.5% year on year to €12.2 million in H2 2020. Debit & ATM card fraud losses rose by 17.7% year on year to €8.4 million, the highest value since H1 2017.

The public health measures introduced to limit the spread of Covid-19 had a huge impact on business and society alike. With many businesses, leisure and social services limited or closed from March 2020, people spent more of their working and social life online.

Card Fraud Gross Losses (€, m)



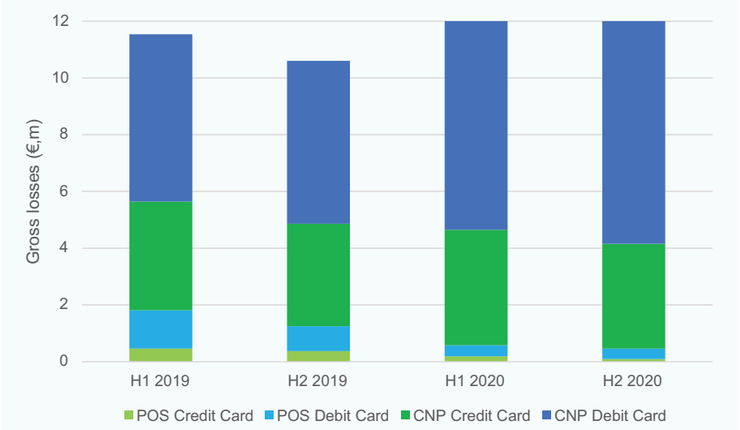
Source: BPFI.

Online sales accounted for 15.3% of total retail sales in April 2020, when the initial restrictions were at the height, according to the CSO. That proportion rose and fell as restrictions eased and tightened with 5.8% of sales online in December 2020 when most businesses were allowed to reopen.

[5] BPFI collects and collates fraudulent payment data from six members: AIB, Avant Money, Bank of Ireland, KBC Bank Ireland, permanent tsb and Ulster Bank.

Debit & ATM card fraud losses rose by **17.7%** year on year to **€8.4 million**, the highest value since H1 2017.

Gross Fraud Losses by Card Type and Channel



Source: BPFI.

Data from the CBI shows that card not present (CNP) spending (mainly online or ecommerce expenditure where the physical card is not present) significantly increased its share of card payments, from 37% in April 2019 to 54% in April 2020.

As online card spending increased, CNP fraud also increased, especially on debit cards. BPFI data indicates that CNP fraud on debit cards jumped by 26% year on year to almost €7.5 million in H1 2020 and by 37% to €7.9 million in H2 2020.

Conversely, as fewer people frequented shops and other retail outlets fraud at the point of sale (POS) plummeted, down 68% year on year in H1 2020 and 63% in H2 2020. Total POS card fraud losses totalled €1 million in 2020, compared with €1.8 million in the first six months of 2019.

CNP fraud on debit cards jumped by **37%** to **€7.9 million** in H2 2020

FraudSmart Tips for Shopping Safely Online

Use secure websites. The website address should be 'https' before the purchase is made, indicating a secure connection.

Use sites where a padlock symbol is shown beside the website address.

Don't use public Wi-Fi when making payments – switch to 3G/4G on your phone if necessary.

Visit the website of the online sales company directly. Don't click on social media or pop-up adverts.

Be cautious about claiming outrageous offers – if it sounds too good to be true it probably is.

Stick to well-known websites or websites that you are familiar with or websites associated with high street retail outlets.

BPFI members recorded some 276,000 fraudulent payment card transactions[6] during 2020. In the second half of the year, there were 136,000 fraudulent transactions, 6.6% more than in H2 2019.

As with gross losses, the number of CNP transactions rose significantly while POS transactions fell sharply. CNP fraudulent transactions on debit cards rose from 162,000 in 2019 to 192,000 in 2020.

In H2 2020, there were fewer than 8,500 POS fraudulent payments with credit and debit cards, down from almost 16,900 a year earlier.

AUTHORISED PUSH PAYMENT FRAUD AND SCAMS

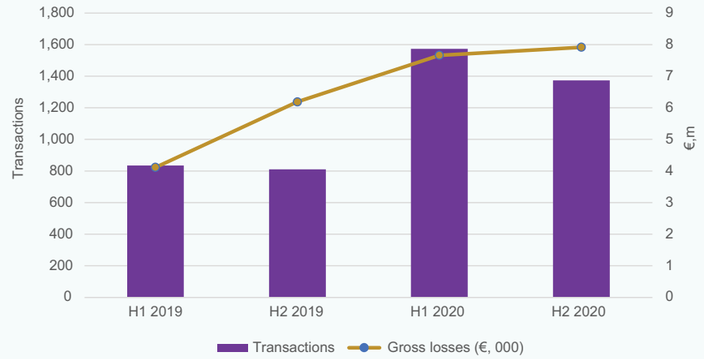
Authorised Push Payment (APP) fraud, also called manipulation of the payer, happens where a fraudster tricks a personal or business customer to instruct their payment service provider (PSP), such as their bank, to send money from their account to an account controlled by that fraudster.

There are two broad categories of APP fraud:

- APP disputed payments, where the customer makes a payment to the account intended but later disputes the payment as the payee has manipulated and scammed the payer. Types of APP disputed payment include advance fee scams, investment scams, purchase/online shopping scams, and romance scams;

- APP misdirection/impersonation, where the customer makes a payment intended for a legitimate recipient but where the scammer manipulates the customer to make the payment to the scammer's account. Types of APP misdirection/impersonation include impersonation scams and invoice re-direction scams.

APP Fraud



Source: BPFI. Note: BPFI APP fraud data only includes electronic credit transfer payments.

APP fraud grew sharply in 2020, according to data reported by members to BPFI on APP credit transfer frauds (including standing orders), with the number of fraudulent transactions jumping by 79% year on year to more than 2,900.

While the number of transactions is low relative to unauthorised fraud the average payment involved is much larger: the average APP fraud transaction was almost €5,300 in 2020, compared with less than €88 per unauthorised card fraud transaction.

Gross losses on APP frauds increased by 51% to almost €15.6 million in 2020.

In this report we look in more detail at the types of scams currently targeting consumers and businesses.

Current Scam Typologies

ROMANCE SCAMS

Victims of romance fraud were conned out of an average sum of €18,000 by fraudsters in 2020.

With an increase in online dating due to Covid-19 restrictions, fraudsters preyed on people's loneliness, isolation and vulnerability increasingly use online dating sites or apps to gain the victim's trust and build up a relationship and emotional connection with their victim.

Frausters will often devote months to this process, after which time they will create a sense of urgency in order to ask their victim for money or indeed in many cases have the victim offer them money.

FraudSmart Tips on Avoiding Romance Scams

Protect your identity: Be careful what you share on social media and online dating websites. Do not reveal your full name or home address. Never provide copies of personal documents such as passports or driving licences.

Use a reputable dating site and use their messaging service. Do not move to social media or texting too quickly.

Never send money or give your bank details to somebody you have never met. Do not pay for flights, visas or customs fees for them to visit you.

If you think you have fallen victim contact your bank immediately, the quicker you act the better chance of recouping any lost funds.

INVESTMENT SCAMS

Media reports based on Garda figures indicate that online investment scam losses jumped by 86% year on year to €7.9 million in the first seven months of 2021. Similarly, banks have reported a large increase in digital currency or cryptocurrency scams in the past twelve months with customers being conned out of as much as €50,000. While investment type scams have traditionally targeted those over 55 years old who have retirement savings, BPFI members have pointed to an increase in cases among those in their 20s who have higher levels of disposable incomes due to the current pandemic.

Victims tend to be cold called or lured by pop-up ads on social media which can often be accompanied by fake celebrity endorsements. The social media ads are linked to cloned websites which look genuine and offer big return on cryptocurrency investments which turn out to be bogus. Individuals actively seeking out alternative investment products are also being caught out as the frausters will create a sense of urgency and pressure not to lose out on a great deal.

FraudSmart Tips on Avoiding Investment Scams

Stop and think: Does this opportunity sound too good to be true? If so, it probably is.

Research thoroughly: Check the individual and firm for qualifications, credentials, reputation and history.

Verify the information: Check all information with a trusted third party such a legal/financial professional and consult family and close friends.

Take your time: There are very few legitimate investment opportunities that require you to hand over or transfer money immediately.

INVOICE RE-DIRECTION SCAMS

Some €10.5 million was lost in Invoice redirect fraud or business email compromise fraud in 2020, according to An Garda Síochána.

This type of fraud typically involves a business receiving an email claiming to be from a supplier/creditor advising of new bank account details to be used for future payments. While the initial email may not come with an invoice, future legitimate payments will be paid directly into the fraudster's account.

FraudSmart Tips on Avoiding Invoice Fraud

- Have fraud prevention processes in place and keep staff regularly trained in fraud prevention and good email practices.
- Implement a procedure to independently verify payment requests with suppliers.
- Review what information you publish about your suppliers online. Providing this information publicly makes you an easier target for fraudsters.
- Always check any change of bank account or payment arrangements directly with your supplier, using existing contact information you have on file.

INTERNATIONAL SCAM TRENDS

Fraud is a global problem and the same scam types reappear in many countries. We draw on data from three large systems for public reporting of scams and fraud: Action Fraud in the UK, FTC Consumer Sentinel Network in the US and Scamwatch in Australia to look at the most common scam and fraud types internationally.[7]

Online shopping or auction scams featured prominently in all three countries in the first half of 2021. These include fraudsters selling poor quality or non-existent goods, fake retailer websites or fake stores on social media platforms and fraudsters using Internet auctions to sell fake or stolen goods.

Scams by Number of Reports			
Rank by Reports	**UK**	**US**	**Australia**
1	Online shopping and auctions **56k**	Imposter Scams **557k**	Phishing **35k**
2	Advance Fee Frauds **35k**	Online Shopping and Negative Reviews **209k**	Threats to life, arrest or other **18k**
3	Cyber Crime **17k**	Prizes, Sweepstakes and Lotteries **72k**	False billing **14k**
4	Investment fraud **16k**	Internet Services **52k**	Identity theft **13k**
5	Dating scam **5k**	Telephone and Mobile Services **52k**	Online shopping scams **11k**

Sources: The City of London Police and the National Fraud Intelligence Bureau (Action Fraud), the Federal Trade Commission and the Australian Competition and Consumer Commission (Scamwatch).

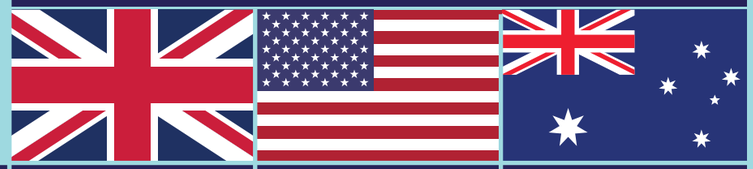
[7] Not all fraud reports involve financial loss for the customer. The FTC excludes almost 287,000 reports of identity theft including card and other bank accounts as losses are not recorded. Some 163,000 Action Fraud reports were uncategorised. Cyber crime and identity theft data is included for Action Fraud and Scamwatch.

Note: Data covers January to July 2021, except FTC which covers January to June.

The concept of imposter or impersonation scams varies by country but they include a range of fraud types such as romance or dating scams, recruitment scams, invoice scams targeting businesses or computer software service/ remote access scams (where fraudsters pretend to be from a legitimate company and convince victims that they have a computer or internet problem that they can fix, for a fee). Many such scams involve fraudsters pretending to be from the police, a bank, or a government department of agency.

These may overlap with advance fee frauds where the fraudster seeks advance or upfront payment for goods, services or opportunities that they never deliver.

Scams by Financial Losses



Rank by Financial Losses	UK	US	Australia
1	Investment Fraud **£410m**	Imposter Scams **$975m**	Investment Scams **A$83.9m**
2	Dating Scam **£57m**	Investment Related **$511m**	Dating & Romance **A$28.1m**
3	Advance Fee Frauds **£51m**	Online Shopping and Negative Reviews **$202m**	False billing **A$10.9m**
4	Corporate Fraud **£38m**	Prizes, Sweepstakes and Lotteries **$117m**	Remote access scams **A$9.8m**
5	Online Shopping and Auctions **£38m**	Internet Services **$94m**	Threats to life, arrest or other **A$8.9m**

An alarming feature of some imposter scams is for scammers to use threats to frighten victims into handing over money. Those threats include legal action, fines, arrest or deportation. This category was the second largest recorded by Australia's Scamwatch in the first seven months of 2021, with about 18,000 attempts during that time. Some 95% of the scam threats were made through phone calls. While only about 2% reported a financial loss, many more would have suffered from anger and stress at being targeted in this way.

Looking at the financial losses on frauds, investment scams accounted for 31% of total losses in the UK, 50% in Australia and 21% in the US. Investment scams incurred the largest average financial loss per fraud reported at $17,000 in the US and £25,000 in the UK.

ABOUT FraudSMART

FraudSMART is a fraud awareness initiative developed by Banking & Payments Federation Ireland (BPFI) in conjunction with the following member banks, Allied Irish Bank plc, Bank of Ireland, Barclays Bank Ireland, KBC Bank Ireland, PermanentTSB and Ulster Bank.

Launched in October 2017, the campaign aims to raise consumer and business awareness of the latest financial fraud activity and trends and provide simple and impartial advice on how best they can protect themselves and their resources.

For further information on the FraudSMART campaign, please contact info@FraudSmart.ie

ABOUT BPFI

Banking & Payments Federation Ireland (BPFI) is the voice of banking and payments in Ireland. Representing over 70 domestic and international member institutions, we mobilise the sector's collective resources and insights to deliver value and benefit to members, enabling them to build competitive sustainable businesses which support customers, the economy and society.

FraudSMART.

Informed. Alert. Secure.

FraudSMART is a fraud awareness initiative developed by Banking & Payments Federation Ireland (BPFI) in conjunction with AIB, Bank of Ireland, KBC Bank Ireland, PermanentTSB, Ulster Bank, An Post Money and Barclays.

Disclaimer Note: The information contained in this advisory is for information purposes only and is intended to enhance awareness and vigilance in this regard.

Follow us on: **@FraudSMART** **@FraudSMART**

www.FraudSMART.ie