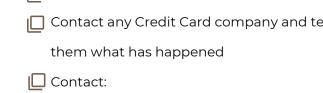## What next?
# POST FRAUD CHECKLIST

## ⚠ PRIORITY

- ☐ Contact your bank/credit card company and report the fraud
- ☐ Report to Action Fraud (UK) and your local police
- ☐ Personal documents, contact departments to notify
- ☐ Secure your number, email and social media accounts

## 🏛 BANKS/CARDS:

- ☐ Phone your bank to alert them to the fraud and secure your accounts
- ☐ Contact:
- ☐ Contact any Credit Card company and tell them what has happened
- ☐ Contact:

## LAW ENFORCEMENT:

- ☐ Action Fraud No:

- ☐ Local Police Ref No:

## PERSONAL DOCUMENTS:

- ☐ Passport
- ☐ Driving Licence
- ☐ National Insurance Number
- ☐ SS card details (USA)
- ☐ ID.me (USA)

## CONTACT & PLATFORMS:

- ☐ Block their number on all platforms
- ☐ Block all associated contacts numbers
- ☐ Block emails
- ☐ Secure and make private, all social media profiles
- ☐ Remove and profiles added around the time of your scammer

# POST FRAUD CHECKLIST

## 🔒 SAFEGUARDING FOR THE FUTURE:

These criminals will always try to come back as long as they have your contact details. They will likely also sell your information to other criminals

- ☐ Get a new phone number
- ☐ Get a new email
- ☐ Change Usernames and profile links on social media
- ☐ Read about 'Follow Up and Recovery Scams' on this link www.catchthecatfish.com

# POST FRAUD CHECKLIST

## £ REIMBURSEMENT:

- ☐ In certain situations, the banks in the U.K, may be able to reimburse you for certain transactions
  - The CRM (Contingent Reimbursement Model) is now mandatory through PSR (Payment Systems Regulator's reimbursement rules. Dates apply for each type.
  - Transfers made from your account to another account should be refunded, if the bank did not do enough to notify you that the payments could be fraudulent (sometimes when they did and didn't stop the payment)
  - The Financial Ombudsman find that most customers did not show gross negligence

Letter templates on the website (or we cn help you).