



Scam and Fraud Reporting Form

Personal characteristics

Age of victim

- ☐ 18-19 years
- ☐ 20-29 years
- ☐ 30-39 years
- ☐ 40-49 years
- ☐ 50-59 years
- ☐ 60-69 years
- ☐ 70 years and over
- ☐ Prefer not to answer / Unknown

Sex and/or gender of victim

- ☐ Male ☐ Female
- ☐ Prefer not to answer / Unknown

Employment status of victim

- ☐ In paid employment [e.g. work for someone else]
- ☐ Self-employed [e.g. work for yourself / own a business]
- ☐ Retired
- ☐ Looking for work [Unemployed]
- ☐ Not working and not looking for work
- ☐ Student
- ☐ Other



Marital status of victim

- ☐ Single
- ☐ Married/common-law
- ☐ Divorced/ separated
- ☐ Widowed

Highest level of education completed by victim

- ☐ Primary school education or vocational school without secondary school course
- ☐ Secondary (complete secondary education)
- ☐ Tertiary (Bachelor's degree or higher professional education)

Language most frequently spoken at home by victim

- ☐ National official language
- ☐ Other Click or tap here to enter text.

Other relevant socio-demographic information, e.g. disability, recipient of income support and/or social security:

Contact or medium form

Victims were first reached via:

- ☐ Applications (apps)
- ☐ E-mail
- ☐ In-person
- ☐ Mail fraud
- ☐ Phone call
- ☐ Social media message

**Scheme or modus operandi**

- ☐ SMS or text message
- ☐ Online advertisements/websites
- ☐ TV or radio advertisements
- ☐ Fax
- ☐ Other Click or tap here to enter text.

What was (were) the tactic(s) of the fraudster or scammer to trick victims?

- ☐ Advanced fee/recovery scam
- ☐ Authorised push payment (APP) scam
- ☐ Biometric ID fraud
- ☐ Blackmail, threat or extortion scams (including ransomware or malware attacks)
- ☐ Charity and disaster scams
- ☐ Dating and romance scams
- ☐ Debt settlement, or debt relief scams
- ☐ Elder fraud (e.g. scams targeting seniors)
- ☐ Easy or cost-free credit scams
- ☐ Identity theft
- ☐ Investment scams (including cryptoasset scams)
- ☐ Insurance fraud
- ☐ Jobs and employment scams (i.e. recruitment fraud)
- ☐ Mobile app fraud
- ☐ Money mule scams
- ☐ Mortgage fraud, including mortgage closing scams



- ☐ Fraudsters posing as real states developers, SACCO/village promoters and governments social protection recruiters
- ☐ Online auction scams
- ☐ Pension scams
- ☐ Pet scams (e.g. scammers posing as pet breeders)
- ☐ Ponzi schemes
- ☐ Sale of non-existent goods or services Financial product(s) or service(s) targeted:
- ☐ Scammers posing as banks, financial advisers, or other financial services providers
- ☐ Scammers posing as representatives of the government or official entities (e.g. revenue services, social assistance)
- ☐ SIM swapping
- ☐ Skimming (when devices illegally installed on ATMs, point-of-sale terminals, or fuel pumps capture data or record cardholders' PINs)
- ☐ Student financial aid scams
- ☐ Travel or vacation scams
- ☐ Tricking consumers to provide personally identifiable information [phishing (online), vishing (over the phone) or smishing (through SMS)]
- ☐ Unexpected money scams (e.g. lottery scams)
- ☐ Other Click or tap here to enter text.

Choose all that apply. Note that this list is broken down by product or service sector (i.e. banking and payments, consumer credit, insurance, investments, and pensions).

Sector Product or service Banking and payments

- ☐ Transaction account
- ☐ Savings account
- ☐ Debit card



- ☐ Mobile money
- ☐ E-money
- ☐ Cross-border transactions (including remittances)
- ☐ Push payments (customerinitiated transfers)
- ☐ Instant payments
- ☐ Account information services
- ☐ Digital wallet
- ☐ Super app (including ecommerce platform)
- ☐ Other product or service Click or tap here to enter text. Consumer Credit
- ☐ Personal loans
- ☐ Buy Now, Pay Later
- ☐ Overdraft facilities
- ☐ Car loans/auto financing
- ☐ Salary advance/earned wage access
- ☐ Payday lending
- ☐ SME loans
- ☐ Peer-to-peer lending
- ☐ Credit cards
- ☐ Other product or service
- ☐ Mortgages/home loans Insurance
- ☐ Life insurance
- ☐ Home buildings insurance
- ☐ Home contents insurance



- ☐ Motor insurance
- ☐ Travel insurance Click or tap here to enter text.
- ☐ Home loan/Mortgage protection insurance
- ☐ Funeral or burial insurance
- ☐ Gadget insurance (e.g. electronic items)
- ☐ Other product or service
- ☐ Health insurance
- ☐ Credit protection insurance (not including home loans/mortgages) Investments
- ☐ Managed funds
- ☐ Equity
- ☐ Sustainable financial products (e.g. sustainable or “green” stocks, bonds and funds)
- ☐ Cryptocurrency/digital assets Click or tap here to enter text.
- ☐ Unit-linked insurance (including hybrid products)
- ☐ Retail/self-directed online investment platforms
- ☐ Derivatives trading
- ☐ Financial advice/advisory services
- ☐ Other product or service Click or tap here to enter text. Pensions
- ☐ Peer-to-peer lending platforms
- ☐ Crowdfunding
- ☐ Management of assets
- ☐ Benefits payments
- ☐ Financial advice
- ☐ Support to transfer assets



☐ Provision of information to members (e.g. account statements) Method of payment or investment

How was the money transferred?

- ☐ Cash
- ☐ Gift cards
- ☐ Crypto assets (including Central Bank Digital Currency)
- ☐ Debit cards
- ☐ Electronic or wire transfers
- ☐ Mobile payments (including QR payments)
- ☐ Other Click or tap here to enter text.

Fraud detection

Who initially detected the fraud?

- ☐ Consumer
- ☐ Financial services provider
- ☐ Law enforcement
- ☐ Financial Authority
- ☐ Other Click or tap here to enter text.

If the consumer detected the fraud, how did they detect it?

- ☐ Unusual transactions
- ☐ Loss of funds
- ☐ Other Click or tap here to enter text.

If the financial services provider detected the fraud, how did they detect it?

- ☐ Unusual transactions



- ☐ Loss of funds
- ☐ Two-factor authentication procedures
- ☐ Other Click or tap here to enter text. Recovery status of funds

What was the total amount of financial loss incurred by the consumer? [Include all funds lost before any recovery or reimbursement]: _____

Were any of the original funds lost to the financial scam or fraud recovered and returned to the consumer (e.g. through transaction reversal, clawback, seizure or investigation)?

- ☐ Yes, fully reimbursed
- ☐ Yes, partially reimbursed
- ☐ Unable to recover funds

If unable to recover funds, please indicate if this is due to gross negligence from the consumer:

- ☐ Due to gross negligence

Were any funds refunded or reimbursed to the consumer by a bank, payment provider, merchant or other entity (e.g. due to liability, policy, statutory obligation)?

- ☐ Yes ☐ No

If yes: Amount refunded/reimbursed:

Refunding entity:

- ☐ Bank
- ☐ Payment provider
- ☐ Merchant
- ☐ Other:



Click or tap here to enter text. Basis of reimbursement (if known):

- ☐ Statutory obligation
- ☐ Policy/goodwill
- ☐ Liability determination
- ☐ Other:

Click or tap here to enter text.

Nature of authorisation

Was there a consumer authorization mechanism in place for the transaction/interaction?

- ☐ Yes ☐ No

If yes, who authorised the transaction/interaction?

- ☐ Account/product holder
- ☐ Authorised representative
- ☐ Fraudster
- ☐ Other Click or tap here to enter text.

Status of entity (if applicable)

What type of fraudster was involved?

- ☐ Individual/ third-party
- ☐ Entity

Was the financial services provider involved licensed/authorized to carry out the activity in the jurisdiction where the fraud took place?

- ☐ The entity was fully licensed to operate for the activity related to the fraud, in the jurisdiction where the fraud took place
- ☐ The entity was licensed to operate for some activities in the jurisdiction, but not the activity related to the fraud



☐ The entity was not licensed to operate in the jurisdiction where the fraud took place, but is authorised in another jurisdiction

☐ The entity was fictitious (e.g. the entity is neither licensed to operate in the jurisdiction where the fraud took place nor another jurisdiction)

If the financial services provider is licensed elsewhere, was the fraud carried out by a third-party fraudster?

☐ Yes

☐ No



诈骗和欺诈申报表格

个人特征

受害者年龄

☐ 18-19 岁

☐ 20-29 岁

☐ 30-39 岁

☐ 40-49 岁

☐ 50-59 岁

☐ 60-69 岁

☐ 70 岁及以上

☐ 不愿回答/未知

受害者性别

☐ 男性

☐ 女性

☐ 不愿回答/未知

受害者就业状况

☐ 有偿就业 [例如：受雇于他人]

☐ 自雇/个体经营 [例如：为自己工作/拥有企业]

☐ 退休

☐ 正在找工作 [失业]

☐ 未工作且未找工作

☐ 学生



☐ 其他

受害者婚姻状况

☐ 单身

☐ 已婚/事实婚姻

☐ 离婚/分居

☐ 丧偶

受害者最高学历

☐ 小学教育或无中学课程的职业学校

☐ 中学（完成中学教育）

☐ 高等教育（学士学位或更高专业教育）

受害者家中主要使用的语言

☐ 国家官方语言

☐ 其他（请在此输入文本）

其他相关社会人口统计信息，例如：残疾状况、领取收入补助和/或社会保障金情况：

联系方式或接触渠道

首次接触受害者的途径：

☐ 应用程序 (App)

☐ 电子邮件

☐ 面对面

☐ 邮寄诈骗

☐ 电话



☐ 社交媒体信息

☐ 短信 (SMS)

☐ 在线广告/网站

☐ 电视或广播广告

☐ 传真

☐ 其他（请在此输入文本）

欺诈者或骗子诱骗受害者所使用的手段：

☐ 预付费/追回款项诈骗

☐ 授权转账支付 (APP) 诈骗

☐ 生物识别身份欺诈

☐ 勒索、威胁或敲诈诈骗（包括勒索软件或恶意软件攻击）

☐ 慈善和灾难捐赠诈骗

☐ 约会和恋爱诈骗

☐ 债务清偿或债务减免诈骗

☐ 针对老年人的欺诈 (例如：专门针对长者的骗局)

☐ 轻松或免费信贷诈骗

☐ 身份盗用

☐ 投资诈骗（包括加密资产诈骗）

☐ 保险欺诈

☐ 求职与就业骗局（即招聘欺诈）

☐ 移动应用程序欺诈

☐ “钱骡”骗局



- ☐ 按揭贷款欺诈（包括按揭交割环节的骗局）
- ☐ 诈骗者冒充房地产开发商、储蓄信贷合作社（SACCO）/村级项目推广人或政府社会保障招聘人员
- ☐ 网络拍卖骗局
- ☐ 养老金骗局
- ☐ 宠物骗局（例如诈骗者冒充宠物繁育者）
- ☐ 庞氏骗局
- ☐ 出售不存在的商品或服务 涉及的金融产品或服务：
- ☐ 诈骗者冒充银行、理财顾问或其他金融服务提供商
- ☐ 诈骗者冒充政府或官方机构代表（例如税务部门、社会救助机构）
- ☐ SIM 卡置换（SIM swapping）
- ☐ 盗刷/侧录（在 ATM、POS 机或加油泵上非法安装设备以获取数据或记录持卡人 PIN 码）
- ☐ 学生经济援助骗局
- ☐ 旅行或度假骗局
- ☐ 诱骗消费者提供个人身份信息 [网络钓鱼 (phishing)、语音钓鱼 (vishing) 或短信钓鱼 (smishing)]
- ☐ 意外之财骗局（例如彩票中奖骗局）
- ☐ 其他 请在此处输入文本。



请选择所有适用项。

注意：此列表按产品或服务领域（即银行与支付、消费信贷、保险、投资及养老金进行分类。领域 产品或服务 银行与支付

- ☐ 交易账户
- ☐ 储蓄账户
- ☐ 借记卡
- ☐ 移动货币
- ☐ 电子货币
- ☐ 跨境交易（包括汇款）
- ☐ 推送式支付（由客户发起的转账）
- ☐ 即时支付
- ☐ 账户信息服务
- ☐ 数字钱包
- ☐ 超级应用（包括电子商务平台）
- ☐ 其他产品或服务 请在此处输入文本。 消费信贷 ☐ 个人贷款
- ☐ 先买后付 (BNPL)
- ☐ 透支服务
- ☐ 汽车贷款/汽车金融
- ☐ 预支工资/已赚工资支取
- ☐ 发薪日贷款
- ☐ 中小企业 (SME) 贷款
- ☐ 点对点 (P2P) 借贷



- ☐ 信用卡
- ☐ 其他产品或服务
- ☐ 按揭/住房贷款 保险
- ☐ 人寿保险
- ☐ 房屋建筑保险
- ☐ 房屋财产保险
- ☐ 汽车保险
- ☐ 旅行保险 请在此处输入文本。
- ☐ 住房贷款/按揭保障保险
- ☐ 丧葬保险
- ☐ 电子设备保险（如电子产品）
- ☐ 其他产品或服务
- ☐ 健康保险
- ☐ 信贷保障保险（不包括住房贷款/按揭） 投资
- ☐ 管理型基金
- ☐ 股票/权益类投资
- ☐ 可持续金融产品（如可持续或“绿色”股票、债券和基金）
- ☐ 加密货币/数字资产 请在此处输入文本。
- ☐ 投资连结型保险（包括混合型产品）
- ☐ 零售/自主型在线投资平台
- ☐ 衍生品交易



☐ 财务建议/咨询服务

☐ 其他产品或服务 请在此处输入文本。 养老金 ☐ P2P（点对点）借贷平台

☐ 众筹

☐ 资产管理

☐ 福利金发放

☐ 财务建议

☐ 资产转移支持

☐ 向会员提供信息（如账户对账单） 支付或投资方式

资金是如何转移的？

☐ 现金

☐ 礼品卡

☐ 加密资产（包括央行数字货币）

☐ 借记卡

☐ 电子转账或电汇

☐ 移动支付（包括二维码支付）

☐ 其他 请在此处输入文本。

欺诈检测

谁首先发现了欺诈行为？

☐ 消费者

☐ 金融服务提供商

☐ 执法部门

☐ 金融监管机构



☐ 其他 请在此处输入文本。

如果是消费者发现了欺诈行为，他们是如何发现的？

☐ 异常交易

☐ 资金损失

☐ 其他 请在此处输入文本。

如果是金融服务提供商发现了欺诈行为，他们是如何发现的？

☐ 异常交易

☐ 资金损失

☐ 双重认证

身份验证程序

☐ 其他（请在此处输入文本） 资金追回情况

消费者遭受的经济损失总额是多少？

[包括在任何追回或补偿之前的全部损失金额]： _____

因金融诈骗或欺诈而损失的原始资金中，是否有部分被追回并返还给消费者（例如通过交易撤、资金追索、扣押或调查）？

☐ 是，全额补偿

☐ 是，部分补偿 ☐ 无法追回资金

若无法追回资金，请说明是否因消费者存在重大过失所致：

☐ 因重大过失所致

银行、支付服务提供商、商户或其他实体是否向消费者退还或补偿了任何资金（例如基于责任认定、政策规定或法定义务）？

☐ 是 ☐ 否



若选“是”:

退还/补偿金额: _____

退款/补偿方:

☐ 银行

☐ 支付服务提供商

☐ 商户

☐ 其他: (请在此处输入文本) 补偿依据 (如已知):

☐ 法定义务

☐ 政策/出于善意

☐ 责任认定 ☐ 其他: (请在此处输入文本) 授权性质

针对该交易/互动, 是否存在消费者授权机制?

☐ 是 ☐ 否

若选“是”, 由谁授权了该交易/互动?

☐ 账户/产品持有人

☐ 授权代表

☐ 诈骗者

☐ 其他 (请在此处输入文本) 实体性质 (如适用)

涉及何种类型的诈骗者?

☐ 个人/第三方

☐ 实体



涉案金融服务提供商在欺诈发生的司法辖区内，是否持有开展该项业务的执照/授权？

☐ 该实体在欺诈行为发生的司法辖区内，拥有开展与该欺诈行为相关业务的完整执照

☐ 该实体在该司法辖区内拥有开展部分业务的执照，但不包括与该欺诈行为相关的业务

☐ 该实体未在欺诈行为发生的司法辖区内获得运营执照，但在其他司法辖区获得授权

☐ 该实体为虚构实体（例如：该实体既未在欺诈行为发生的司法辖区获得执照，也未在其他司法辖区获得执照）

如果该金融服务提供商在其他地区获得执照，那么该欺诈行为是否由第三方欺诈者实施？

☐ 是 ☐ 否