PIMFA

The Personal Investment Management & Financial Advice Association

CURRENT FRAUD TRENDS – HOW TO PROTECT YOUR FIRM AND YOUR CUSTOMERS

CURRENT FRAUD TRENDS – HOW TO PROTECT YOUR FIRM AND YOUR CUSTOMERS

Fraud is a form of "criminal deception" – it's when someone deceives you into giving them your property (money, assets or other things of quantifiable economic value).

The main difference between fraud and theft is that a thief would take property from you without your consent, whilst a fraudster will deceive you into giving them the property.

Fraud has become one of the most frequent risks a financial institution has to deal with. Fraud can affect a firm in many ways, directly and indirectly: a firm can be the victim of fraud, or a customer can be the victim of fraud or, finally, a member of the public can be the victim of fraud by criminals who claim to be employed by or associated with the firm.

The Covid-19 pandemic has seen a growth in fraud and scams. The disruption caused to normal business processes and controls and working conditions, together with heightened consumer vulnerabilities has given malicious actors more opportunities to commit fraud. Scammers have taken advantage of the conditions created by the health crisis with a particular increase of impersonation fraud, online scams and fake investments promoted by search engines.

This paper will provide an analysis of real-life fraud events that have been experienced by PIMFA member firms, as well as resources that you can use to mitigate fraud risk for your business, your customers and your prospects.

FRAUD IN THE RETAIL INVESTMENT SECTOR – FEEDBACK FROM FIRMS

Based on the evidence provided by PIMFA member firms, the following types of fraud were observed:

Fraud against customers or prospects

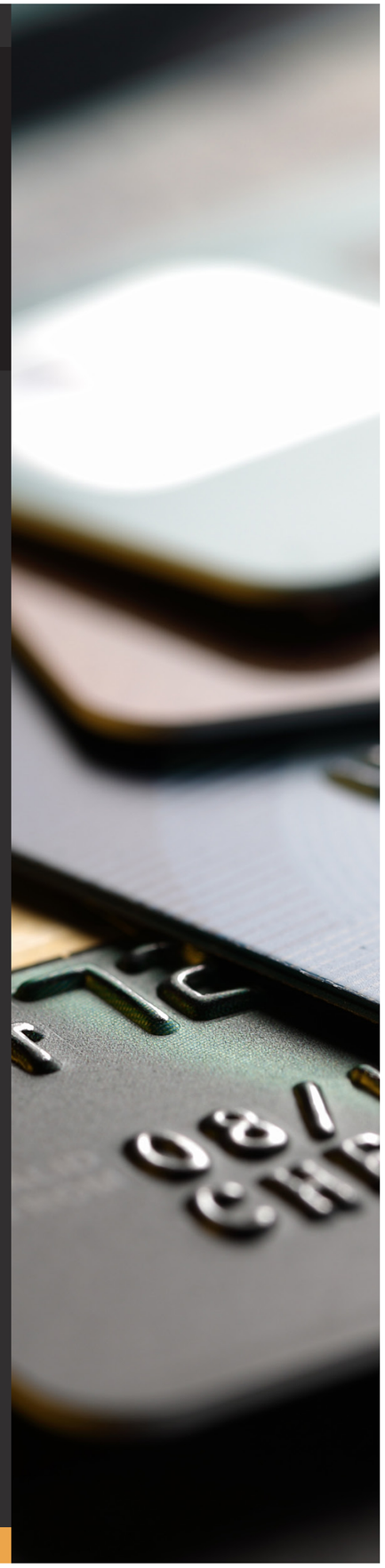
WEBSITE CLONING – this is a website that has the look and feel of that of a legitimate business, but is in fact run by criminals posing as the business. The site can look very professional.

How do you recognise a clone?

- Observe the URL – if you know the legitimate business's domain name and this is different, do not trust it. Many cloned websites have a URL which is very similar to the legitimate business's one, bar a typo or an additional word.
- Check the FCA warning list – firms notify the FCA when they find out that their website is being cloned, and the FCA keeps a register of these cloned websites. However, the website will not be in the register if the firm has not yet picked up that it has been cloned.
- Use the FCA financial services register of authorised businesses to find the legitimate contacts of the firm, call the firm and enquire about the website/investment that you have found. If the website is a clone, the firm will tell you so OR if it is a fresh clone that the firm is not yet aware of, they will notify the FCA.

What to do if you spot a clone

- Report the clone to the FCA on its Report a Scam page. The FCA will include it in the warning list.
- Report the clone to Action Fraud via this email address (Ref #OP'GIANTKIND (clones))
- Contact the website host and ask them to have the fraudulent website taken down. For UK website, a takedown notice from Action Fraud should compel the host to proceed with the takedown. For overseas hosts it may be a longer and more costly process.
- Fraudulent advertisements, whether attached to a clone website or not, can be reported to the Advertising Standards Agency



CLONE FIRM INVESTMENT FRAUD

Clone firms are fake firms set up by scammers using the name, address and 'Firm Reference Number' (FRN) of real companies authorised by the FCA. A spoof domain is created which resembles a legitimate firm email with some minor modifications, however a clone website is not created. Rather, once set up, these fraudsters will then send sales materials from the spoof email address whilst referencing the genuine websites of legitimate firms to dupe potential investors into thinking they are in contact with the legitimate firm when they are not.

Often, fraudsters will place adverts on social media platforms and search engines. Victims, some in search of a genuine investment opportunity, will then click on these adverts and be directed to a fraudulent website where they proceed to input their contact details and details of their enquiry. Action Fraud have reported that there are also instances of victims inputting their contact details into genuine price comparison websites and then being phoned by criminals purporting to be from a well-known, legitimate investment firm.

Once victims have registered their interest, they are contacted by the fraudsters, who often assume the names of genuine employees of investment firms and create seemingly legitimate company email addresses, but with very subtle changes. The fraudsters will use literature and branding that mirror those of the legitimate firms that they have cloned, as well as actively encourage investors to check the Firm Reference Number (FRN) on the FCA Register to sound as convincing as possible.

A cloned firm has no visibility of the cloned firm fraud at this stage. Liz Field, the chief executive of PIMFA, said such scams showed the increased sophistication of online fraudsters.

"It is a cause of deep frustration to our members and the regulator that they can do little more themselves to combat these criminals and prevent harm from being perpetuated, than report such frauds to internet service providers (ISPs), domain name registration services and online platforms," she said.

These measures are an important step, however, takedown can still prove difficult with some hosting companies, particularly in non-UK jurisdictions, refusing to take down domains as there is no associated website clone, rather just a holding page. A takedown notice from Action Fraud can assist resolve the situation with UK hosting companies.

Feedback from member firms shows that in these cases engaging a third party to help with brand protection and assist with the take down of spoof domain names can be beneficial.

IMPERSONATION THROUGH HACKED EMAILS

Scenario 1 – A client or associate's email is hacked and used to communicate instructions to transfer or withdraw funds. The fraudsters have accessed template payment instructions from previous emails within the hacked address, which include signatories and changing only the account number.

Scenario 2 – A client or associate's email is hacked and criminals use stolen personal details gathered from the hacked email account to impersonate the individual and request the financial institution to perform a static data change (e.g. home address, telephone number).

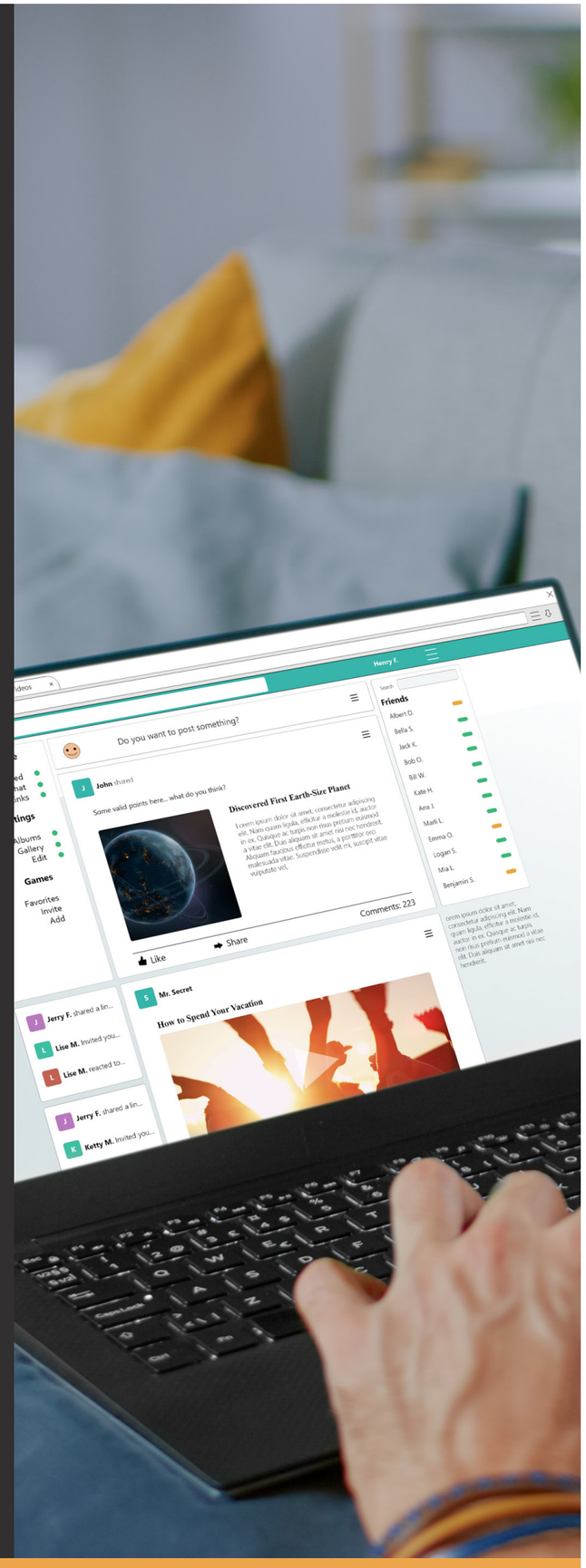
Scenario 3 – No hacking, but instruction is sent from clients to make payments or change bank details etc from an email address that appears to be from a recognised client.

Scenario 4 - Firms have also seen examples of "double-impersonation", with the fraudster hacking into the client's email and impersonating the firm with the client and the client with the firm. Here is an example: the client's email was hacked and the fraudster impersonated the client with the firm and asked for money to be moved. The fraudster then impersonated the firm with the client, responding to emails the client had sent to the investment manager and deleting the genuine emails that the investment manager was sending to the client. The fraud was discovered because the investment manager, not receiving a response from the client, decided to give them a call. Further to this experience, the firm has introduced a policy mandating investment managers to always call the client before moving money.

PHISHING

Phishing emails – fraudsters target consumers with spam emails, using genuine firms' details and offering 'investments opportunities'.

Phishing telephone calls - similar to the above, genuine firms' names are mentioned to encourage consumers to disclose personal information for the purpose of an alleged investment opportunity.



"NEW COURIER FRAUD" – this is when a customer is:

Contacted by telephone/email or both, by a scammer who claims to be from the Police, FCA, HMRC, the fraud/compliance department of their wealth manager, or even MI5 (a firm has recently experienced this one, and the fraud wasn't successful only because the wealth manager was incredibly diligent in detecting unusual client behaviour). Emails and calls appear entirely genuine and the scammers are highly skilled at impersonation.

Informed that they personally, or their wealth manager, are under investigation for a financial crime, breach of regulation/law, or part of a 'sting' operation to expose/arrest a certain organization/ person.

Threatened with further legal action or criminal prosecution if they do not withdraw all or part of their investment funds to their nominated bank account. From there they are further threatened and coerced via regular and often sinister ongoing contact into transferring the funds onward to a 'single use' international online holding account, where they are then withdrawn by the scammer and bounced around the system before being converted into cryptocurrency and therefore becoming effectively untraceable.

Pressurised not to disclose to their wealth manager the reason for the withdrawal and to insist it is 'their money' so they are not required to provide any detail, or say they are 'buying/renovating a property'.

This type of fraud does not appear to be very common, however, successful attempts tend to be high value and focus on wealthy and vulnerable clients. This modus operandi is so sophisticated it can well circumvent standard anti-fraud controls given the funds are initially withdrawn into their mandated and verified bank account.

Firms can work on both staff and customer awareness to successfully prevent or stop this type of fraud.

As seen under points 3 and 4 above, fraudsters can be very convincing and put a real sense of urgency onto the victim. Victims of these types of fraud will act out of character and ask to withdraw funds quickly without giving explanations. Staff needs to be trained to help these individuals understand that they are a victim of fraud and make them feel safe.

On the other hand, customers need to be made aware that public authorities will never call an individual and ask them to withdraw their money. It just does not happen. This fraud can be particularly damaging to vulnerable customers who may fall for the fraudster's claims of authority, so extra care should be taken with regard to these customers.

POST INTERCEPTION

Fraudsters intercept customers' post and steal personal information. They use that information to pose as the client with the firm and e.g. change customer settings/gain access to online portal. Firms are an important blocker of these frauds. A process should be in place to ensure the customer is notified of changes to their online settings.

FRAUD AGAINST A FIRM

CEO FRAUD – this is fraud perpetrated against a firm to steal their money. A fraudster pretends to be the CEO and sends an email/calls an individual asking them to make a payment into a new bank account and not to be contacted because they are busy. Phone numbers and email addresses can be spoofed, and so can be the CEO's voice thanks to "deep fake" technology. Therefore, it is important that staff remain vigilant and that a procedure is in place to minimise the risk of losing money to these types of fraud.

INVOICE FRAUD AGAINST THE FIRM

Scenario 1 – a fraudster posing as a supplier and presenting an invoice looking like that of the supplier at a time when the supplier invoice may be expected.

Scenario 2 – the genuine supplier's email gets hacked so the firm receives a fraudulent invoice from the genuine supplier account.

Scenario 3 – Invoice interception: this is most effective with new suppliers. The invoice is intercepted before reaching the customer, and it is re-issued by fraudsters with changed bank details.

- Look out for the supplier bank details in the invoice. If different from those usually provided, contact the supplier directly and enquire. When paying a supplier for the first time, contact them and verify their bank details.
- Do not use contact details on the invoice as if the invoice is fake chances are the contacts are fake too.
- Put in place a process aimed at mitigating the risk of money leaving the firm unchecked – for example:
    - Introducing processes requiring the person processing the payment speak to the person requesting the payment – either in person or via video call – to confirm the instructions.
    - "Three-way-matching" or third person verification for fund movements can help mitigate fraud risk.

GOOD PRACTICE FOR FIRMS: IDENTITY AND VERIFICATION

With regard to systems and controls to prevent these forms of fraud, firms might wish to consider the following Identification & Verification (ID&V) best practice points provided by our membership:

- Reduce or where possible remove email as a means for clients (or internal functions) to communicate transactional instructions
- Require client transaction instructions to be submitted:
    - Clients - Via a secure messaging portal that is only accessible via two-factor authentication
    - Internal – Via a secure instant messaging service, backed up with a verification phone call to the requester (regardless of seniority)
- Follow up all client transaction instructions with a verification call, requiring two-level identity verification, for example:
    - Address/Postcode, DoB and an allocated PIN, plus
    - Account activity-specific security questions (i.e. known only to the client)
- Provide regular anti-fraud training to all staff who handle transactions, including how to identify suspicious activity and report it via the MLRO. Examples of such activity include:
    - Overseas/unrecognised number on caller ID
    - Request to pay away to new/different bank account
    - Reluctance to provide a reason for the transaction
    - Eagerness to process quickly/pressure to avoid questions or security measures

Staff must be made aware that 'tipping off' is a criminal offence, how this is defined and the potential sentences

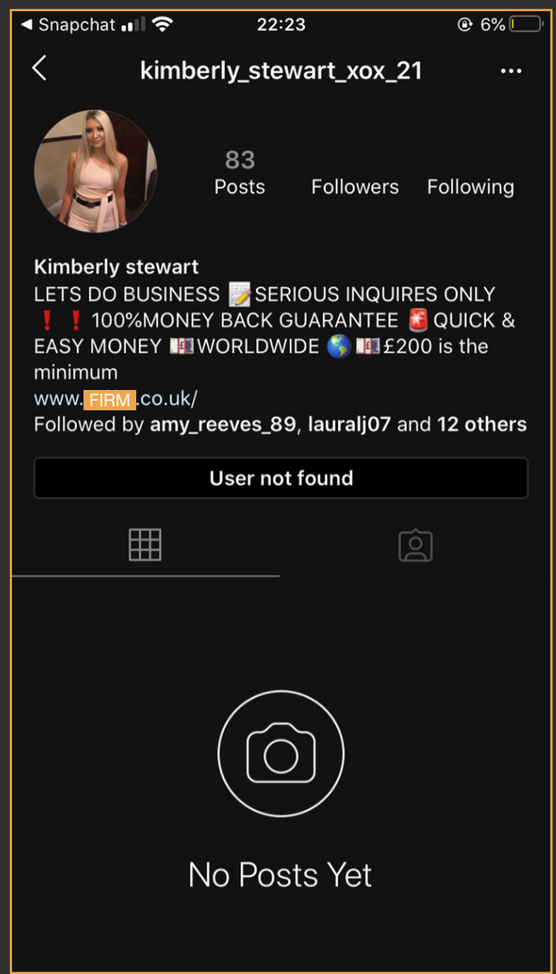
REAL LIFE FRAUD SCENARIO ANALYSIS

Based on the evidence provided by PIMFA member firms of SOCIAL MEDIA FRAUD

Below is an example of a fraudulent post that was found on social media. Feedback from PIMFA firms shows that these types of post are getting more and more common. Fraudsters are exploiting social media platforms to spam their fraudulent offerings to the public. Social media platforms are an easy target for fraudsters as they have a very wide reach into people's life and they are mainly automated, which means that the fraudulent accounts may take some time before being picked up and taken down. Also, once a fraudulent account is taken down, fraudsters can easily create a new account and continue their activities.

This is why it is very important both for businesses and customers to keep vigilant and not fall for these scams.

Look at this example of fraudulent account:



What can we see that we should be looking out for?

Glamorous profile photo – probably stolen from an unsuspecting model

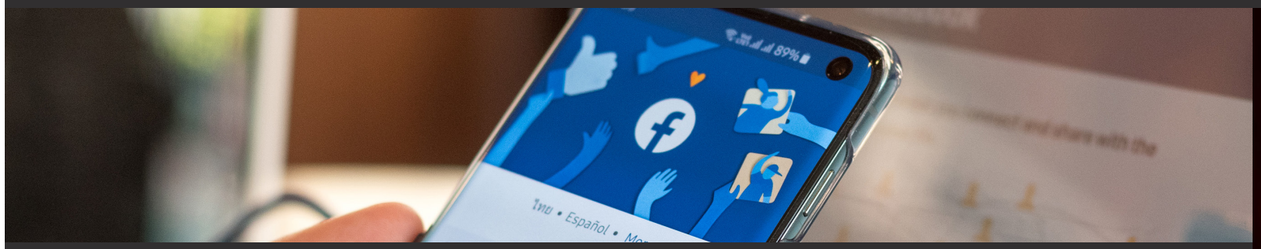
Name written in a hurry – surname is not in capital letters – may indicate that the account was opened quickly and "not there to stay"

Advertising glamorous lifestyle – "look at me, you can have this too"!

Advertising "quick and easy money" – there is no easy money, do not fall for it. Making money, especially a lot of money, is usually not easy nor quick.

Look at the profile page – the account info says this person has posted 83 times so far, yet all posts have been deleted. Considering the profile information, this should raise suspicion.

Look at the bottom line of the account info – there is the website of a legitimate business. This person claims to be somewhat connected to a legitimate business. However, a legitimate business would never advertise their services this way. A legitimate business would never claim to be able to make "quick and easy money" to their customers.



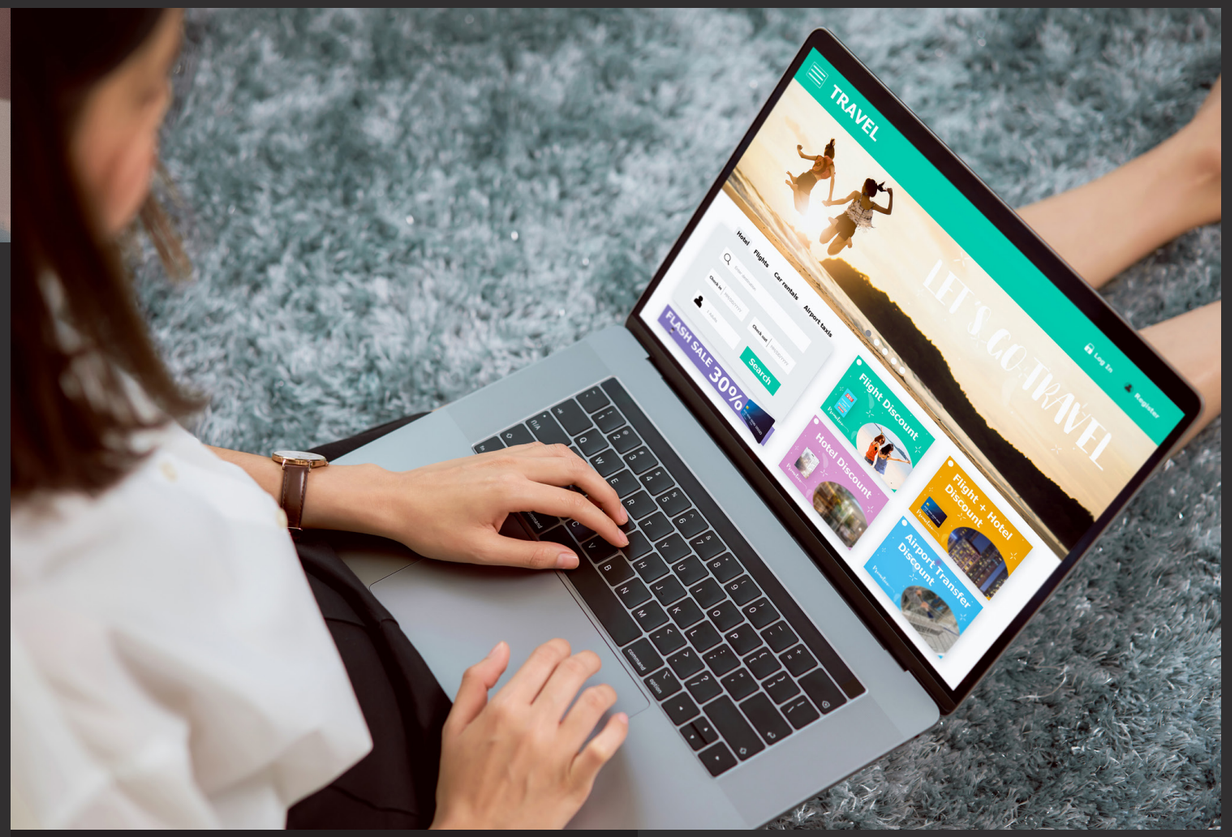
So, what to do when faced with such posts?

For customers:

- Do not believe the posts, do not contact the account holder: fraudsters can be quite persuasive and your risk of becoming a victim of fraud will increase if you contact them.
- Posts containing the following hashtags - the City of London Police has identified them as most likely to be fraudulent or criminal in nature:
    - #Moneyflipsuk
    - #Mflipssss
    - #Deetsandflips
    - #Deetsandflipping
    - #legitmoneyflips
    - #flipsanddeets
    - #PayPalFlip
    - #RealMoneyTransfers
    - #UkFlips
    - #EasyMoney
- If the post contains references to a legitimate business, contact the business through the contact details provided in the FCA register and enquire about the post.
- Report the post to the Advertising Standards Agency through this website:
- Report the account to the social media platform using the dedicated functions – the more people report the account, the more the platform's algorithm will prioritise it for review
- Report to Action Fraud – through the Action Fraud Portal (you can find this on the Action Fraud website). Remember: every report matters

For firms:

- Unfortunately, social media platforms do not allow search by website, so you will have to search accounts/posts using common fraudulent/criminal hashtags such as the following ones identified by the City of London Police (same as for customers):
    - #Moneyflipsuk
    - #Mflipssss
    - #Deetsandflips
    - #Deetsandflipping
    - #legitmoneyflips
    - #flipsanddeets
    - #PayPalFlip
    - #RealMoneyTransfers
    - #UkFlips
    - #EasyMoney
- When you find or are alerted of a fraudulent account/post by a customer or member of the public, report the account/post to the social media platform.
- Report the post to the Advertising Standards Agency
- If the account/post references your firm, report it to Action Fraud – through the Action Fraud Portal (on the Action Fraud website)
- You can report more general patterns and trends by emailing NFIB-Intelligence@cityoflondon.pnn.police.uk for intelligence submissions / sharing intelligence reports
- Report to the FCA. The FCA keeps a register of clone website. Whilst this is not strictly a clone, the more information they receive about these activities the more they will learn about them and think about them. To inform the FCA please email the FCA's Supervision Hub at firm.queries@fca.org.uk. This page also links to a live chat function. Firms can also call the FCA on 0300 500 0597 from the UK, or +44 207 066 1000 from abroad. The lines are open Monday, Tuesday, Wednesday and Friday 9am to 5pm, and Thursday 9.45am to 5pm.



RETAIL BOND FRAUD – FIRM SCENARIO 1

The fraudsters established a website cloning the logo, look and feel of that of a legitimate business; they then ensured that their website would feature highly in search engine results when members of the public entered queries on fixed income investments, for example '12 month bond'. The website promoted retail bonds of a household brand with a 7.5% annual coupon. Members of the public would then click on the link and end up on the cloned website. The website required them to enter their contact details (this was the only functionality of this site). An individual would then contact the member of the public, encouraging them to invest in the bond – the individual would be pertaining to be calling from the legitimate business – in fact, fraudsters pretended to be real members of staff during the call. Fraudsters managed to pose as real members of the firm's staff by accessing firm website's public domain area and taking staff details. Members of the public would then invest in these fraudulent bonds and therefore lose their money.

The fraud was identified due to the firm's call centre staff being contacted by members of the public, looking to ascertain if the offer was legitimate. Once the fraud was identified, the firm updated their website with warnings of the scam, providing guidance and support to those who had been contacted. The firm also ensured that they were in the top results for Google under certain searches and partnering with the company whose bonds were impersonated in getting the website closed down.

The firm worked out that the largest loss identified was £50,000. However, they also managed to prevent most of the victims' assets from being taken: out of around 40 individuals who had been contacted, the firm identified only 2 who lost money. This amounted to saving over £1 million from the fraudsters.

RETAIL BOND FRAUD – FIRM SCENARIO 2

During 2020 the firm has been aware of a number of sophisticated online scams which are targeting two of their group brands.

Summary

Consumers are being targeted by a sophisticated investment scam whereby (predominantly older) investors are coerced into investing into fictitious investment products in the belief that they are transacting with the firm. Fraudsters have cloned ISA/bond literature, created fake corporate email domains, spoofed corporate websites and used the names of some the firm's genuine employees to add credence to the scam.

To date the impact on consumers has been severe. To date the firm is aware of 220 victims of the scam, 60 of these victims have lost over £1.2m to the scam and hundreds more have provided identity documents and banking information which could be used for fraudulent purposes in the future. The success rate of this scam appears to be particularly high.

Scam Initiation

A large proportion of victims referred to having clicked on ads via social media, search engines or well-established comparison websites (e.g. Go Compare). Additionally, a number of victims confirmed that they submitted contact details to lesser-known comparison or lead generation websites, enticed by attractive investment returns on offer. Once contact details are submitted victims are contacted by the fraudsters shortly afterwards.

Use of employee names

To add further credence to the scam, the fraudsters use the names of existing or previous employees of the firm when corresponding with victims. We believe that the names and titles have been harvested from LinkedIn profiles. Victims have reported checking LinkedIn or contacting our switchboard to validate the names provided before investing.

Use of branding and intellectual property

Throughout the investment process, victims are provided with falsified product literature, including prospectuses, application forms and contract notes. The documents use the firm's branding and whilst they often refer victims to genuine corporate websites, all correspondence is directed to scam telephone lines or fake corporate email domains

Bank accounts – proceeds of crime

Approximately 35 bank accounts have been used to launder the proceeds of this scam. Where possible the banks have been contacted to inform them that they are in receipt of the proceeds of crime and to encourage them to freeze the accounts and disclose the activity to the NCA. However, a number of institutions used to facilitate payments are not traditional high street banks, but banking platforms or fintech banks.

Scam identification

We have found that individuals generally start to become suspicious of the investment where they have been unable to get in contact via the number or email provided (probably because these have been taken down by the firm through their investigations) or 3-6 months after they have paid away funds and have not received a hard copy of their contract note. In a number of instances the victim has not been aware until they contact the firm for an update on their investment.

Impact on victims

As mentioned above many of the victims are elderly and are looking to invest their life savings and on a number of occasions the firm has been made aware that the victim has actually been looking to invest inheritance from a loved one who has passed away (a number of these have passed due to COVID 19). When the victims find out they have been a victim of a scam they are understandably devastated and find the situation hard to comprehend, with some not knowing what they are going to do or how they are going to tell other family members what has happened. The firm does provide guidance on who to contact if they feel vulnerable e.g. Victim Support/Samaritans but many may be too embarrassed and upset to admit what has happened.

BLOOMBERG FRAUD

The firm was contacted by a member of the public who was looking to ascertain the legitimacy of a borrowing note in the name of the firm, which they had been offered by individuals pertaining to call from Bloomberg. The victim was also offered an HM Treasury Gilt. Having spoken to the individual, the firm understood that they had been searching for investments on the internet and identified a website via the search engine results which they clicked upon.

They then must have entered their contact details onto this website and were contacted originally in June 2020 by an individual from the "Bloomberg Trading Facility" who was offering a UK Gilt paying 8% (GB0009997999).

The individual was then contacted at a later date by an individual pertaining to be from Bloomberg who sent them a factsheet about a 6.95% Fixed Rate Note – again, in the name of the firm – looking to get them to invest.

The note is a real instrument, however not suitable for retail investors. The firm worked out this was a scam and that the fraudsters would claim to sell victims a real instrument, but instead take the individual's money.

With regard to the firm being represented as the broker (Bloomberg) there were two firms which the fraudsters impersonated:

- Bloomberg Index Services Limited (Reference number: 829278) – this is a real firm – indeed checking permissions the firm's is "Administering a Benchmark".
- Bloomberg Trading Facility B.V. (Reference number; 832477) – On the product information, there are details of a Bloomberg Trading Facility B.V. This is a recently established trading platform firm which is passporting into the UK from Holland.

The firm reached out to Bloomberg and they managed to shut the cloned websites down. Bloomberg were aware of these instances and had already been trying to get them closed down.

For firms:

- If your firm's brand is being used to commit impersonation scams like the ones listed above, and if fraudsters are also impersonating another business or an instrument issued by another business, consider working together with this company to have the cloned websites shut down
- It is good practice to help fraud victims, even if they are not your customers. They are people who would have invested with you, and may still do so if you help them recover their money.

For customers:

How do you spot an impersonation fraud?

Impersonation fraud can be very hard to spot. A cloned website can look exactly like the real one, and the products on offer there can be from recognisable brands and very attractive financially.

Here are a few tips:

- Follow the tips above under the identification of a cloned website
- Investments that carry an unrealistic rate of return are either fake or not suited to the retail mass market. If you are an investor looking to invest in high risk instruments do so by calling a reputable firm and getting proper advice.
- If you receive a cold call about an investment, do not give your details to the caller. Put the phone down and contact the firm through the details contained in the FCA register.
- If you see a financial promotion from an investment firm on the internet, do not just input your details: use the FCA register, contact the firm through the details provided there and enquire about the promotion this way.

CLONE FIRM INVESTMENT FRAUD

The firm first became aware of a scam circulating using their name when they were contacted by an individual requesting to purchase a bond on an execution-only basis. When the dealer quoted the current market price for the client, they expressed his surprise and asked why they could not purchase the bond at the price quote in the documents that the firm had sent them. This triggered some alarm bells, as the firm does not produce marketing material of this type and on further questioning about who sent the client such documents, they named an individual working in the firm's wealth management subsidiary company and who would not normally have any involvement in this type of investment. At this point, the dealer asked if the client could send them a copy of the correspondence received. This was done by copying the email and attaching it to a new email as the firm found out that if the client simply forwarded the email, it was not received by the firm: the client's email had somehow been hacked as well.

Following some discussions with the client, they told the firm that they had found the scam firm online. Further investigations identified that the fraudsters had purchased a domain name very similar to the firm's legitimate one and that, by clicking on this link, it forwarded the user to the firm's own website, making it seem legitimate.

Shortly after the call above, an ex-client of the firm called asking if they could check that the firm's bank details were correct. Following some further conversations, it came to light that the contact telephone number this person had been given was not the firm's telephone number and that the employee contact name provided by the fraudsters was of someone on long-term sick leave. Unfortunately this person had already invested £30,000 before they became suspicious. They gave the firm all the information they held, including the bank details they had transferred the money to and the firm was able to notify the bank who very quickly put a hold on the account. The firm believes that the bank has been able to return the money to the victim.

RESOURCES

The Action Fraud website is a treasure trove of information on fraud, news and data https://www.actionfraud.police.uk/

FCA Financial Crime Guide

The FCA Financial Crime Guide FG4 contains guidance on fraud systems and controls, including good and bad practice examples. Given that this is regulator-made guidance, it is the starting point for the creation of a firm's fraud risk function. The examples are very high level so they would need to be adapted to the reality of the firm. FG4 also contains links to other bodies that can provide additional information and guidance on fraud.

https://www.handbook.fca.org.uk/handbook/FCG/4/?view=chapter

FCA ScamSmart page

This page contains a wealth of advice for consumers. It can be used to build customer fraud prevention training https://www.fca.org.uk/scamsmart

NCSC Cyber Aware Campaign to stay safe online

https://www.ncsc.gov.uk/cyberaware/home

Met Police Little Book of Big Scams

https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/the-little-book-of-big-scams.pdf

UK Finance "Take Five" materials

UK Finance has published a number of fraud sources. They are created for banks, but there are interesting materials that can apply across the board too.

Take Five to Stop Fraud website: www.takefive-stopfraud.org.uk

Take Five toolkit https://takefive-stopfraud.org.uk/toolkit/

Advice (General): https://takefive-stopfraud.org.uk/advice/general-advice/

Advice (Businesses): https://takefive-stopfraud.org.uk/advice/business-advice/

Advice (Romance): https://takefive-stopfraud.org.uk/advice/general-advice/romance-scam/

Advice (Investment Scams): https://takefive-stopfraud.org.uk/advice/general-advice/investment-scam/

Fraud the Facts - https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2020

UK Finance – 2020 Half Year Fraud Update - https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/2020-half-year-fraud-report

PIMFA

The Personal Investment Management & Financial Advice Association