护航数字经济 监管力促网络安全保险

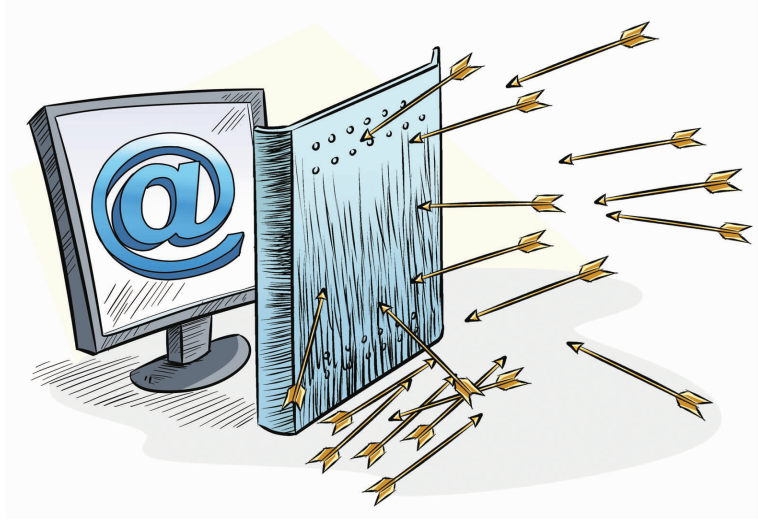
本报记者 陈晶晶 广州报道

截至2022年，我国网民规模达10.67亿，互联网普及率高达75.6%。与此同时，我国数字经济规模达50.2万亿元，占GDP比重提升至41.5%。数字化时代，数据成为生产资料，计算能力成为生产力，互联网成为生产关系。但同时也滋生了数据泄露、数据损毁、网络攻击等网络风险，成为影响人们生产与生活的新型风险。

而网络安全保险是为网络安全风险提供保险保障的新兴险种，是转移、防范网络安全风险的重要工具，在推进网络安全社会化服务体系建设中发挥着重要作用。发展网络安全保险，有利于助力网络强国建设，护航我国数字经济可持续发展，也是加快形成“发展+安全”双轮驱动发展态势的关键举措。

公开数据显示，2022年，我国网络安全保险整体保费规模约为1.4亿元，虽然较2021年翻一番，但与全球网络安全保险百亿美元的市场规模还有很大差距，一定程度上存在供需双冷的问题。

《中国经营报》记者注意到，近日，工业和信息化部与国家金融监督管理总局联合印发《关于促进网络安全保险规范健康发展的意见》（以下简称“《意见》”）。作为我国网络安全保险领域的首份政策文件，《意见》从当前我国网络安全保险亟待解决的问题出发，围绕完善政策标准、创新产品服务、强化技术支持、促进需求释放、培育产业生态提出5方面10条意见。



近日，工业和信息化部与国家金融监督管理总局联合印发《关于促进网络安全保险规范健康发展的意见》。 视觉中国/图

5方面支持网络安全保险

工信部将从政策宣贯、标准研制、试点推广、生态培育等方面进一步深化工作部署，推进网络安全保险工作。

《意见》提出，要建立健全网络安全保险政策标准体系、加强网络安全保险产品服务创新、强化网络安全技术赋能保险发展、促进网络安全产业需求释放、培育网络安全保险发展生态等五大内容。

其中明确，要完善网络安全保险政策制度。加强网络安全产业政策对网络安全保险的支持，推动网络安全技术服务赋能网络安全保险发展，引导关键信息基础设施保护、新兴融合领域网络安全保障等充分运用网络安全保险。加强保险业政策对网络安全保险的支持，指导网络安全保险创新发展，引导开发符合网络安全特点规律的保险产品。推动健全完善财政政策，充分利用地方首台（套）、首版（次）等现有政策，提供保险减税、保险购买补贴等措施。健全网络安全保险标准规范。支持网络安全产业和保险业加强合作，建立覆盖网络安全保险服务全生命周期的标准体系，统一行业术语规范，明确核保、承保、理赔等主要环节基本流程和通用要求。研究制定承保前重点行业领域网络安全风险量化评估相关标准，规范安全风险评估要求；承保中网络安全监测管理服务相关标准，规范监测预警方法；承保后理赔服务实施要求相关标准，规范网络安全保险售后服务。

记者注意到，《意见》还鼓励各方主体积极推进网络安全保险产品和服务创新。在产品创新上，鼓励保险机构面向不同行业场景的差异化网络安全风险管理需求，开发多元化网络安全保险产品。一是面向重点行业企业开发网络安全财产损失险、责任险和综合险等，提升企业网络安全风险应对能力。二是面向信息技术产品开发产品责任险，面向网络安全产品开发网络安全专门保险，为信息网络技术产品提供保险保障。三是面向网络安全服务开发职业责任险等产品，转移专业技术人员在安全服务过程中因人为操作可能引发的安全风险。服务创新方面，鼓励网络安全保险服务机构协同合作，探索构建以网络安全保险为核心的全流程网络安全风险管理解决方案。一方面，充分发挥保险机构专业优势，联合网络安全企业、基础电信运营商等加快保险与网络安全服务融合创新；另一方面，充分发挥网络安全企业、专业网络安全测评机构技术优势，联合保险公司提升网络安全保险服务能力。

工信部网络安全管理局表示，下一步将从政策宣贯、标准研制、试点推广、生态培育等进一步深化工作部署，深入推进网络安全保险工作。

有望开辟千亿级市场

跨行业、跨领域开展网络安全保险，成为保险行业发展的又一市场增长点，有潜力挖掘一个千亿乃至万亿级的蓝海市场。

近期，国家工业信息安全发展研究中心发布的《网络安全保险研究报告》（以下简称“《报告》”）显示，我国网络安全保险产品供给能力有限，较难满足多样化需求，发展共识尚未形成，跨行业领域认知壁垒较难突破。

目前，网络安全险存在“供需双冷”的问题，即保险企业“不愿投保”、保险公司“不敢承保”。

“一方面，从需求侧看，网络安全保险仍属于新兴业务，产品形态复杂，市场的接受度提升需要一个过程；另一方面，从供给侧看，承保初期，保险公司在风险评估、定价及服务方面专业力建设滞后，无法提供充足的承保能力。因此，加强产品、服务和模式创新，强化网络安全技术对保险的赋能发展，充分发挥网络安全保险在风险管理中的作用，已经成为各相关方的重要任务。”中国人寿财产保险股份有限公司副总裁傅天明撰文表示。

值得一提的是，近年来，保险行业已开展一些“保险+服务”的有益尝试，主要包括：以保险产品为核心的风险减量管理模式；以安全产品为核心的剩余风险保障模式。除上述两种模式以外，行业也在积极开展针对细分领域的创新模式探索，例如普惠保险、个人网络安全保险、供应链网络安全保险等，为保险服务网络安全提供了更多颇有价值的发展路径。

根据《报告》，目前我国共有30余家保险公司备案了78款网络安全保险产品。其中，2022年新增网络安全保险产品数量24款，是上一年备案产品数量的两倍以上。2022年，我国网络安全保险的保费规模为1.4亿元，虽较上一年翻一番，但不足财产保险保费规模的万分之一，相较全球近百亿美元的保费规模也还有很大发展空间。

《2022年网络安全保险科技白皮书》也显示，目前，由于全球IT网络发展的起步时间不一、发展进程不对称，网络安全保险在各国各地区存在不同的市场成熟度与社会普遍接受度。我国在网络安全保险行业正处于发展前期，并开始进入风口阶段。与此同时，借助科技手段，跨行业、跨领域开展网络安全保险，成为保险行业发展的又一市场增长点，有潜力挖掘一个千亿乃至万亿级的蓝海市场。

需各方协同推进

探索网络安全保险本土化应用，推进网络安全服务模式创新，需要保险行业、网络安全行业等多方凝聚共识、形成合力。

众安保险相关负责人接受记者采访时表示，网络安全保险区别于传统保险模式，它的发展无法脱离网络安全服务和技术支撑。在网络安全保险的完整业态中，网络安全企业采取网络安全技术与服务，协助保险公司为客户方提供全面风险管理方案；保险科技公司针对场景化网络安全风险，协助保险公司基于数据清洗整合优势，优化风险定价模型、构建全流程保险业务体系；第三方风险管理技术机构则将网络安全企业的安全技术能力与保险科技公司的科技能力进行有机整合，逐渐成为保险生态中关键一环。

“探索构建以网络安全保险为核心的全流程网络安全风险管理解决方案，首先，需要网络安全产业与网络安全保险产业深度融合，由产品粗放式绑定向产品服务深度转变；其次，由于网络安全保险不同于传统的物理承保的险种，其通常具有虚拟性，且不受地域限制，这也为产业融合降低了技术门槛，加速了服务耦合；最后，围绕多层次的市场需求，网络安全保险的产品与服务进一步细化，全方位开发网络安全保险产品体系，丰富网络安全保险细分险种，提供解决方案。”上述众安保险相关负责人进一步表示。

对于如何在新形势下加快网络安全保险创新发展的思路，国家工业信息安全发展研究中心主任、党委副书记赵岩公开撰文提出，探索网络安全保险本土化应用，推进网络安全服务模式创新，需要保险行业、网络安全行业等多方凝聚共识、形成合力。一是坚持标准引领，完善网络安全保险流程机制。加快构建系统、科学、规范的网络安全保险标准体系，加强对网络安全保险发展的指导和规范。二是坚持创新驱动，促进供给能力有效提升。充分发挥各方主体优势，探索发展以网络安全保险为核心的全流程网络安全风险管理解决方案。三是坚持技术赋能，强化网络安全风险应对。探索网络安全技术改进优化，强化对网络安全保险关键业务环节的赋能作用。四是坚持生态协同，营造规范健康发展氛围。引导网络安全企业、保险机构等积极参与，构建多方协同、优势互补、融合发展的网络安全保险发展生态。

反电信网络诈骗：银行信用卡探索长效治理机制

本报记者 王柯瑾 北京报道

日前，公安部公布了十大高发电信网络诈骗类型及相关典型案例，包括刷单返利类、虚假网络投资理财类、虚假网络贷款类、冒充电商物流客服类以及冒充公检法类等，引发社会广泛关注。

当前，电信网络诈骗手段不断更新迭代，各种套路让人防不胜防。作为账户开立以及资金转移的关键环节，银行信用卡肩负着反电信网络诈骗的重要责任。

《中国经营报》记者了解到，在《中华人民共和国反电信网络诈骗法》（以下简称“《反电信网络诈骗法》”）和监管部门的指导下，多家银行信用卡中心加速落实内控机制，持续完善账户管理机制，构建信用卡反电信网络诈骗风控体系，探索金融反电信网络诈骗的长效治理机制。

完善内控 提升监测识别能力

无论是网上购物还是线下刷卡消费，银行信用卡都给生活带来了极大的便利。但同时，它也容易成为不法分子盗取的“猎物”以及电信网络诈骗的目标。

按照《反电信网络诈骗法》中的解释，电信网络诈骗是指以非法占有为目的，利用电信网络技术手段，通过远程、非接触等方式，诈骗公私财物的行为。

自2022年12月1日起，《反电信网络诈骗法》正式实施。该法规定，金融、电信、网信部门依照职责对银行业金融机构、非银行支付机构、电信业务经营者、互联网服务提供者落实本法规定情况进行监督检查，有关监督检查活动应当依法规范开展。

在《反电信网络诈骗法》和监管部门的指导下，多家银行进一步加筑反电信网络诈骗“安全网”。

据悉，中信银行信用卡以《反电信网络诈骗法》实施为契机，持续开展消费者权益保护知识的宣教活动，并积极运用大数据、人工智能等技术，建立健全异常账户和可疑交易监测机制，提高风险识别防范能力。

兴业银行信用卡中心表示，其以“监测—处置—宣教”三个核心维度为抓手，构建信用卡反电信网络诈骗风控体系。从严格落实反电信网络诈骗内控机制和持续完善账户管理机制两方面为入口，做到分工明确、职责清晰。

首先，兴业银行信用卡中心严格落实主体责任，明确各业务环节对于反电信网络诈骗工作的职责与具体处理要求，将反电信网络诈骗工作纳入申请、开户、交易等信用卡全生命周期管理中。同步建立以案倒查常态化工作机制，由点及面查补风险防控的薄弱环节与作业漏洞，从业务层面将各项反电信网络诈骗工作落到实处。

其次，兴业银行信用卡中心不断落实和完善《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》，调整信用卡新户开户数量限制，严格落实“断卡”行动相关要求，常态化开展存量账户的排查清理工作，对存在风险的账户及时采取管控措施，必要时移送公安机关。

此外，金融机构对信用卡业务管理中，身份识别以及尽职调查机制十分重要。

在兴业银行的实践过程中，在开户环节，严格审核客户身份文件的真实性、完整性和合规性，了解客户的办卡意愿、办卡用途；在卡片存续期间，加强身份证有效期识别，严格审核客户提交的身份证文件并留存相关记录。对于审核存在异常、身份证超出有效期等情况，采取相应风险管理措施，最大程度防范银行账户被用于电信网络诈骗活动。

对于银行而言，识别客户是否由于遭遇电信网络诈骗而出现信息泄露或遭遇卡不在场交易仍存难点。因此，在交易监控方面存在一定盲区。

为扫除监控盲区、捕捉隐秘诈骗交易，兴业银行信用卡中心表示，该行不断优化监控规则和涉诈模型，持续提升交易监测识别能力。一方面，持续优化交易监控规则。在信用卡交易监控过程中，密切关注电信网络诈骗批量事件，深入挖掘交易异常特征，并据此调整监控指标和参数配置，通过跟踪调整效果持续完善规则，尽可能减少后续客户因遭受电信诈骗而产生损失。

另一方面，持续动态优化涉诈模型。兴业银行信用卡中心依托该行企业级平台强大的运算能力与大数据支持的优势，结合行业成熟的专家规则模型和XG-Boost机器学习算法模型，通过对黑样本特征的提炼定义涉案特征标签，并将标签组合构建规则库。同时，通过对黑白样本的学习构建机器学习模型。借助规则库和机器学习模型两大利器，产出预警名单，并对预警名单内的账户进行调查、核验。据了解，该行依托涉诈模型高效监测识别，同一信用卡账户的涉诈资金金额下降超八成，风控效果提升显著。

多方协作 守护好个人“钱袋子”

电信网络诈骗犯罪名目繁多，涉及范围广、社会危害性大、公司化、专业化、职业化特征明显，甚至形成犯罪“产业链”。

建设银行官网信息显示，对于信用卡而言，常见的骗局包括：第一，积分兑现。不法分子冒充银行、电信运营商等官方号码发送含有钓鱼链接的虚假短信，谎称积分可兑换现金，一旦点击链接并在虚假网页输入卡号、有效期、安全码、动态验证码等重要信息后，不法分子就可冒用用户的身份盗用账户资金。第二，提升额度。不法分子冒充银行官方号码发送虚假短信，假借提升信用卡额度诱骗用户点击短信中的虚假链接，盗取卡号、有效期、安全码、动态验证码等重要信息后实施盗用。第三，网购退款。不法分子假冒网店客服，谎称物品缺货或存在质量问题可办理退款，借此引诱用户提供银行卡号、密码、动态验证码等信息，或让用户扫描二维码进入事先制作好的虚假页面窃取信息，从而实施诈骗。

当持卡人陷入电信网络诈骗陷阱从而遭受财产损失后，金融机构如何快速且有效地处置止损显得尤为重要。

兴业银行信用卡中心认为，打击治理电信网络诈骗是一场协同战、持久战。据介绍，该行信用卡中心与公安机关建立了高度协同、密切协作的合作关系。一方面，对于公安机关通过“电信网络新型违法犯罪交易风险事件管理平台”发出的查询、止付、冻结等指令，兴业银行信用卡中心依托7×24小时紧急联系人机制迅速响应，当下立即对涉案账户采取紧急止付、快速冻结等措施，确保账户“只进不出”，保证客户资金安全；另一方面，对于经公安机关认定的买卖冒名账户、涉案账户等风险名单，兴业银行信用卡中心积极开展倒查与处置，结合尽职调查与交易风险监测情况采取针对性、分等级的风险防控措施。

此外，为了应对电信网络诈骗的最新风险特征与作案手法，对症下药加强风险防控措施，兴业银行信用卡中心持续加强与同业的信息交流、共享与协作，以行业联动协作方式提高个体机构的反诈风控能力。

据悉，在中国银联的牵头推动下，兴业银行信用卡中心与银行同业协同合作，参与开发“跨行风险监测与账户核验平台”，建立跨行开户开卡核验机制。通过跨机构开户数量核验，清楚掌握客户名下同业信用卡数量，结合其兴业银行信用卡持卡情况，进一步完善账户管理。

此外，为减少信用卡持卡人资金财产等受到侵害的可能性，强化电信网络诈骗宣传教育和风险提示，提高民众反诈防骗意识尤为关键。

面对类型多样的电信诈骗手段，多家银行信用卡中心提醒消费者切勿向陌生人透露个人信息，提升金融安全知识储备，守好自己的“钱袋子”。

兴业银行信用卡中心从新型电信网络诈骗手法科普和加强银行卡管理风险警示两方面入手，通过多种渠道和形式向广大持卡人进行科普和宣传教育，强化金融安全与风险防范意识，保护个人财产安全。

民生银行信用卡亦提示消费者，时刻提高警惕，加强自我防范，不轻信来历不明的电话和短信；不透露自己及家人的身份信息、金融信息；不向陌生人汇款、转账等。

“持卡人首先保护好个人身份证、银行卡号、密码等相关信息；警惕利益诱骗，坚信天上不会掉馅饼；加强网上业务办理的安全性，警惕钓鱼网站和各类木马病毒；及时关注查看持有的银行卡的消费信息等。”光大银行金融市场部宏观研究员周茂华如是表示。

总体来看，在《反电信网络诈骗法》的指引下，商业银行信用卡正在通过多样化的风险防控手段，持续推动反网络电信诈骗系统建设精细化、智能化和一体化，维护用户用卡安全。