

数字经济背景下商业银行反欺诈风险防控策略面临的挑战及完善方法 ——以中国工商银行为例

Challenges and Improvement Methods of Commercial Banks' Anti Fraud Risk Prevention and Control Strategies under the Background of Digital Economy

—Taking Industrial and Commercial Bank of China as an Example

徐晓琳

Xiaolin Xu

哈尔滨工业大学 中国·黑龙江 哈尔滨 150000

Harbin Institute of Technology, Harbin, Heilongjiang, 150000, China

摘要: 目前,中国线上经济蓬勃发展,2022年数字技术已经广泛扩展到智能化支付、智慧型网点建设等多领域,数字技术的推广也推动了金融业务模式的多样化和灵活性。但是,数字经济背景下的金融欺诈金额不断攀升,论文以中国工商银行(以下简称工商银行)为例,分析中国工商银行反欺诈风险防控策略存在的问题并给出完善方法,为反欺诈防控策略体系建设提供参考。

Abstract: At present, China's online economy is booming. In 2022, digital technology has been widely extended to intelligent payment, smart network construction and other fields. The promotion of digital technology has also promoted the diversification and flexibility of financial business models. However, the amount of financial fraud in the context of the digital economy continues to rise. Taking Industrial and Commercial Bank of China (hereinafter referred to as ICBC) as an example, this paper analyzes the problems existing in ICBC's anti fraud risk prevention and control strategy and provides improvement methods to provide reference for the construction of anti fraud prevention and control strategy system.

关键词: 反欺诈; 风险防控策略; 商业银行; 风险; 数字经济

Keywords: anti fraud; risk prevention and control strategy; commercial banks; risk; digital economy

DOI: 10.12346/emr.v4i5.7263

1 数字经济下商业银行反欺诈概述

1.1 数字经济下反欺诈发展情况

1.1.1 数字经济下商业银行反欺诈内涵

数字经济是以数字化的知识和信息作为关键的生产要求,具体包括数字产业化、产业数字化、数字化治理和数据贾志华。数字经济下商业银行反欺诈是指利用数字技术进行金融反欺诈,即通过数字化技术进行识别并且防止欺诈行为的发生。充分利用人工智能神经网络、大数据等先进技术,架构一套完整的风险防控策略体系,从传统的事中规则校验等反欺诈手段,衍变为主动出击,提前阻止反欺诈行为的

发生,从而化被动为主动,在欺诈行为发生前进行主动拦截,具有跨行业、高准确度等特征,以毫秒级为单位进行拦截,并且能够依靠高容量实验室进行模型建设和风险智能化决策。

1.1.2 数字化经济下反欺诈发展

①数字化转型下反欺诈形势不容乐观。

疫情催化下的数字经济发展速度之快,前所未有的,2021年,中国数字经济规模达到45.5万亿元,同比名义增长16.2%。数字经济已然成为推动金融转型升级、服务实体经济的重要抓手,在这样的大背景下,反欺诈风险随之上升,

【作者简介】徐晓琳(1991-),女,中国黑龙江七台河人,硕士,初级经济师,从事区域经济、企业管理研究。

反欺诈风险防控升级也亟须提上日程。随着数字经济的发展,网上银行、移动支付等线上的金融服务不断壮大,带来了高额利润的同时,也带来了高风险。在利益的驱动下,不法分子通过广告、某多多砍一刀等多种形式化手段盗取客户的资金或个人信息。如何有效构建反欺诈风险防控策略,阻止分工专业、精细的黑色产业链给客户及企业造成的损失,是金融机构亟须解决的问题^[1]。

②技术迭代加速反欺诈效能

数字经济下,高速的发展催生了新型的欺诈犯罪行为,数字经济背景下的金融欺诈也属于犯罪行为,相对于线下的金融欺诈和互联网的一些欺诈手段,数字化经济下的欺诈手段更具有联合作案的特征,且黑色产业链较为成熟,欺诈的场景更为复杂化,给数字金融的普及和技术的创新带来了影响的同时,金融机构也因此面临风险防控的严峻挑战。

2 中国工商银行反欺诈风险防控状况及面临的挑战

2.1 中国工商银行基本情况介绍

中国工商银行总部位于中国北京市复兴门内大街55号,是一家大型国有商业银行,按照国家法律法规为中国经济建设服务。2022年,工商银行资本充足率18.31%,不良贷款率1.41%。上半年境内人民币贷款新增1.61万亿元,投向制造业中长期贷款及信用贷款余额均突破1亿元,普惠贷款户数较年初增加12.3万户,较年初增长27.4%。6月末,本外币各项存款余额(含同业存款)突破20万亿元,客户总量突破1000万户。随着业务的不断发展,反欺诈风险也随之上升,如何在保证盈利的前提下有效防范反欺诈风险,是亟待解决的问题。

2.2 中国工商银行反欺诈策略现状介绍

中国工商银行从传统的事中识别,发展到从事前、事中、事后三个阶段进行风险预警或识别。具体三阶段防控如下。

①事前预防主要采用客户画像。

工商银行利用技术性的手段在金融服务客户端和网络公开信息中查找、搜集、整合数据,多维度多渠道的金融数据是使用金融科技反欺诈工具的基础。通过海量丰富的数据信息流,可以形成更为全面的用户画像。在获得用户画像之后,更可以结合不同用户的数据内容,如共用IP地址、通讯记录、交易记录等,构建包含海量用户的大数据关系图谱,有效防范团伙欺诈行为。

②事中应对主要采用欺诈拦截。

因应不同欺诈场景,反欺诈可以采取更具针对性的干预措施。第一类措施是通过金融科技反欺诈系统精准识别风险用户,防范并拦截金融欺诈行为,辅助互联网金融平台过滤可疑信息量。第二类措施是对金融平台上的交易行为进行风险估测,拦截可疑交易并通过验证码或人工方式进行核实,且在后台登记交易拦截记录甚至冻结欺诈者的账号。第三类

措施是借助数据库和反欺诈模型审核互联网金融平台的用户资料,提前阻止黑名单和高风险用户的金融服务申请,并利用核心算法对所有用户进行风险评估^[2]。

③事后溯源主要是数据挖掘。

对于已经发生的欺诈事件,企业可以利用相关日志溯源,挖掘整个犯罪过程,帮助同业及时预警,防范更多欺诈事件的发生。基于知识图谱的黑产特征挖掘方法被提出,将知识图谱思想和机器学习算法结合,以恶意欺诈账户为分析源,从多个维度挖掘关系属性,实现多源数据融合建模,并利用算法智能识别强关联账户,从复杂的数据关联中汇总梳理发现隐藏关系,进而暴露黑产团伙。

2.3 中国工商银行反欺诈策略面临的挑战

随着数字化背景的延伸,欺诈的手段也在不断升级,工商银行面临的挑战随着欺诈手段不断升级,论文仅讨论欺诈手段带来的挑战。

2.3.1 欺诈手段更加专业化

目前的欺诈手段呈现场景化,常见的数字金融欺诈场景有网络借贷、网络支付、消费金融和供应链金融等。在网络借贷场景、账户注册阶段,欺诈者采用伪造身份注册、冒用他人身份注册、自动化垃圾注册等手段完成注册;在账户登录阶段,欺诈者的金融账号往往存在盗用、冒用、异常共享等行为;在贷款申请阶段,欺诈者通过提供虚假申请信息获得超额贷款;在还款阶段,欺诈者可能恶意拖欠,或利用非法取得的他人信用卡进行欺诈性交易^[3]。在网络支付场景,黑色产业团伙往往通过社会工程学方式与技术手段,如虚假WiFi等,盗取个人姓名、手机号码、身份证号码和银行卡号等直接关系账户安全的要素信息,用于精准诈骗、恶意营销。

2.3.2 欺诈手段快速迭代

根据公安部数据统计,数字金融欺诈手段快速发展,目前已经形成了互联网社交软件诈骗、车票机票退改签诈骗、虚假购物消费诈骗、虚假网站和链接诈骗等至少18类诈骗手段,并且诈骗手段仍在持续快速更新和发展。仅在2018年,网上信用卡诈骗、网上购物退款诈骗及利用社交平台伪造身份诈骗等诈骗案件共立案38.6万起,占网络诈骗案件总数的61.8%(公安部数据)。

截至目前,科技欺诈手段呈现以下发展趋势。一是覆盖面更广。犯罪分子在实施犯罪的过程中通过电话、短信、社交平台、网络等手段,地毯式发布虚假信息,造成较大范围的损害。二是手段更新更快。诈骗分子的犯罪手段层出不穷,从一开始只是利用冒充电话、虚假中奖短信等简单实施犯罪。三是反侦查能力更强。在诈骗案件中,犯罪团伙往往有细致的分工,并且采取远程的非接触式的诈骗。

2.3.3 欺诈产业链分工精细化

欺诈属于技术含量高、流程复杂的高智商犯罪,以团伙联手的产业链或供应链方式,使整个作案流程化,构成一定

的欺诈系统。信息源、协作方、实施方相互合作，彼此交融，涉及欺诈金额巨大，涉案人员众多，形成一条犯罪产业链，造成了严重的不良社会影响。具体而言，欺诈产业链主要包括诈骗源头、信息贩卖、诈骗实施、资金转移分赃几部分。欺诈产业链第一部分为诈骗源头。对于当今组织化规模化越来越强的欺诈团伙来说，各类账号已经成为欺诈的核心资源，各类欺诈工具是欺诈者获取批量收益的基础。欺诈账号的来源主要包含注册和盗号两类渠道。欺诈产业链第二部分为信息贩卖。个人信息批发商从黑客和线下信息收集者手中购买用户数据，而钓鱼网站批发商则购买木马和钓鱼网站。欺诈产业链第三部分为诈骗实施。诈骗实施者通过组合资源与基础工具，把所有核心资源串联起来，形成各作恶场景的业务工具，提升作恶效率。欺诈产业链第四部分为资金转移。诈骗得手后，资金将会转入一个不属于诈骗者名下的银行账户，然后迅速将资金在多个账户中转移并逐步分散至上百个账户内，期间还可能利用第三方支付平台，以此提高警方侦查难度。为了提高安全性，甚至有诈骗团伙通过将资金转移到海外再转回的方式规避监测。

3 中国工商银行反欺诈风险防控策略完善措施

3.1 强化员工培训

疫情的影响下，传统的方式方法已经无法更好地适应数字背景下的欺诈手段。当下更需要技术和业务都相对熟练的高复合型人才，如建模人才、大数据人才等。所以，面对这一现状，亟需加强对高复合型人才的培养。一线员工对业务较为熟练，但是对技术的了解和使用相对薄弱，所以可以开展一些有针对性的技术类培训，将日常一线工作中会接触到、涉及的技术性知识进行归纳梳理，也便于一线员工在日常工作中加深对业务知识的理解及增强对客户服务的体验感。同时，对于后台的技术专业员工，要持续强化业务知识的培训，技术的加持实际上还是为了一线业务服务。当技术和业务高度融合时，才能更有效强化对欺诈风险的反制。

此外，人事部门可以积极探索适合人才激励的薪酬体系，将培训与薪酬挂钩，提升员工的主动性和积极性，对于成效较好的培训项目可以进行奖励，从而有效推广优质培训项目在行业内的推广。

3.2 筑牢技术系统防线

随着数字化经济时代的来临，黑色产业也逐渐向着智能化与集团化发展，线上与线下的高度融合，欺诈手段越来越隐蔽，并且呈现出了跨越行业的欺诈行为。针对庞大繁杂的欺诈产业链，建立一套连续的、一致的数据流是整个反欺诈系统运行的关键。但是数据流的建设就意味着个人信息安全要在数据流中运行，所以如何有效保障个人信息安全，是系统防线建设的一大重要课题。目前，央行对个人信息监管不断加强，个人信息也具有极高的价值。对于核心数据的管理，既要做到加强隐私性，又要做到在不泄露客户个人信息及模

型资产的前提下进行数据的梳理和分流，达成模型所需数据需求，进而完成共享数据的价值。目前，业务场景安全策略与业务风险防护仍然没有统一标准，所以目前面临技术与业务的冲突。所以，如何从技术层面改进，系统性做好身份的识别、交易判定等重要环节的高质量实时安全把控，做好业务与技术的平衡，也是技术层面需要创新的主攻点。

3.3 做好反欺诈宣传教育

虽然监管机构每年会要求开展“3.15 金融消费者权益保护日”“钱袋子”宣传等强制性宣传活动，但是对于低净值人群、老龄化群体等特殊群体，还需要培养反欺诈意识。一是做好金融相关的法律法规、政策的宣传讲解，才能更好地让金融消费者了解到“红线”，从而有效提升对于自身的保护意识。二是针对喜闻乐见的金融欺诈案例进行宣传和讲解，深入老年大学、教科书等多渠道多角度宣传，针对欺诈案例通过专业化的讲解，模拟诈骗的场景，可以有效提升群众对欺诈的认知。三是充分利用LED屏、宣传手册、微信群等渠道开展形式多样的宣传教育手段。结合当前时事热点，如苏州某物业公司，针对欺诈案例悬挂条幅，通过趣味性的反欺诈案例引导，以喜闻乐见的方式向群众宣传了反欺诈知识。当下如热议较高的“老陈”，通过抖音直播的形式向群众普及反欺诈知识，目前有很多的公安分局、金融机构等也在利用抖音、快手、微信公众号等塑造网红形象大使的途径向广大群众宣传反欺诈知识。

3.4 完善法律法规

虽然国家已经出台了《网络安全法》《个人信息保护法》等相关的法律依据，国家对于欺诈的监管也在逐步清晰，但是在具体的操作中还是会出现不明确的问题。尤其是一线工作人员，由于日常工作较为繁重，身兼数职，对于业务知识的日日更新已经自顾不暇，业绩考核压力威胁到了绩效，所以疏于对相关法律法规的理解和深度探索。针对这一实际问题，应该继续完善聚义要求，对于技术标准等仍然需要进一步的细化。尤其是数据要素的合理利用，作为有效防范反欺诈风险的要素，需要进一步细化要求。在明确梳理数据的使用权问题后，还需要逐步探索适应当下实际数据化中面临的市场化流转机制和技术基础，才能有效加快多层面上的数据交易市场流动。对于法律法规完善问题，可以采用试点实验的方法。在不影响效力的基础上采取试点实验，选取多个样本试验点，将具体操作进行测试，并根据遇到的实际情况进行不断的修改和完善。

参考文献

- [1] 李志刚,张文宾,高倩倩.个人客户智能化风险监控场景研究与实践[J].现代金融导刊,2021(1):87.
- [2] 刘超.商业银行信用卡风险与防范对策研究[J].现代商贸工业,2019,9(12):25-28.
- [3] 周晓军.对互联网金融背景下“羊毛党”的评析及管控对策研究[J].法制与社会,2017(27):75-76.