数字金融反欺诈
——洞察与攻略

2018年11月

腾讯大金融安全 Tencent Financial Security | CAICT 中国信通院 | 腾讯金融科技智库

版权声明

目 录

前 言

随着大数据、人工智能和区块链等数字化技术在金融领域的广泛应用，数字金融服务不断普及，显著提升了金融服务能力，有力推动了普惠金融的发展。然而，数字金融在提升行业服务能力的同时，也客观上给金融欺诈带来了新的空间。尤其是欺诈方式也利用新技术出现了新的变化，呈现出金融欺诈产业化、犯罪组织职业化、作案目标精准化、欺诈活动移动化、诈骗场景多样化等新特征，损害了广大金融用户的合法权益，加深了金融市场的风险，也给整个社会经济的稳定发展带来了负面影响。

本白皮书依托于腾讯公司多维度和广覆盖的大数据资源，对当前数字金融欺诈的总体形势、典型手法、相关区域和人群特征，进行了深入分析。前瞻性的解读了大数据、人工智能和区块链等新兴技术在数字金融反欺诈领域的典型应用，并总结了交易延时到账机制、异常交易的提醒、账户管理机制、平台赔付制度等一系列创新型的数字金融反欺诈措施。从监管立法、行业联防、科技应用和常识教育等多维度提出了强化数字金融反欺诈的相关建议。

最后的附录成为了本白皮书的一大特色。在附录中，收集整理了数字金融欺诈的多个典型套路及其特点，并提出了相应的防骗原则，真正为广大用户提供最直接的“防骗攻略”。

一、数字金融欺诈概述

（一）数字金融欺诈的基本概念

金融与我们的日常生活息息相关，是现代经济的核心。随着金融科技的不断应用发展，金融服务的数字化逐步成为行业发展的主流方向，无论是服务形式、服务渠道都呈现出数字金融的新特征。数字技术应用到金融领域，一方面有效提升了金融服务效率，降低了服务成本，但另一方面也带来了一系列新型的金融风险，尤其是出现了众多利用数字技术进行的新型金融欺诈行为。

理解数字金融欺诈，首先需要回到“金融欺诈”这个基本概念：所谓“金融欺诈”是指以非法占有为目的，采用隐瞒真相或虚构事实的欺诈手段，用以骗取公私财物或者金融机构信用、破坏金融管理秩序的违法犯罪行为。“数字金融欺诈”并没有改变金融欺诈的本质，它强调的是在欺诈手法上的变化，主要是与数字技术相结合而产生的一系列新型的金融欺诈行为，如网贷平台欺诈、大数据精准欺诈等。

在利益的驱使下，数字金融欺诈逐渐形成了“黑色产业链”，并不断“发展壮大”，所带来的社会危害也在不断加深，已经引起了社会各界的广泛重视。具体而言，根据欺诈方式和行为对象，当前的数字金融欺诈主要表现为高利理财、网络借贷、网络众筹、消费金融、非法集资等五种类型。

图 1：数字金融欺诈五种类型

高利理财类诈骗主要是利用受害人期望“高额回报”的心理，对其进行“利益”诱惑。据相关报告显示，在金融诈骗众多类型中，金融理财类诈骗所涉及的总金额和人均损失额度，均是最高。高利理财类欺诈手段比较多样，以低投资获得高利息、“消费返利”、投资境外股权、期权、外汇，私募入股、投资“虚拟货币”、“区块链”等为噱头的互联网金融理财欺诈行为。

网络借贷类诈骗通常是通过网络操作，盗取投资者信息，以低息贷款获利高进行引诱，迷惑投资者。由于网络借贷诈骗造假成本低，操作简单，不易被发现，成为金融诈骗高发类型。据调查，通常网络借贷诈骗的主要方式有包装骗贷、组团诈骗、中介代办、担保公司模式、虚假广告引诱、缴纳保证金、冒充他人，信息盗取等。

网络众筹类诈骗主要表现在投资众筹、众筹开店、电影众筹、扶贫救助众筹、熟人众筹等形式。无论是非法吸收公众存款，还是冒充上市公司发行股票往往都是外表披着“众筹”的外衣，但是实则由于缺乏资金的第三方托管，信息披露不健全等问题，再加上项目发起人和项目投资人信息强烈不对称，使得投资者陷入非法集资

的陷阱。

消费金融欺诈主要表现为网络支付诈骗、虚假营销、骗取网购运费险、骗取消费退款、网络刷单诈骗等欺诈方式。欺诈手段包括，利用第三方支付账户安全系统的漏洞，造成信息泄露，进行支付诈骗和套现，以及虚假宣传、信用卡欺诈、刷单诈骗、退款诈骗、骗保、被骗保证金等消费金融类欺诈。其中，买方对网购退货运费险的恶意欺诈行为已经成为消费金融类欺诈的高发事件。据中国保险行业协会数据显示，某公司上市运费险之初的赔付率竟高达90%，可以推断其中有大部分骗保行为。

非法集资类欺诈是指公司或个人未经批准，违反法律、法规，通过不正当的渠道，向社会公众或者集体募集资金的行为。欺诈手段包括擅自发行股票、债券，利用传销或秘密串联的形式非法集资，甚至利用地下钱庄等民间会社形式非法集资，签订商品经销等经济合同的形式进行非法集资。

（二）数字金融欺诈的发展历程

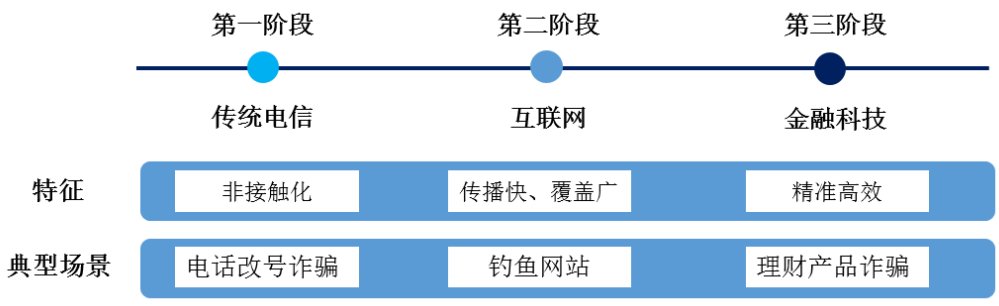


图 2：数字金融欺诈发展历程

1. 第一阶段：利用传统电信的金融欺诈

第一阶段的金融欺诈是以电信为媒介，向社会不特定人群发布

虚假诈骗消息，来骗取、非法占有他人公私财物，迫使被害人自愿交付财物的行为。此类案件采用非接触化的方式，是目前最为常见的一种诈骗类型。

此类诈骗由于作案工具简单，只需要获取他人个人信息，一部电话、一个可改号的软件，再加上骗子精心编制的场景，就可以实施作案。针对传统电信的反欺诈行动，重点应放在有关部门的宣传和教育上，加强防骗宣传和防范措施，提高全民的防范意识。

2.第二阶段：利用互联网的金融欺诈

第二阶段的金融欺诈是以互联网为媒介进行传播，相比于电话传播，其传播速度快、覆盖人群广，通过某圈、某博、某公众号便可进行指数化传播。

此类诈骗常见的场景包括：网址有木马链接、冒充公安、冒充客服人员、冒充好友、网络招工、钓鱼短信网站等等。此类诈骗具有作案方式信息化，作案手段智能化，作案地域跳跃化，作案行为场景化等特点。往往采用团体作案，分工清晰，手段新颖，且隐蔽性较强，给侦破带来一定难度。有关媒介应负起监督审核的责任，不传播虚假信息；对于个人，要善于判断与识别，提高警惕。

3.第三阶段：利用金融科技的金融欺诈

第三阶段的金融欺诈结合了金融科技常见技术，尤其是大数据和人工智能技术，与第二阶段的互联网技术相比，其通过大数据分析可以对不同群体进行标签化特征的精准定位，根据不同的标签编制不同的场景，“因人而异，因地制宜”，大大提高了诈骗的成功

率与效率，减少了诈骗成本。

此类诈骗是随着金融科技技术的发展应运而生的，能够精准定位目标受众，准确匹配犯罪场景。如：可根据收集到的用户个人信息，分析其资金状况、家庭关系、消费习惯、生活习惯等等，有针对性地编制承诺高风险高收益的理财产品，谎称可以无风险获得贷款等场景进行金融诈骗。

（三）数字金融欺诈的发展特点

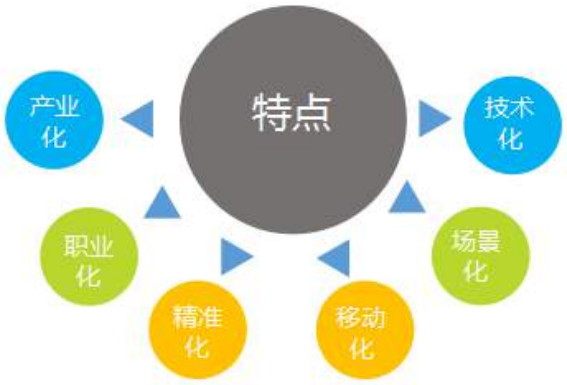


图 3：数字金融欺诈特点

1. 金融欺诈产业化

金融欺诈呈现出产业化的特征。围绕着欺诈的实施，形成了身份信用包装产业、虚假身份提供产业、业务漏洞发现产业和欺诈手段传授产业。各产业通过网络通讯工具进行匿名交流，看似组织松散，其实合作紧密。数亿级账号密码关系为地下黑色产业链所掌握，所掌握的被盗号数量占到整体被盗账号的 80%，而盗号所衍生的黑产业链年获利超百亿元。据《电子商务生态安全白皮书》数据测算，中国“网络黑产”从业人员已超过 150 万，市场规模高达千亿级别。

2. 犯罪组织职业化

与传统金融诈骗相比，数字金融诈骗犯罪往往由多人共同实施，相互间有明确分工，既有策划整个诈骗活动的“导演组”，也有“因人而异”编制特定场景的“编剧组”，实施具体对话诈骗的“演员组”，同时还有专门负责网上转存、资金分解的“制片组”及组织实施取款提现的“场务组”，各环节分工明确，高度职业化。

3.作案目标精准化

数字技术，如：大数据、人工智能、区块链技术的应用，使得诈骗方式由原来的遍地散网到精准定位，如：从学校获得的数据可贴上为教育需求者的标签，针对其教育的推销诈骗往往成功率较高；从医院获得的数据可贴上医疗资源需求者的标签，针对其药物、保健品的诈骗推销往往比随机成功率大大提升；同理发生在银行针对贷款、理财产品的推销，发生在房屋中介针对房屋租赁的推销等等。诈骗分子利用数字技术的手段，精准化定位加深了犯罪带来的危害。

4.欺诈活动移动化

截止2018年6月，我国手机网民规模达 7.88 亿，较2017 年末增加 4.7%，网民手机上网比例继续攀升。相应地，金融欺诈呈现移动化趋势。2017年，全球重大数据泄露事件达1765个，平均每家企业数据泄露成本是362万美元，比2016年增长10%。平均每次数据泄露或记录被盗的成本是141美元，比2016年增长11.4%，其中60%以上来自移动设备。

5.欺诈行为场景化

数字金融业务依托特定的场景开展，对应的金融欺诈也呈现出场景化特征。常见的场景有：假冒公职人员，冒充熟人，购车退税，银行卡消费透支，无抵押贷款，短信电话中奖，利用 QQ 等聊天工具，虚假购物网站等等。诈骗分子利用不同场景，精准定位目标人群，准确掌握被害人心理，从而实施诈骗行为。

6.欺诈行为技术化

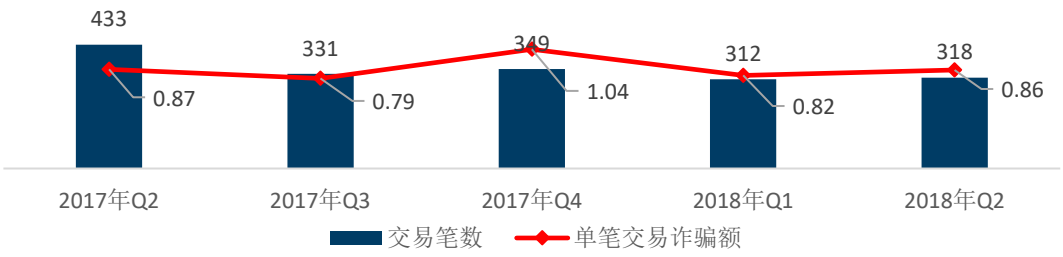
随着技术的快速发展，技术在提升服务效率，降低服务成本的同时也为欺诈行为提供了抓手，一些欺诈软件的开发，钓鱼网站的设计、用于刷单的“猫池”以及各类“羊毛党”的出现无一不在利用科技的手段开展欺诈活动，欺诈行为的技术化带来了欺诈成本的降低和欺诈威胁的扩大。

二、数字金融欺诈总体形势分析

根据监测数据显示[1]，数字金融诈骗交易笔数和诈骗交易收款账号数量方面，出现了逐步下降的态势；以季度为周期，2018 年第二季度比第 2017 年第二季度的诈骗交易笔数下降了 26.6%，诈骗作案收款账号数量下降了 42.0%。**这说明随着监管打击措施的强化和人们防骗意识的提升，数字金融欺诈案件的发生数量和作案人群均在减少。**然而，支付账号单笔被骗金额和数字金融欺诈案件涉及总金额，却呈现较为明显的上升趋势；以季度为周期，近 1 年内的诈骗交易金额的平均复合增长率达到 17%，单笔支付的诈骗金额平均复合增长率达到 14%。**这意味着单笔诈骗给用户带来的平均损失在增加，相应的诈骗危害性在增强。**

（一）诈骗交易笔数呈下降趋势

从诈骗涉及的交易笔数来看，2017 年第三季度诈骗交易笔数明显下降，环比下降 23.6%，在近一段时间整体交易笔数保持平稳下降趋势。从单笔交易诈骗金额来看，随着春节的临近，2017 年第四季度单笔交易诈骗金额比值明显高于其他季度单笔交易诈骗金额。



[1] 本白皮书所用数据均来自于腾讯公司金融反欺诈监测渠道

图 4：诈骗交易金额及单笔交易额规模趋势（2017 年 Q2~2018 年 Q2）[1]

（二）诈骗作案收款账号数量显著下降

从诈骗作案人收款账号数来看，作案人使用的收款账号数量在 2017 年第三季度和第四季度连续大幅下降，2017 年第三季度环比下降 50%以上，但随后作案人收款账号数比值有缓慢增长趋势。从收款账号单笔诈骗金额来看，2017 年第四季度收款账号单笔诈骗金额最大，且收款账号的单笔诈骗金额比值有增长趋势。

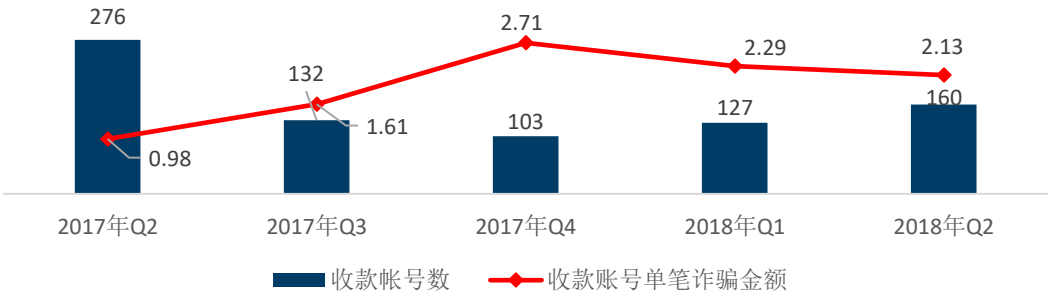


图 5：收款账号数及收款账号单笔诈骗金额趋势图（2017 年 Q2~2018 年 Q2）

（三）支付账号单笔被骗金额上升明显

从数字金融诈骗涉及的受骗用户支付账号数量来看，受骗涉及的支付账号数量呈下降趋势，与 2017 年第二季度相比，2018 年第二季度支付账号单笔被骗金额比值同比下降 26.1%。但受骗人单笔支付的诈骗金额增长趋势明显。2017 年第二季度到 2018 年第二季度，单笔支付的诈骗金额复合增长率达到 14%，受骗人被骗损失程度加深，欺诈带来的危害在加深。

[1] 白皮书中所有呈现数据均为脱敏处理后的比值数据，除百分比数据可以表示真实比例外，其他数值为比例数字，仅呈现发展趋势，本身不代表实际意义，所以数据无数值单位。

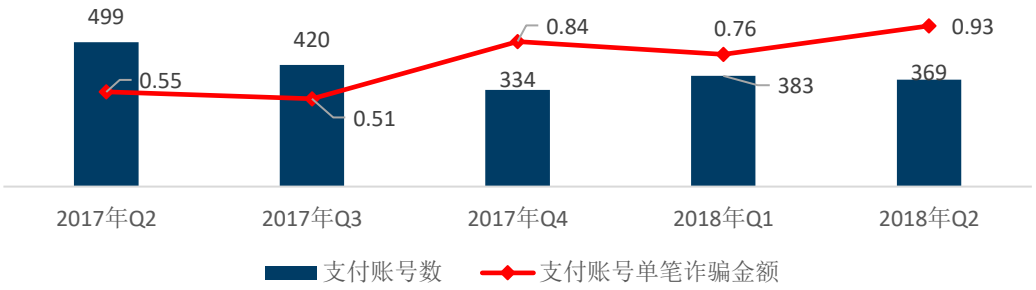


图 6：支付账号数及支付账号单笔诈骗金额趋势图（2017 年 Q2~2018 年 Q2）

（四）诈骗案件金额呈现上升趋势

数据统计显示，2017 年第二季度到 2018 年第二季度期间，全国诈骗交易金额总体呈上升趋势。与 2017 年第二季度相比，2018 年第二季度诈骗交易金额比值同比增长 25.7%。从 2017 年第三季度开始，诈骗交易金额复合增长率达到 17.3%。

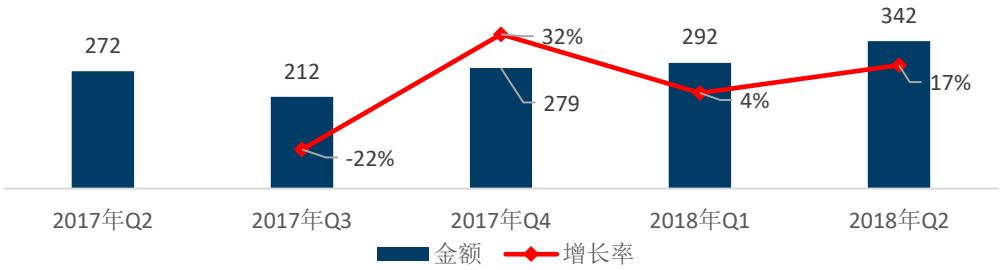


图 7：诈骗交易金额规模趋势（2017 年 Q2~2018 年 Q2）

三、 数字金融欺诈手法分析

目前，腾讯开通人工客服、社交报障系统和商业报障系统三个渠道对诈骗案件进行监测。人工客服渠道是指致电腾讯客服进行欺诈投诉。社交报障渠道是指在C2C（用户与用户）交易过程中，对出现的欺诈行为，利用交易发生的社交工具进行欺诈投诉。商业报障渠道是指在C2B（用户与商家）交易过程中，对出现的欺诈行为，利用交易发生的社交工具进行欺诈投诉。其中，社交报障渠道和商业报障渠道属于自助渠道，举报量级比人工客服渠道更大。

通过对近两年各渠道的诈骗数据统计分析发现，诈骗团伙在数字金融常用诈骗手法中，最主要的三类诈骗方式为**退款诈骗、刷单兼职诈骗和仿冒各种身份诈骗**。具体到各个渠道来看：

人工客服渠道统计的诈骗手法主要有退款诈骗、刷单被骗、冒充好友被骗、冒充公安被骗、付款码被骗、好友账号被盗诈骗、商户交保证金被骗以及冒充客服被骗。社交报障系统渠道统计的诈骗手法有刷单兼职、仿冒身份、冒充微粒贷骗钱、被骗保证金、虚假投资理财、假冒客服、假冒共享单车欺诈等。商业报障系统渠道统计的诈骗手法有兼职、返利和诱导三大类。

最主要的三类数字金融诈骗方式 **退款诈骗、刷单兼职诈骗、仿冒各种身份诈骗**		
人工客服	**社交报障**	**商业报障**
• 退款诈骗 • 刷单被骗 • 冒充好友被骗 • 冒充公安被骗 • 付款码被骗 • 好友账号被盗诈骗 • 商户交保证金被骗 • 冒充客服被骗	• 刷单兼职 • 仿冒身份 • 冒充微粒贷骗钱 • 被骗保证金 • 虚假投资理财 • 假冒客服 • 假冒共享单车欺诈	• 兼职 • 返利 • 诱导

图 8：腾讯反欺诈渠道的欺诈方式统计

（一）诈骗金额最多的诈骗手法

通过三个反欺诈监测平台的数据显示，人工客服渠道接到的数字金融欺诈案件投诉电话中，诈骗手法集中度高，退款诈骗、刷单诈骗两种诈骗手法诈骗金额占总案件金额的 84.5%；其中超过一半的作案人群使用退款诈骗的手段，刷单被骗诈骗金额占比近 30%。社交报障渠道获得受骗人举报最多的诈骗手法是刷单兼职和仿冒身份，两者诈骗金额占比超过 70%；商业报障渠道获取的数据中，诈骗手法种类较少，以兼职为主的商业诈骗手法诈骗金额占比达到 72.9%。

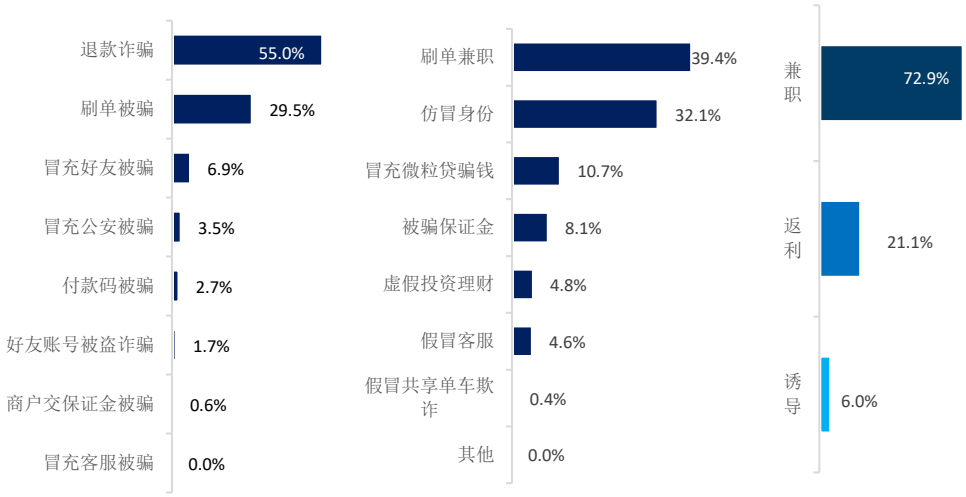


图 9：诈骗手法占比——诈骗金额（2017 年 1 月~2018 年 8 月）

（二）诈骗交易笔数最多的诈骗手法

从诈骗交易笔数来看，人工客服渠道诈骗交易笔数最多的是刷单被骗，占比 56.3%，其次为退款诈骗，占比 30.6%；社交报障渠道中，刷单兼职涉及的交易笔数最大，占渠道总交易笔数的 50.9%，其次为采取仿冒身份进行的诈骗手法，交易笔数占比 21.5%；商业报障渠道，兼职诈骗涉及的交易笔数占总交易笔数的近 60%，成为商业诈骗的主要诈骗手法。

图 10：诈骗手法占比——诈骗交易笔数（2017 年 1 月~2018 年 8 月）

（三）诈骗支付账号数最多的诈骗手法

从诈骗支付账号数来看，人工客服渠道获取数据结果显示，刷单被骗涉及到的受骗人数最多，占比 51.7%，其次为退款诈骗，占比 34.0%;社交报障渠道因刷单兼职而受骗的人群比例最高，为 50.5%,其次为仿冒身份，占比 22.2%。商业报障渠道，兼职被骗涉及的支付账号数最多，占比 56.7%，其次为返利形式的诈骗，占比 23.6%。

图 11：诈骗手法占比——诈骗支付账号数（2017 年 1 月~2018 年 8 月）

（四）诈骗收款账号数最多的诈骗手法

从诈骗涉及的收款账号数来看，人工客服渠道，诈骗收款账号数最多的诈骗手法是退款诈骗，占比 36.7%，其次是刷单诈骗，占比 32.2%，另外冒充好友诈骗涉及的收款账号数占第三位，占比 19.2%。社交报障渠道中，刷单兼职涉及到的收款账号数最多，占比 48.3%，其次位仿冒身份，占比 23.1%；商业报障渠道中，采用兼职诈骗手法使用的收款账号数最多，占比将近 50%，其次为采取返利手段的诈骗，涉及收款账号数占比 30.5%。

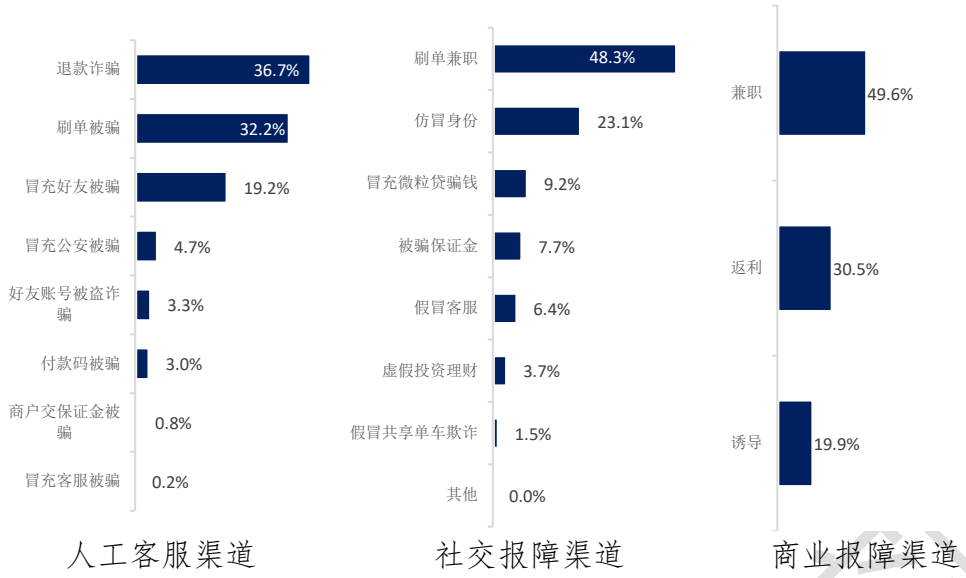


图 12：诈骗手法占比——诈骗收款账号数（2017 年 1 月~2018 年 8 月）

（五）诈骗单笔交易金额最多的诈骗手法

从诈骗单笔交易金额来看，人工客服渠道监测结果显示，仿冒身份诈骗手法危害最大，在各诈骗手法中单笔诈骗金额最大，其次为虚假投资理财和冒充微粒贷骗钱。社交报障渠道中，冒充公安被骗单次骗取的金额最大，其次为退款诈骗和好友账号被盗诈骗。商业报障渠道的三种诈骗手法中，诈骗单笔交易金额由大到小顺序为兼职诈骗、返利诈骗和诱导诈骗。

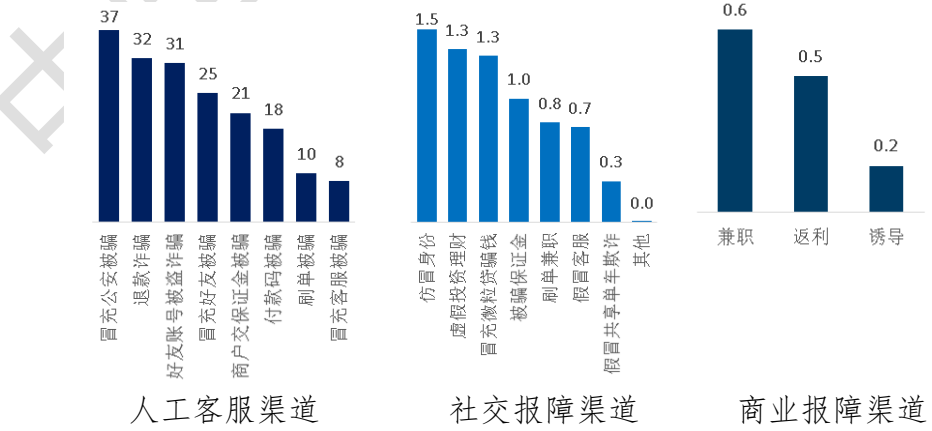


图 13：诈骗手法占比——诈骗单笔交易金额（2017 年 1 月~2018 年 8 月）

四、 数字金融欺诈人群与区域特征分析

（一）受骗人群画像特征分析

监测统计结果显示，全国涉及数字金融诈骗的受骗人群中，男性受骗人数量是女性受骗人数量的两倍以上，其中，男性受骗人占比 69%，女性受骗人占比 31%。

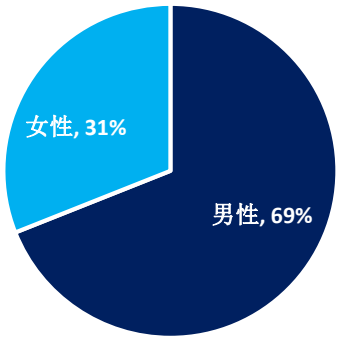


图 14：受骗人群性别占比（2017 年 1 月~2018 年 8 月）

受骗人群在不同省份之间性别分布存在差异。广东、福建、河南、广西和江西五省的受骗人群中男性占比均在 70%以上，受骗人群中女性占比在 30%以下。上海、北京、新疆、天津、黑龙江五省是受骗人群中女性占比最高的省份，女性占比超过 35%。

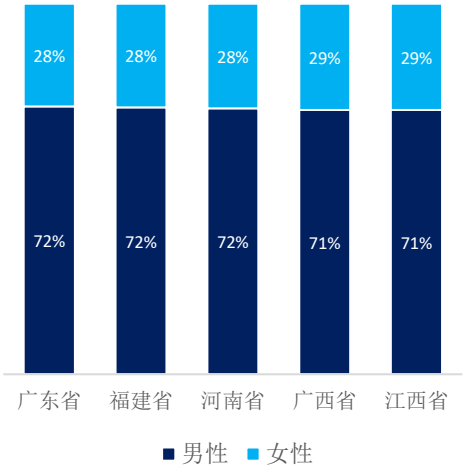


图 15：受骗人男性比例排名前五省份

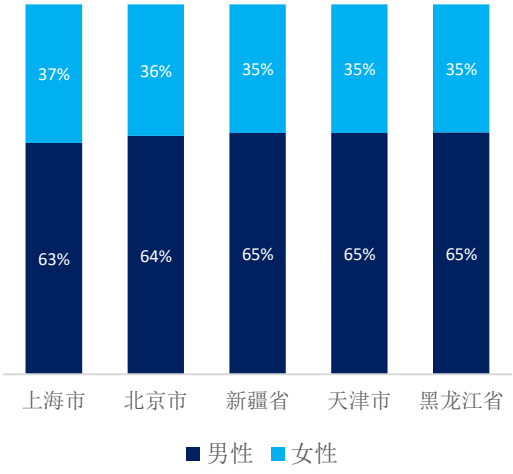


图 16：受骗人女性比例排名前五省份

（2017 年 1 月~2018 年 8 月）　　（2017 年 1 月~2018 年 8 月）

从全国来看，受骗人群呈年轻化。受骗年龄集中在 18~35 岁之间，占受骗人群总数的 71%，其中，18-24 岁年龄段年龄占比最高，是最容易在数字金融领域受骗的人群，占比高达 36%。46 岁以上中老年人群受骗比例最低，46~59 岁、60 岁以上两个年龄段占比 6%。

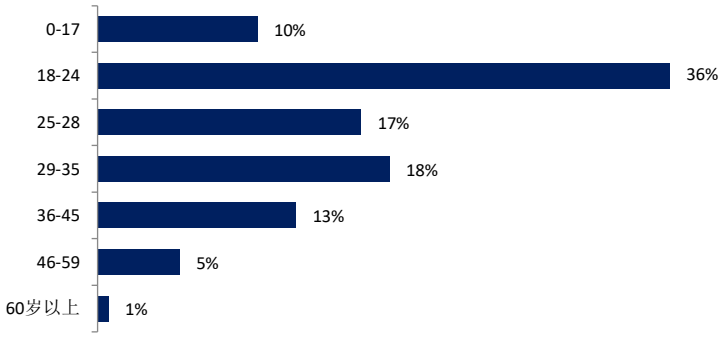


图 17：受骗人群年龄分布（2017 年 1 月~2018 年 8 月）

从全国来看，在最易受骗的 18~24 岁的受骗人群中，受骗人分布占比排名前五的省份分别是广东省、河南省、四川省、湖南省以及广西省。其中，广东省 18~24 岁的受骗人数占比最高，为 11.3%；河南省和四川省紧跟其后，占比分别为 8.2%和 7.1%。

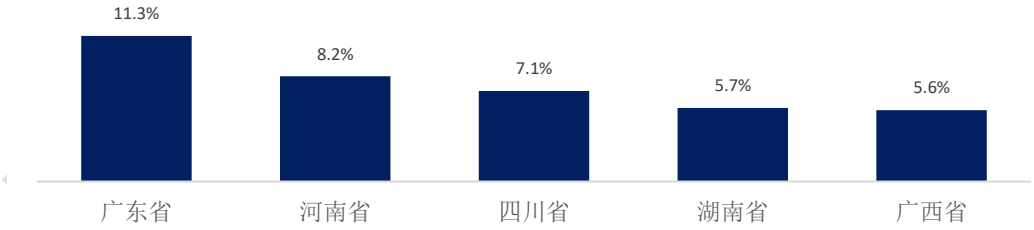


图 18：事件前五省份年龄分布（2017 年 1 月~2018 年 8 月）

（二）受骗人群区域分布特征

从受骗人损失金额来看，诈骗损失金额排名前十的省份损失金额约占全国总金额的 60%，其中，广东省受骗损失的金额位居全国之首，占比 8.8%；其次是河南省，受骗损失金额占比 7.6%；四川省

以受骗损失金额占 6.8%位居第三。

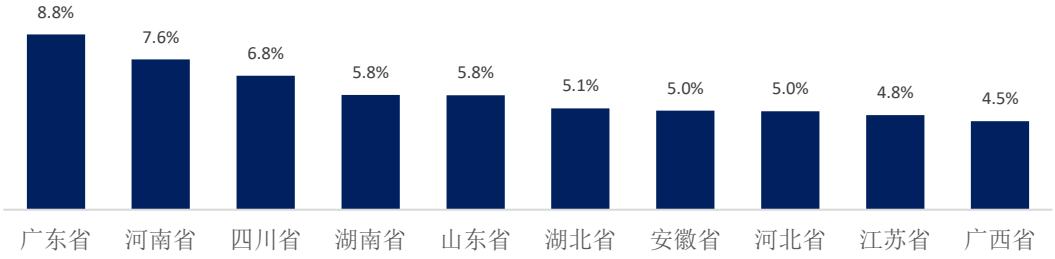


图 19：受骗损失金额排名前十省份（2017 年 1 月~2018 年 8 月）

从受骗人数来看，广东省涉及到的受骗人数最多，占全国受骗总人数的比例达到 10%，河南省位居第二，受骗人数占比为 8.2%；四川省、湖南省两省占比分别为 6.4%和 6.3%，排在第三和第四位。

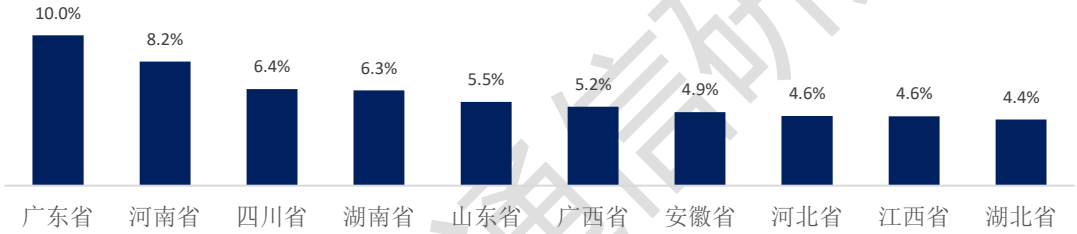


图 20：受骗人数量全国排名前十省份（2017 年 1 月~2018 年 8 月）

从人均损失额来看，参照人均损失金额比值，上海市人均损失额最高，比值 0.47，是全国人均损失金额最低的内蒙古比值（比值 0.23）的两倍。排名前五的省份还有浙江省、北京市、天津市以及新疆。

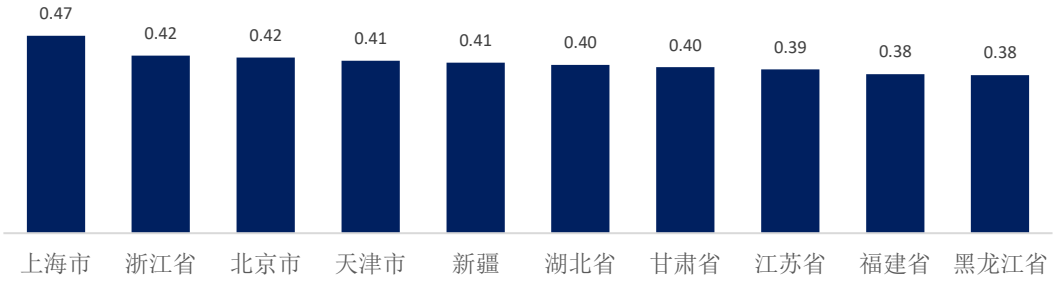


图 21：人均损失金额排名前十省份（2017 年 1 月~2018 年 8 月）

（三）作案人群画像特征分析

从作案人性别来看，在全国数字金融欺诈作案人群中，男性参与作案的人数略高于女性，但占比差距不明显。其中，男性作案人数占比 57%，女性作案人数占比 43%。

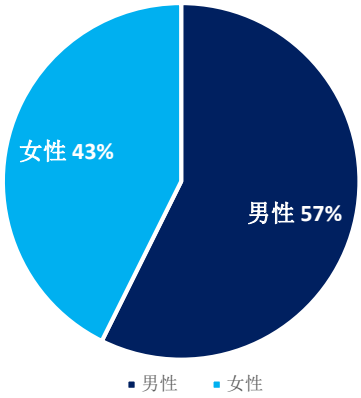


图 22：作案人群性别占比（2017 年 1 月~2018 年 8 月）

从全国整体作案人群来看，作案人男性占比排名前五的省份有上海、青海、西藏、广东和海南。其中，上海、青海和西藏三省市男性作案人占比均在 70%以上，上海市最高为 76%。作案人女性占比排名前五的省份中，云南作案人中男女比例各占一半，贵州女性作案人占比 48%，重庆女性作案人占比 47%。

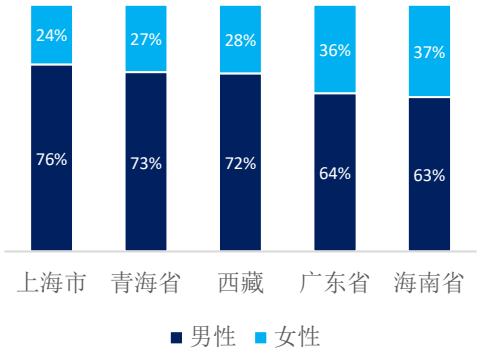


图 23：作案人男性比例排名前五省份

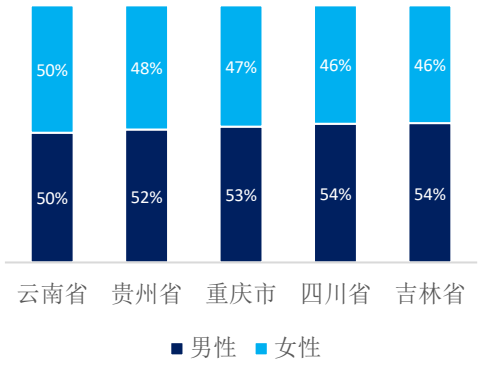


图 24：作案人女性比例排名前五省份

从作案人年龄分布来看，全国作案人年龄分布较为平均，除 18

岁以下未成年和 60 岁以上老年人外，其他年龄段作案人群分布相对均衡。其中，36~45 岁，29~35 岁以及 18-24 岁三个年龄段的作案人群占比均在 20%以上，占总人数 65.7%，占比分别 22.5%，22.4%和 20.8%。

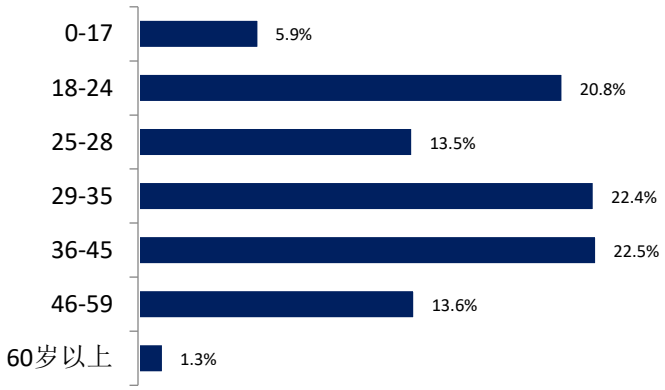


图 25：作案人群年龄分布（2017 年 1 月~2018 年 8 月）

在作案人年龄相对较多的 29~35 岁、36~45 岁两个年龄段中，29~35 岁作案人占比排名前五省份中，河南占全国作案人比例为 9.5%，占比最高，其次为广东省，占比 8.9%。全国 36~45 岁作案人中，占比排名前五的省份分别为广东、河南、湖南、安徽和福建。其中广东占比最高，为 9.7%，河南占比 9.3%，位居第二。

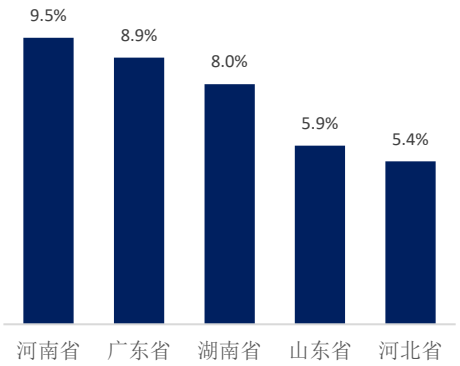


图 26：29~35 岁作案人占比排名前五省份

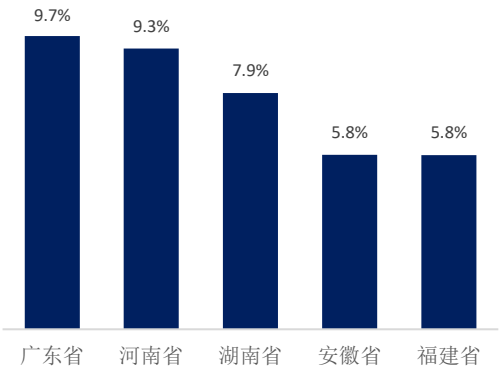


图 27：36~45 岁作案人占比排名前五省份

（四）作案人群区域分布特征

监测数据显示，从全国作案人分布区域来看，排名前十的省份占全国总作案人数的绝大部分，占比 67%。其中，广东、河南、湖南三省作案人数量明显高于其他区域。广东作案人数最多，占比 12%,河南排名第二，占比 9.8%，湖南以 8.5%的占比排名第三。

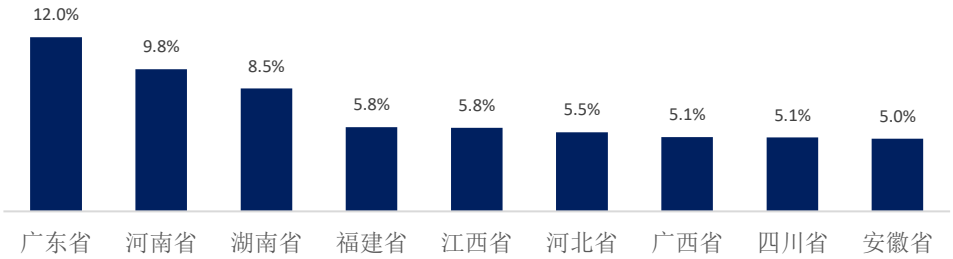


图 28：作案人数占比排名前十省份（2017 年 1 月~2018 年 8 月）

人工客服渠道监测数据显示，事件排名前五的省份中，广东采用刷单诈骗和退款诈骗的比例相同，占作案手法总数的 74%；河南和四川以刷单诈骗手法为主，占比分别高达 64%和 54%；福建和江西采用退款诈骗方式居多，占比均超过 50%。

社交报障渠道监测数据显示，事件排名前五的省份使用的诈骗手法比较相似，均以刷单兼职为主导，除广东外，其他省份占比均超过 50%，是主要的诈骗手法，其次为使用仿冒身份的方式进行诈骗，事件占比在 20%以上。

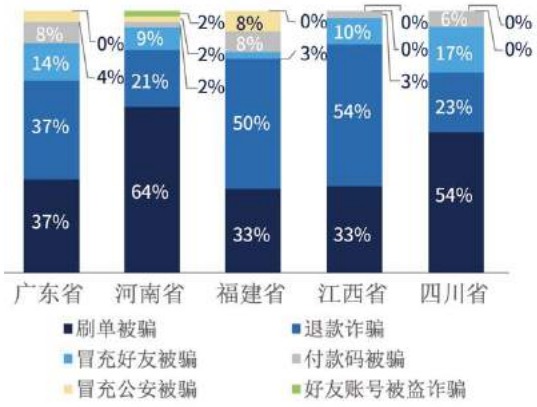


图 29：人工客服渠道事件前五省份诈骗手法分布

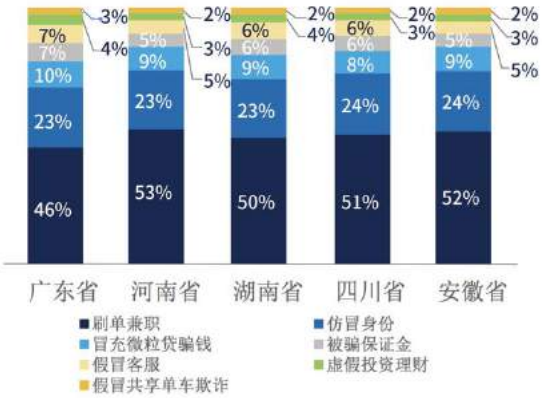


图 30：社交报障渠道事件前五省份诈骗手法分布

从全国来看，人工客服渠道作案人使用最多的诈骗手法是刷单诈骗和退票诈骗。其中，刷单诈骗事件作案最多的省份是河南，占比为 10.3%，其次为四川和山东，占比均为 6.5%。退款诈骗事件作案最多的省份是江西，占比 10.3%，其次为福建和广东，占比分别为 9.9%和 8.9%。

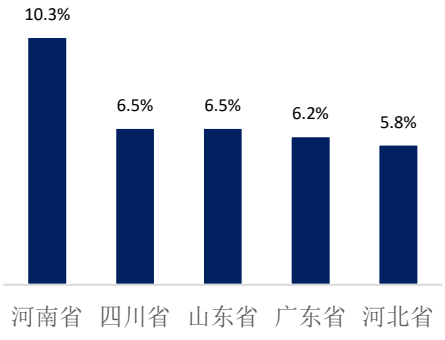


图 31：刷单诈骗手法前五省份

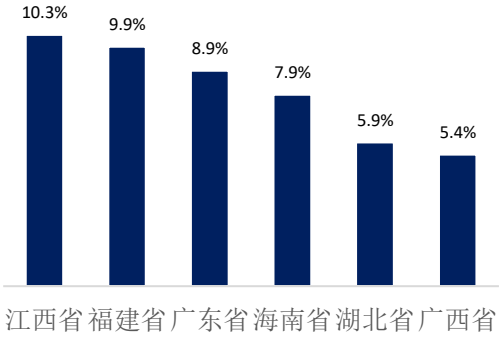


图 32：退款诈骗手法前五省份

社交报障渠道作案人使用最多的诈骗手法是刷单兼职和仿冒身份。其中，刷单兼职事件作案最多的省份是广东，占比为 10.1%，其次为河南和湖南，占比分别为 9.7%和 7.4%。仿冒身份诈骗事件作案最多的省份是广东，占比 10.7%，河南次之，占比 8.9%，湖南位

居第三，占比 7.2%。

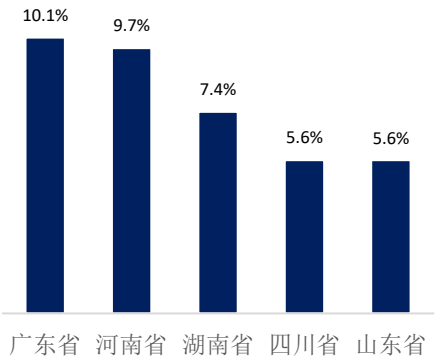


图 33：刷单兼职诈骗手法前五省份

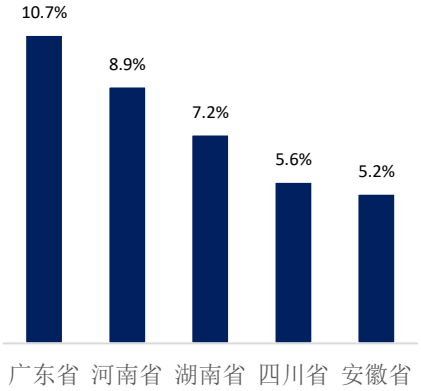


图 34：仿冒身份诈骗前五省份

五、 金融科技助力数字金融反欺诈

当前随着技术的不断演进，大数据、人工智能、区块链等新兴技术已广泛应用于各项金融业务，在金融反欺诈领域也得到了深入而广泛的应用：大数据为反欺诈奠定了数据基础、模型基础，人工智能使得反欺诈手段更加多样化、智能化，区块链在促进数据共享、构建生态联防体系等方面发挥重要作用。随着欺诈手段的不断升级演进，科技将在金融反欺诈中发挥越来越重要的作用。

（一）大数据在数字金融反欺诈中的应用

大数据在金融反欺诈领域的应用主要体现在以下三个方面：一是利用大数据相关技术实现数据的广泛采集，从而建立来源广、范围宽、多维度的反欺诈基础数据库；二是大数据分布式支持高并发的架构实现了对于海量数据的实时处理能力，能做到对于风险的实时监测，有助于构建金融交易实时反欺诈系统；三是大数据的强大分析能力，依托已有的海量数据进行深度挖掘，建立用户画像，形成反欺诈模型，为金融反欺诈提供决策依据。

图 35：大数据技术在反欺诈领域应用

在数据获取层面，目前金融机构主要有三种方式：在自有系统中沉淀、在网上采集和从第三方购买。通过爬虫技术等相关数据采集方法能帮助金融行业有效地从一些公开场合采集到包括行业舆情数据、企业经营数据以及个人行为数据等相关信息。这些数据对于金融行业反欺诈而言是一个重要的补充，为后续开展数据分析和数据挖掘，识别金融欺诈行为，构建更加完备的反欺诈体系奠定数据基础。

在数据处理层面，随着金融业的快速发展，金融业务量正迅猛增长，因此对于金融反欺诈而言更需要系统具备实时计算和监测的能力，对数据处理速度提出了更高的要求。大数据因其采用分布式集群架构，实现了对于海量交易的快速处理，同时也具备了支持高并发的架构，能有效应对在特殊时段业务量骤增而带来的高压状况。当前为了实现数据的快速处理一般采用流处理技术，因此流式计算框架的实时计算大数据平台目前逐渐在金融行业得到应用，以满足金融反欺诈等低延时的复杂应用场景需求。

在数据分析层面，大数据强大的数据挖掘和分析能力可形成较精准的用户画像，能有效识别欺诈用户。同时，也可根据对海量历史交易数据的分析挖掘提炼出不同统计指标和特征变量，从而识别欺诈交易的一些典型规律，通过对交易的实时监测，采用模糊匹配、相似度计算等技术手段能快速的对异常交易进行预警。此外，大数据的分析也越来越依赖于人工智能的应用，针对一些复杂的欺诈场景，需要结合更多维度的数据，通过机器学习等智能算法构建

更加复杂的分析模型从而更精准的识别欺诈行为。

目前，大数据在金融反欺诈领域已经有许多实际应用。以腾讯公司为例，其根据海量的历史交易数据和诈骗案例，从多个维度提炼了 3000+规模的分析变量，并根据欺诈对抗特征制定了 2000+规模的安全策略，在用户的支付前、支付中、支付后、用户教育感知等多个方面，打造保障用户支付安全的立体安全策略体系。

（二）人工智能在数字金融反欺诈中的应用

人工智能综合了计算机科学、生物学、心理学、语言学、数学哲学等学科知识，使用机器代替人类实现认知、识别、分析、决策等功能，其本质是对人的意识与思维的信息处理过程的模拟。

目前人工智能的关键技术主要包括机器学习、自然语言处理、计算机视觉、生物识别、知识图谱等。相关技术已经在金融领域得到初步探索和应用，在征信和风控领域，设备指纹、知识图谱、生物探针、行为序列、人脸识别、活体检测、语义分析等技术已经用于防范和监测金融欺诈活动。

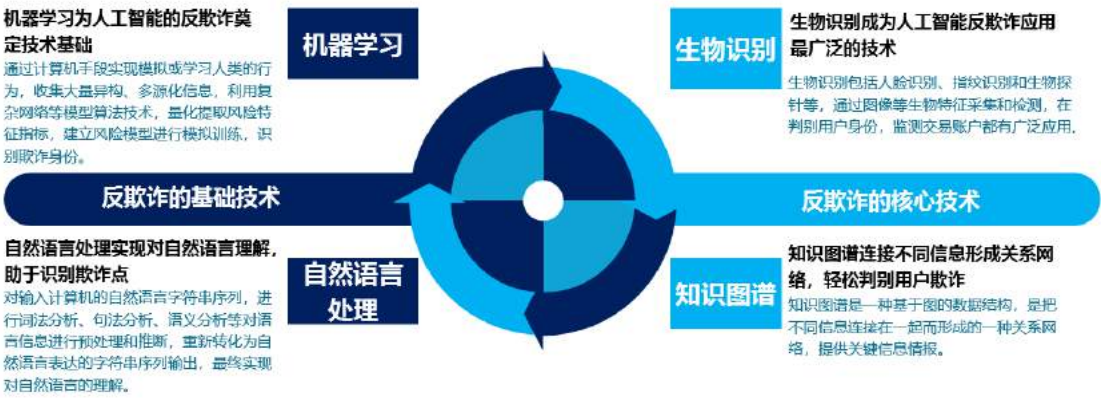


图 36：人工智能技术在反欺诈领域应用

人脸识别是一种依据人的面部特征(如统计或几何特征等)，自

动进行身份识别的一种生物识别技术，技术上包括图像采集、人脸检测、人脸特征提取、人脸特征比对（身份的确认和查找）等，在反欺诈领域可利用该技术识别客户是否是欺诈惯犯，为业务事前审核提供技术抓手，同时在识别真正用户、防止盗刷等方面起到重要作用。

自然语言处理主要是指对于输入计算机的自然语言字符串序列，计算机通过词法分析、句法分析、语义分析等对语言信息进行预处理，将分析的结果映射为机器内部可以识别与处理的表示形式，并可对该内部表示进行推理，重新转化为自然语言表达的字符串序列输出，最终实现对自然语言的理解。在反欺诈领域可以利用NLP技术针对特定的欺诈信息和虚假信息进行有效识别，从而进行适当拦截或风险提示。

知识图谱是一种基于图的数据结构，是把不同信息连接在一起而形成的一种关系网络，从而可以整体、全面的了解不同主体间的关联关系并以此为依据进一步开展深度分析。在反欺诈领域通过知识图谱的应用可以实现将不同类型数据汇聚在一起，从而有效分析出复杂业务关系中潜在的风险，及时识别欺诈行为，对于打击团伙欺诈，防范潜在欺诈用户等方面发挥重要作用。同时，还可以通过知识图谱为执法部门追踪诈骗份子提供相关信息情报。

设备指纹技术是指通过利用设备的多种相关信息来完成设备识别的相关技术统称。随着移动支付的发展，传统的设备识别技术已无法满足对于设备识别的需求，欺诈软件的出现、利用“猫池”进

行的刷单、“羊毛党”的出现等给各大平台运营带来了极大挑战。而设备指纹技术的出现将有效打击综上欺诈行为，通过设备指纹技术给相关设备打上独一无二的标签，从而可以准确识别出欺诈使用的相关设备，即使通过软件篡改设备 ID、使用 IP 代理等方式，设备指纹技术也能够识别出使用的是同一个设备，从而能有效的实现线上欺诈行为的识别和预警。

在实际应用方面，人工智能已经在数字金融反欺诈的多个领域得到实现。例如腾讯公司利用自然语言处理技术，从大量的投诉数据源里提取投诉文本，通过多维度的分析剖析不同的可疑特征，再通过不同的可疑特征制定文本挖掘维度与监控维度去过滤风险词，并搭建了集成文本分析、信息汇总、账号审核、策略打击、大盘搜索、数据导出的文本审核平台。文本审核平台会针对每个挖掘维度统计特征或给出评分，作为评判、筛选可疑账号的标准。

（三）区块链在数字金融反欺诈中的应用

区块链本质是将非对称加密算法、共识机制、分布式存储等相关技术进行融合而形成的一种分布式数据库解决方案，其在金融反欺诈领域的主要作用体现在以下三点：一是有助于推动金融行业信息的共享，搭建反欺诈数据库，构建生态联防体系；二是区块链技术能保护用户的数据安全避免数据的直接泄露，从源头杜绝欺诈发生；三是区块链中的智能合约，能根据自定义的要求自动筛选合规用户及设定相关金额，有效防止欺诈行为。

图 37：区块链技术在反欺诈领域应用

在信息共享方面，区块链因其技术特点能有效的保证信息交换、共享过程中的安全性和隐匿性，将有助于进一步打破行业数据孤岛的现状，促进行业数据的共享。

一方面，区块链的应用将有助于推动金融行业内黑名单客户及相关风险信息的共享，以此建立行业内反欺诈数据库，这将有助于金融机构更全面的做好相关业务的风控，在打击多头借贷、票据作假、重复质押等欺诈行为方面发挥重大作用。

另一方面，区块链的应用也能推动金融行业与其他行业在相关业务层面开展数据的共享，尤其伴随着金融业务的创新，仅仅依靠金融行业内部数据无法实现对于欺诈行为的及时发现，因此通过区块链的应用将有助于在金融行业与其他行业间构建反欺诈生态联防体系，对于打击跨行业的欺诈行为将发挥重要作用。

在数据安全保护方面，区块链运用非对称加密算法，针对链上相关信息都进行了加密处理，与对称加密相比，非对称的加密方式更能确保数据的安全性，能有效避免因数据的泄露而造成欺诈事件的发生。

目前许多欺诈案件的发生是因为用户的相关数据发生了泄露，一些犯罪分子利用平台系统漏洞进行拖库，而许多数据是以明文的形式存在，一旦突破了数据库的安全防护就会导致数据的直接泄露。在区块链系统中通过公钥加密的数据目前只有用私钥才能打开，因此对于存在于区块链系统上的数据来说，即便是区块链系统本身的节点，如果没有对应的私钥也无法获得对应的真实数据，保证了数据的安全。

在智能合约应用方面， 区块链技术通过编译程序来强制自动执行合同内容，能够直接设置风控条件，同时可有效减少因人为因素而引发的欺诈行为。

智能合约在执行中会首先明确交易双方的权利和义务，可以通过在智能合约中设定相关交易人的资格条件，从而判断交易人是否符合相关风控条件，同时也可以在合约中根据交易人相关信息确定允许的对应交易金额，从而在源头上避免交易欺诈的行为发生。此外，在合约执行的过程中，如果没有满足对应的条件合约是不会执行下去，整个过程都是根据代码自动执行，可以避免因人被欺骗从而造成的损失。

（四）数字金融反欺诈创新策略应用

随着欺诈手段不断多元化和技术化，一些交易平台从保护用户的角度开创了一些新机制用于防范欺诈行为，这些机制涵盖事前、事中、事后整个交易流程，对于帮助用户识别欺诈行为，及时提醒用户异常交易以及挽回用户损失方面发挥重要作用。

1.交易延时到账机制

移动支付时代，交易变得更加便捷的同时也给欺诈带来了便利，许多欺诈案件中，受害者通过移动支付等手段快速实现平台转账，而诈骗者账户一旦到账立马将赃款迅速分散转移出去，给追回资金方面带来了极大困难。一些交易平台通过设置延时到账功能，即转账过程不会立马实现，会有相应的延时，只要用户在延时到款期内及时报案，转账可以原路返回，从而帮助受害者避免损失。

腾讯公司充分利用交易延时到账机制来保障用户账户交易安全。在用户转账交易时及时根据用户的历史交易行为、接收方的可疑程度等多个维度进行可疑判断，并对用户发起预警提示。与此同时，腾讯宾果防诈骗系统及时识别了可疑诈骗线索，并将线索推送至当地警方进行预警，警方收到预警后及时通过去电、短信推送，上门劝阻等多种方式阻断用户的被骗转账行为。最终经过多方努力，成功帮助用户冻结已转账资金，帮用户挽回损失。

2.异常交易的提醒

目前许多平台机构也开展了针对于异常交易的及时提醒，主要针对以下两个方面：一是针对用户大额的交易会通过不同方式综合进行提醒验证；二是针对异常登陆，异常地点支付，异常操作等方面及时提醒用户。平台采取的手段主要包括：输入手机验证码、回答预留问题、直接提示本次交易可能存在异常等。

3.账户管理机制

在账户管理方面，主要采取以下措施：一是针对账户的安全等

级进行分类，针对低安全等级的用户提醒包括建议更换密码，开启支付多重验证等；二是针对存在异常交易和不良交易的账户加强管理，提高针对这类账户交易时的风控标准，限制其部分功能；三是针对一些正常账户与疑似欺诈账户交易时及时提醒该账户可能存在异常情况；四是针对疑似欺诈账户进行关联账户分析识别潜在欺诈账户。

4.平台赔付制度

随着人们消费观念的转变和生活条件的提高，基于互联网平台的消费购物已经成为时尚，并且交易量逐年增加。但是，由于多样化的欺诈手段，平台类的金融诈骗接踵而至，为了保护消费者权益，避免或减少合同纠纷和消费纠纷，一些互联网平台建立了平台赔付制度，确保网络交易安全可靠。以腾讯为例，为保障用户的资金交易安全，财付通与中国人民财产保险股份有限公司进行合作，向用户提供保障计划。在用户出现符合保障计划要求的损失时，用户可以按照保障计划的规定及时申请挽回损失。

六、 数字金融反欺诈未来趋势及建议

（一）监管立法势在必行，完善反欺诈制度体系

近年来，我国数字金融欺诈案件呈现高发态势。然而，对于数字金融欺诈相关的监管法律法规相对缺失。在《刑法》中，虽然规定了“金融诈骗罪”，但更多的是针对传统金融欺诈行为的考量，对于数字金融欺诈的一系列新型欺诈行为仍缺乏明确的法律监管依据。例如针对网络借贷、消费信贷、移动支付等领域的金融欺诈行为，均缺乏明确的法律定罪依据，发生欺诈案件更多依靠最高法的司法解释。总体而言，我国在数字金融反欺诈的识别预警、监管拦截、取证侦破等方面存在较多的法律法规缺失，数字金融反欺诈存在一定的主体缺位、监管机制不完善等问题。

未来，我国应不断完善数字金融领域法律法规，以信息安全保护、知识产权保护、虚拟财产保护等为重点方向。一方面，数字金融领域立法要维护正常的金融秩序，打击数字金融欺诈违法犯罪活动，另一方面是要为新产业、新业态、新模式的发展“保驾护航”，鼓励企业创新数字金融反欺诈工具和手段，强化数字金融反欺诈方面的知识产权保护，激发社会主体参与反欺诈的积极性。

（二）推进行业生态联防，构建协同治理新平台

数字金融欺诈具有跨部门复杂性、跨区域高发性和跨行业隐蔽性等新特点，对反欺诈提出了更高的要求，客观上需要政府监管部

门、金融机构、科技企业以及行业协会等市场主体形成联防联控的生态联盟，反欺诈方式从单个企业的孤军奋战走向跨行业、跨企业的协同作战。例如中国互联网金融协会在 2018 年 3 月份成立了区块链反欺诈联盟，旨在加强对以虚拟货币 ICO 为代表的新型违法违规金融活动的风险提示，协同打击金融欺诈行为。

通过筹建数字金融反欺诈联盟等行业组织，搭建起数字金融反欺诈协同治理的新平台，能够有效整合政府和社会机构的力量，推进欺诈案件的信息共享、数据共享，建立全方位反欺诈联防和信息互通机制，及时识别和预警数字金融欺诈风险，不断加强欺诈的风险管理。例如腾讯曾与招商银行在金融大数据反欺诈领域达成合作，腾讯金融云联合腾讯安全反诈骗实验室，通过 AI 技术把反欺诈能力开放给招商银行，帮助招商银行更好地识别金融业务中的欺诈行为，共建金融安全生态圈。

（三）深入融合金融科技，提升反欺诈防控能力

正如前文所述，通过大数据、人工智能和区块链等新技术能够有效预判各种金融欺诈行为，提示交易风险，通过高效率、低成本的方式，辅助人工做出反欺诈决策。例如：可以利用大数据的获取、整合和处理数据的能力，快速判定异常状况，为防控金融欺诈提供技术支撑；基于机器学习、行为序列、人脸识别、生物探针、关系图谱的人工智能技术能够进行精准画像、判别用户身份，识别潜在风险，提升交易安全性；利用区块链的数据、信息共享机制，有效打击供应链金融欺诈、银行票据欺诈以及保险欺诈。

通过充分利用人工智能、区块链、云计算和大数据技术的特点和能力，贯穿数字金融业务的全流程，建立反欺诈规则、反欺诈引擎、关系图谱、风控模型、态势感知等模块，创新数据收集、加工、建模、识别、匹配等环节的模型和算法，提升反欺诈防控效率。腾讯云的人工智能和机器学习能力，能够准确识别恶意用户与行为，解决客户在支付、借贷、理财、风控等业务环节遇到的欺诈威胁，帮助客户提升风险识别能力，降低企业损失。

（四）普及金融诈骗常识，增强用户反欺诈意识

我国普通消费者的金融知识仍相对薄弱，金融科技能够帮助识别欺诈风险，建立反欺诈策略和手段，但数字金融反欺诈更应注重做好数字金融反欺诈知识的宣传和普及。数字金融欺诈案件体现出一些新特点新手段，而普通消费者的识别能力有限，应明确对消费者进行反欺诈教育的主体责任，政府和企业部门应在数字金融领域做好宣传，普及反欺诈教育和金融消费者权益保护等知识，积极传播反欺诈手段。

特别是以腾讯为代表的互联网企业，基于自身广泛普及的用户沟通渠道，有必要牵头组织各种金融反欺诈教育活动，向社会公众提供获取金融知识的途径，推广防范风险的相关策略技能，采取知识传播和生动案例讲解，来宣传反欺诈重要性，普及识别和防控反欺诈手段。

附录：用户反欺诈教育攻略

一、高利理财类欺诈

1.典型诈骗套路一：代客理财诈骗

①通过短信发布代客理财、投资等信息引诱用户添加或者主动添加用户微信，通过朋友圈发布各种盈利截图，转账截图等，并主动联系用户称可帮用户理财，周期灵活收益高。

②用户通常先用小额尝试，骗子按承诺周期以及利润连本带利返还给用户获取用户信任。

③主动联系用户告知有新的投资产品，利润更高但需加大投资本金，待用户上钩转账支付后卷款跑路。

④用户到期联系不上对方，拿不回本金才意识被骗。

骗术特点：利用广大群众有闲置资金但不懂投资的特点，先让用户稍尝甜头，一旦投入更多资金便会携款潜逃。

防骗原则一：不轻信个人的代客理财

作为个人，我们应明白高收益意味着高风险，不要轻易相信低投入高产出的“投资”，投资前应对投资对象、投资标的进行深入研究，根据自己的实际情况和风险承受能力，选择适合自己的理财产品，而不是轻易地相信某个人。

2.典型诈骗套路二：收费荐股诈骗

骗子冒充“股神”以推荐股票为由，骗取用户钱财的案件。

①骗子主动搭讪，添加用户微信好友，并长期通过朋友圈宣传股票推荐信息以取得用户的信任。

②已跟着“股神”赚钱为诱饵，将用户拉进所谓的投资群；

③投资群内有很多托，假装在“股神”的指导下有超高的收益率，并营造出不少用户在“股神”的指导下都小赚了一笔的假象，刺激用户寻求“股神”指导。

④用户上钩后，“股神”以一对一指导收取高额的指导费、推荐费，而用户不仅付出了高额的费用，还在不准确的信息下血亏。

骗术特点：利用广大群众对股市的追捧，以跟着股神赚钱为诱饵，形成一个小圈子。群内的托谎称在股神的指导下有超额收益，引诱用户上钩，骗取指导费。

防骗原则二：不轻信“股神”的专业推荐

所谓的专家，往往都是拿着市场上可以公开得到的信息来兜售，即使存在套利机会，一旦有所谓专家的存在，机会便稍纵即逝。对于投资者来说最好的方法是自己懂一些技术分析。

二、网络贷款类欺诈

3.典型诈骗套路三：网络贷款诈骗

①用户接听虚假贷款业务员电话后添加对方微信号，首先了解贷款方式、额度以及贷款前所需要的个人所有信息。

②提供对应贷款的页面信息给到用户,并让用户签订贷款协议,用户放松警惕确认对方可帮忙贷款。

③对方声称已提交贷款业务,需缴纳担保费,手续费,保证金等虚

假流水证明等服务费用（用户期间若有所疑虑，对方还会提供公司营业执照、工作证、身份证等信息获取用户信任）。

④服务费用已转账，再联系对方核实办理进度，对方未理会或被拉黑，电话关机，已联系对方协商无法退回，用户意识被骗。

骗术特点：犯罪分子通过电话、短信散布能够贷款的虚假信息，一旦当事人与之联系便会告知必须预先支付 1 万至几万的保证金或者部分利息。利用当事人急于用钱的心理，放松警惕，给了犯罪分子可趁之机。

防骗原则三：不乱点陌生人的“雪中送炭”

谨防急需资金、无需抵押的心理被人利用，不轻信陌生人的“雪中送炭”，不要相信愿意垫付部分资金等假象信息，要辨识短信和网站的真实可靠性，此类号码多数为外地号，或者模拟号，而且服务器不在我国境内的多为虚假网站。

4.典型诈骗套路四：额度强开诈骗

①通过微信朋友圈以及各种论坛发布广告信息，声称可以强开微粒贷、蚂蚁借呗等额度，仅需支付少量手续费，并附上大量成功案例截图（自己制作成功案例聊天记录，高额度截图）

②待用户主动联系，骗取用户支付手续费，后续提供用户所需额度的假截图界面让用户相信可以开通，再以需要用户支付担保金或证明还款实力为由让用户支付资金，并告知该笔资金在开通微粒贷、蚂蚁借呗后均会返还给用户。

③待各种理由诱导用户支付多笔用户不愿再支付或用户已意识

被骗后拉黑。

骗术特点：犯罪分子利用朋友圈宣布可以强开微粒贷、蚂蚁借呗等额度，继而骗取用户手续费、担保金。

防骗原则四：不随意相信通过个人可以强开额度

微粒贷、蚂蚁借呗已逐渐成为越来越多年轻人消费习惯的一部分，犯罪分子抓住人们提前消费导致额度不够的心理进行诈骗。为此，我们不要随意相信通过个人可以强开额度，真要提高额度需要查询官网或者咨询客服。

5.典型诈骗套路五：信用卡提额诈骗

①通过微信朋友圈以及各种论坛发布信用卡提额广告信息，并附上大量成功案例截图（自己制作成功案例聊天记录，高额度截图）。

②待用户主动联系，通常会以贷款公司或银行工作人员的名义称可以帮用户提额，若用户质疑，期间会提供公司营业执照以及工作证、工牌（假的）来打消用户疑虑。

③待用户相信之后，以手续费、包装费为由或者以需要“刷流水”等理由骗取用户资金。

④用户支付多笔不愿继续支付后，拉黑用户。

骗术特点：不法分子利用现代媒体的传播效力，一旦有用户主动联系，便开始场景化诈骗，伪造信息，冒充银行工作人员，分分钟让不懂操作流程的用户上当受骗。

防骗原则五：不轻信信用卡提高额度

对于此类诈骗，不要轻信自己不了解的信息。骗子定位到需要用钱的用户后，投其所好，对症下药。一旦对方再能提供证明自己身份的信息，我们便放松警惕，给了对方可乘之机。最好的防骗措施是亲自到银行等地去核实，不要单凭对方几句话就绝对相信，尤其是涉及到钱财的事情一定要慎重。

三、网络众筹类诈骗

6.典型诈骗套路六：共享单车众筹诈骗

①主动添加用户好友，通过朋友圈发布广告，以缴纳固定金额资金认购共享单车，由其公司统一运营投放市场，每天返还一定金额共享单车运营收益。

②用户交钱认购单车后统一拉群管理，固定发放承诺收益。用户拿到收益后信以为真，推荐周边朋友加入并获得推荐奖励。

③待一定量用户认购单车，资金累计到一定程度，骗子散群卷款跑路，用户意识被骗。

骗术特点：犯罪分子利用某圈、某论坛、某公众号，利用热点词汇非法集资，由于媒介的非接触性和广泛传播性，使得虚假信息得以广泛传播。

防骗原则六：不轻信无正规渠道的集资信息

利用社交媒介的广泛传播性，利用某圈使得诈骗人数信息得以指数化增加。谣言止于智者传播，不要贪图小恩小惠，对于无正规渠道的集资信息仔细辨别，不要盲目转发。

7.典型诈骗套路七：电影众筹诈骗

APP 金谷影视疑似涉及虚构电影投资项目，宣传投资后有大额资金回报，经调查核实疑似套用互联网金融概念的非法集资电影投资项目，极有可能套现跑路给用户带去大额损失。

骗术特点：犯罪分子利用某圈热门影视剧的概念非法集资电影投资项目，由于影视化制作过程涉及众多，一旦集资成功极易造成道德风险，形成跑路现象。

防骗原则七：不轻信电影众筹

用户不要被低投资高回报的宣传广告所吸引，电影制作涉及领域人员众多，不可控因素极大。对于电影众筹项目保持警惕。

四、消费金融类欺诈

8.典型诈骗套路八：网购退款赔付诈骗

①冒充天猫客服致电客户，告知客户由于工作人员操作失误，无意中帮用户开通了一个付费铂金会员业务/加盟商业务，每个月只要银行卡有余额就会扣除 500 元费用，如需取消，客户必须联系银联获取凭证取消。

②帮客户转接假冒的银联客服电话。银联客服引导客户把各类贷款借出，并说借出后转入一个监管帐号，银联要核对用户的信用总额，才能给客户凭证，后续资金后会退回。

③引导用户通过手机浏览器打开虚假的银联网站用于核对业务信息客户按照指引操作，在对方指引的多个贷款平台中借款后转入对方指定的银行卡。

④支付多笔后，资金并未退回用户才发现被骗，期间一直与对方电话沟通。

骗术特点：利用网购场景及人们对客服的信任，设计陷阱引人上钩。

防骗原则八：客服来电需要警惕

随着网购场景的普及化，骗子的作案方式、作案场景越来越接近日常大众。对此,用户的防骗意识也要随之升级，尤其是涉及到银行卡、汇款的问题，要保持时刻警惕。由于客服人员造成的损失，应由客服来解决，我们自身不用慌张。

9.典型诈骗套路九：刷单兼职诈骗

①通过短信/社交网络/58 同城/赶集网等宣传兼职信息

②加好友/加群/加语音房间，渲染刷单高额利润/简单操作/时间自由，告知任务流程与规范，同时强调公司资质，有担保平台等，打消疑虑

③获取用户姓名/手机/收货地址/支付账号/账号余额等信息，做入职登记。

④骗子引导用户开始通过淘宝店下单，拍下商品截图不必付款，通过其提供的二维码扫码支付完成付款（首单一般金额较小，及时返回本金+佣金，以诱导用户入局）。

⑤后续任务多为多个订单叠加模式，且金额大，以各种隐性条款/系统问题为由不予结算，期间为躲避拦截变换多种支付方式（支付宝+微信），例如扫码 C2B 支付给商户，如果被拦截就为用户“申

请”拍下商品后通过红包支付，或通过转账到银行卡支付订单等多种方式轮换。

⑥若用户起疑，骗子就提供公司工商注册资料安抚或以不按要求做任务将延迟结算为由威胁用户。

⑦用户发现被骗后，骗子拉黑用户、以捣乱为名踢出群/房间

骗术特点：犯罪分子利用高薪、工作时间自由为诱饵，提供资质证明使受害人相信。一旦受害人起疑就以不按要求做任务将延迟结算为由威胁。

防骗原则九：不劳而获的兼职需慎重考虑

针对此类诈骗，我们不要相信天上掉馅饼的事情，不轻信有既高薪又轻松的工作。尤其涉及到需要自己先垫资更要保持高度警惕。

10.典型诈骗套路十：冒充客服诈骗

①在论坛、搜索网站等发布电话号码信息，伪装小贷公司客服。

②部分使用相关贷款平台的用户为咨询还款方式等自行网上搜到假冒的客服电话，拨打咨询后对方引导用户添加“客服”微信。

③引导用户直接转账还款或提供“财务银行卡”让用户转账还款

④用户后续接到真正的贷款平台客服电话提醒还款，意识之前上当受骗。

骗术特点：利用社交平台、搜索网站发布的信息，吸引资金需

求者，假冒客服人员进行诈骗。

防骗原则十：不轻信他人提供的网站、电话

骗子可以通过钓鱼网站、改号软件窃取你的个人信息，改造成任意的电话，因此不要轻信他人提供的网站、电话，去正规官网去检索。

11.典型诈骗套路十一：伪装成公检法诈骗

①骗子电话联系用户，自称是公安机关，表示用户在海关查走私、贩毒等案件发现用户名下银行卡，怀疑用户涉及走私、贩毒等，或者告知用户身份涉及电信诈骗等。

②称现在检查机关要追查案件，同时告知用户身份证信息也可能被他人冒用，为了查清案件帮用户洗清嫌疑，需要验证客户的身份信息以及目前用户的资金是否是正常渠道得来的，让用户将名下资金转入对方提供的安全账号内。并且对方也告诉用户所验证的资金确认无误后会退回，期间骗子还可能一步步诱导进行了借款，让用户将借款到账后进行验证转账到所谓的安全账户。

③待用户不愿再配合转账或借款支付，或者用户意识到被骗后，挂机拉黑。

骗术特点：利用群众对公检法部门的陌生与畏惧，通过改号软件将来电显示设置为“110”等政府机关的号码，称涉嫌诈骗、贩毒、洗黑钱等犯罪，然后要求将银行卡的钱全部转入“安全账户”进行审核。

防骗原则十一：警惕陌生短信和来电

针对此类诈骗行为，我们应明白公检法等国家机关工作人员执行公务时，一定会持相关法律手续当面询问当事人，不可能通过电话要求转账，所谓“安全帐户”也是子虚乌有，凡是自称国家机关要求把钱汇入安全帐户的都是诈骗，对此切勿相信。电商客服、银行、民航等，因来电显示可改号，所以均要以自己主动拨打官方电话核实为准。

12.典型诈骗套路十二：高额返利诈骗

①骗子加好友后会长时间潜伏在朋友圈，会统一使用美女头像，昵称统一为“张可欣”“陈诗涵”“颖颖 baby”等女性化昵称。

②通过朋友圈宣传遇到富二代渣男，渣男分手后给了她一大笔微信零钱作为补偿。

③宣传让男性用户给她转 520,1314,3344 等特殊金额，会给予十倍资金返还，为了截图气死渣男。（会附上部分 PS 的成功返还的聊天记录以及转账记录截图）

④用户信以为真，贪小便宜，多次转账后未收到对方返现才意识被骗。

骗术特点：编造一个拥有钱财只为气前男友的故事，利用男性容易对美女放松警惕、爱贪小便宜的心理，结果往往得不偿失。

防骗原则十二：不贪图朋友圈他人钱财

对于陌生人的朋友圈内容我们不要尽信，尤其是对方炫富、有什么悲惨故事的内容，如果对方不是你亲朋好友或者有工作上往来

的人可以直接拉黑。

13.典型诈骗套路十三：机票改签退款诈骗

①以航空公司的客服人员名义，电话联系用户（或者通过短信通知），告知用户所定航班停飞了，随后引导添加微信，会有专人引导退款。

②待用户添加“客服”微信后，对方用群收款的方式，诱骗用户转账，用户以为是对方转账过来，就输入密码支付。

③用户支付后，对方会以网络故障未退成功，操作失误扣错款为由让用户重新支付。待用户多次支付或识破骗局后拉黑用户。

骗术特点：假冒航空公司客服人员，以航班停飞需要退款为由引导用户转账，再以网络故障、操作失误为由多次支付，用户识破后即被拉黑。

防骗原则十三：通过正规渠道辨别信息真伪

骗子的目标即为需要用户转账支付，为此会编制如机票改签退款等理由。当有航空公司客服人员联系时，尤其是涉及到转账退款时，要保持格外警惕，最好是查询相关订票软件，通过正规渠道自主联系客服询问具体情况。

14.典型诈骗套路十四：冒充微博好友诈骗

①盗取或伪冒用户微博，通过私信联系用户亲友，以本人在国外现准备回国，钱包丢失或者由于自己银行卡转账到账时间久，急需支付购买机票为由，让亲友代为支付。

②提供航空公司“票务经理”的手机、微信亲友联系，后续引

导亲友支付。用户亲友在轻信骗子的情况下转账。

③后续联系上真是用户核实后才发现被骗。

骗术特点：利用人们好面子，不好意思针对“熟人”询问，听不出来对方的弱点，不核实对方身份，轻信于他人，面对“熟人”给出的汇款理由，放松警惕，轻易将钱财转给他人。

防骗原则十四：通过其他途径确认朋友消息是否属实

当接到自称“老朋友”“猜猜我是谁”电话时，要保持高度警惕，注意核实对方身份，必要时向老朋友电话核实或者向相关办案部门了解，不要轻易相信对方的种种理由而给其汇款。

【主编】

何宝宏　中国信息通信研究院云计算与大数据研究所所长

许国爱　腾讯金融科技副总裁

【统筹策划】

张雪丽　中国信息通信研究院云计算与大数据研究所副所长、金融科技研究中心主任

蓝烈华　腾讯金融科技副总裁

【研究撰写】

何　阳　中国信息通信研究院云计算与大数据研究所金融科技研究中心产业咨询部主任

韩永娟　中国信息通信研究院云计算与大数据研究所金融科技研究中心研究员

许一骏　中国信息通信研究院云计算与大数据研究所金融科技研究中心研究员

王春蕊　中国信息通信研究院云计算与大数据研究所金融科技研究中心研究员

周治明　腾讯金融科技风险管理部高级总监

吴　鸣　腾讯金融科技风险管理部总监

黄杰威　腾讯金融科技风险管理部总监

宋丽婷　腾讯金融科技风险管理部项目经理

李永斌　腾讯金融科技风险管理部工程师

赵　维　腾讯金融科技风险管理部工程师

王　钧　腾讯金融科技智库首席研究员

曾美娜　腾讯金融科技智库高级研究员

郭　倩　腾讯金融科技智库高级研究员

数字金融反欺诈
——洞察与攻略