

# 网号、网证热点六问

## ——详解《国家网络身份认证公共服务管理办法(征求意见稿)》

近期,公安部、国家网信办等研究起草的《国家网络身份认证公共服务管理办法(征求意见稿)》,向社会公开征求意见,引发广泛关注。

网号、网证是什么?将对公众和数字经济发展产生怎样的影响?新华社记者梳理当前公众关心的热点问题,采访了有关权威专家。

### 问题一:网号、网证是什么?

根据征求意见稿起草说明,网号是由字母和数字组成,不含明文身份信息,网络身份符号;网证是承载网号及自然人非明文身份信息的网络身份认证凭证。

通俗地说,网号是用户在网络空间中的身份编码,同时隐去了个人信息;网证是一种简化版的数字证书,在网络社交、即时通讯等法定实名制领域以及其他需要验证身份的场景,作为一种可选择的身分认证方式。

公安部第一研究所研究员于锐介绍:“用户不是‘持证’才能‘上网’,而是在需要证明身份的场景中多了一种更加安全、方便的选择,不需要反复向各个平台提供明文的个人信息。同时,原有的身份认证方式仍可使用,没有网号、网证也可正常使用。”

### 问题二:国家网络身份认证公共服务相比现有认证方式有哪些优势?

根据有关规定,目前,用户使用

网络服务遵循“后台实名、前台自愿”原则,需向不同的互联网平台以明文方式重复提供个人真实身份信息。

国家信息中心研究员李新友表示,对于传统的身份认证方式,互联网平台从前端采集到后台存储链条较长、环节较多,并且网络传输环境较为复杂,个人信息安全保障有难度,泄露事件时有发生。

推行网号、网证,旨在减少互联网平台收集姓名、身份证件号码、人脸等个人信息,实现公民身份信息的“可用但不可见”。

电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者可使用国家网络身份认证公共服务,对涉诈等异常账号进行动态身份认证,最大限度减少“实名不实人”的情况,提高网络黑灰产违法犯罪的成本。

于锐表示,国家网络身份认证公共服务的工作原理,是基于国家人口基础信息库对用户身份进行远程比对核验,人口信息是国家本已掌握的信息。用户在申领、使用网号、网证的过程中,公共服务按照“最小必要”原则,仅采集与用户身份认证密切相关的信息,如通过NFC功能识读证件来验证证件真伪,通过人脸识别来验证用户本人操作,通过手机号来确认本人意愿和应急联络,通过手机参数来确认运行环境的安全性,除此之外,不采集其他个人信息。

在用户注销网号、网证时,相关个人信息将全部删除。而且,对上述个人信息,国家投入强大的技术力量

保证信息安全。

### 问题三:国家网络身份认证公共服务能给用户带来哪些便利?

李新友表示,与其他身份认证服务相比,国家网络身份认证公共服务具有很大的便利性,使用智能手机即可证明身份,方便人民群众在数字化、网络化、智能化条件下办理事项。

比如,网上购买门票时,通常需要输入姓名、身份证件号码等信息,比较繁琐,如果依托国家网络身份认证公共服务,经点击跳转即可完成认证。此外,国家网络身份认证公共服务还可跨应用、跨平台使用,有效减少记忆各种网站和互联网平台账户、口令的负担。

在一些需要出示身份证进入场馆的场景中,参观者可以使用国家网络身份认证App快速通行,在一定程度上减轻了携带实体身份证件的负担,也避免了一些个人信息泄露等安全风险。

### 问题四:如何保障个人基于自愿原则使用网号、网证?

征求意见稿规定,持有有效法定身份证件的自然人的,可自愿向公共服务平台申领网号、网证;鼓励有关主管部门、重点行业按照自愿原则推广应用网号、网证;鼓励互联网平台按照自愿原则接入公共服务。

于锐表示,特别是反电信网络诈

骗法等上位法规定,国家推进网络身份认证公共服务建设,支持个人、企业自愿使用。对存在涉诈异常的卡、号、电信业务经营者、互联网服务提供者等“可以”而不是“应当”通过网络身份认证公共服务对用户身份重新进行核验。这充分体现了用户自愿使用网号、网证的原则。国家网络身份认证公共服务管理办法作为下位的部门规章,不可能在该问题上突破上位法规定。

于锐介绍,用户接受或者退出国家网络身份认证服务,完全基于用户自愿。从App操作层面,国家网络身份认证App自愿下载、申领,并不会强制或强迫用户使用。从推广应用层面,互联网企业、接入单位也是自愿使用,可将公共服务作为可选项而非唯一项,保留现有其他方式。

### 问题五:国家网络身份认证公共服务有何法律依据?

于锐介绍,国家网络身份认证公共服务在网络安全法、个人信息保护法、反电信网络诈骗法等法律中均有相关规定和依据。

网络安全法第二十四条提出“国家实施网络可信身份战略”,明确了网络可信身份的概念。

个人信息保护法第六十二条规定“支持研究开发和推广应用安全、方便的电子身份认证技术,推进网络身份认证公共服务建设”,明确在国家层面建设网络身份认证公共服务。

反电信网络诈骗法第三十三条规定,“国家推进网络身份认证公共服务建设,支持个人、企业自愿使用,电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供

者对存在涉诈异常的电话卡、银行账户、支付账户、互联网账号,可以通过国家网络身份认证公共服务对用户身份重新进行核验”,明确了国家网络身份认证公共服务在打击电信网络诈骗中的地位。

根据上述法律,公安部、国家网信办会同有关部门组织建设了国家网络身份认证公共服务平台,并在相关领域开展了试点应用。同时,为了规范公共服务的运行管理,进一步保护用户的个人信息权益,研究制定部门规章——国家网络身份认证公共服务管理办法。

### 问题六:国家网络身份认证公共服务将对数字经济产生怎样的影响?

数据要素是发展数字经济的关键和核心,激活数据要素,实现数据要素流动的前提是明确数据权属,其基础便是个人身份的确权。李新友表示,基于国家网络身份认证公共服务,个人可实现对数据的有效确权 and 授权,进而形成并固化自身数据资产,以此促进数据要素的有序流动和增值,助力数字经济发展。

数字经济时代,信任是基石。李新友认为,国家网络身份认证公共服务为网络交易、在线服务等提供了更加可靠的身份验证手段,减少了因身份冒用带来的经济损失,通过提高网络诚信水平改善营商环境。同时,由国家提供身份认证服务,为企业降本增效,促使其把更多精力投入到提高产品质量、提升用户体验感中,推动互联网产业和数字经济持续健康发展。

李新友表示,将构建可信数字身份体系作为发展数字经济的重要措施,这是当前世界各国的通行做法。欧盟的eID、新加坡的SingPass、印度的Aadhaar已形成具有自身特色的可信数字身份体系,其经验做法值得我们学习借鉴。

(据新华社)

## 网络安全为人民 网络安全靠人民

“即申即放”“无需担保”,通过租借手机、回收购物卡、回收黄金提货券即可获得贷款……这些往往都是高利贷的陷阱。

近期,上海警方调查发现,部分网络平台以物品租借和回收为名放高利贷,收“砍头息”,部分借款者借贷年化利息最高可达400%。

### “商品回收”成高利贷“新马甲”

记者采访发现,一些非法放贷平台改变过去“放贷—收债”的套路,将放贷行为包裹在回收实物或虚拟产品的外衣里,通过将环节拆分,增加犯罪隐蔽性。

——“手机租借型”。上海市民姜女士与某借款平台约定,她以“租借”一部价值9000元的手机为名进行借款。平台实际上并未把手机寄给姜女士,而是将手机寄给回收商进行倒卖后,再把手机款打给她。不过,扣除首期“租金”和“中介费”等,姜女士实际上只拿到6300元。此后,姜女士要分12期在3个月内返还平台18000元。

在犯罪嫌疑人的引导下,姜女士以这种方式在多个App共获得资金14万余元,但3个月就需偿还42万余元。

姜女士报案后,警方展开侦查,先后抓获袖商南城、优租、壹点商城等5个非法放贷平台的实控人11人。经初步核查,这些平台已累计向不特定人群非法放贷2000余万元,涉案人数达数千。

——“黄金提货型”。来自河北的周先生表示,他在一个名为“小兔花”的App上借贷,收到的不是现金,而是平台给予的购买黄金提货券的授信额度。

“黄金提货券并不能直接兑换黄金。平台要求对黄金提货券回收后,才能放款。我使用4.3万元的额度买了57克黄金提货券,意味着跟平台借了4.3万元。黄金提货券被回收后,平台要扣除各种手续费,实际到手只有2.9万元。”他说。

部分借款者表示,有的平台提供专门用于购买黄金的借款额度,但只能在该平台购买,而该平台上的黄金价格比市场价高出近200元/克。借款者在收到黄金后以市价套现,相当于被平台收了很高的“砍头息”。

### ——“购物卡回收型”。来自浙江的赵先生告诉记者,他在某金融平台上借款2400元,借款周期是一个月。平台实际向其发放1900元面值的购物卡,外加在线视频和音乐会会员权益;平台承诺可对1900元购物卡进行现金回收,但需扣除折现费208元。

“借2400元,实际到手只有1692元。此外,我还要额外支付130元利息。”他说。

上海市公安局静安分局经侦支队金融犯罪侦查队长张晨晖表示,嫌疑人之所以将放贷环节复杂化,目的是通过复杂的实物或虚拟物品流转,让非法放贷看上去更像是正常交易,躲避警方侦查。

### 变换名目“软暴力”催收

今年以来,上海公安机关已侦破非法放贷案件30余起,抓获犯罪嫌疑人110余名。办案人员表示,当前相关非法放贷案件呈现出多个新特点。

一是不断变换“中介物”作为障眼法。有的不法分子以会员“权益卡”“代金卡”等不具备流通性的虚拟物品充抵部分贷款本金,增加借款人融资成本,变相发放高利贷。有的不法分子非法开发所谓“融资租赁”或者电商平台App,以手机和电脑等电子产品融资租赁、充值卡等有价实物买卖为幌子,通过“租机变现”“实物回收”等方式变相发放高利贷款。

二是不断变换“砍头息”的名目。与以往直接从本金中预先扣除利息的“砍头息”不同,部分不法分子会以担保费、服务费、手续费为名变相收取“砍头息”。

在警方侦破的案件中,有的不法分子以“即申即放”“无需担保”“不查征信”等噱头诱导借款人下载App,通过事先设置的隐藏条款,使借款人在App中输入身份证

及银行卡信息后,自动收到一笔小额贷款且不能提前还款。这笔贷款会被不法分子以担保费、服务费、手续费等名义变相收取“砍头息”,导致实际放款金额远远小于App上显示的贷款金额。

三是不断拓展招揽客源的渠道。不法分子利用互联网平台的



隐蔽性和快捷性,通过网络论坛、社交群组、App平台及各类自媒体等线上平台招揽客源,获取的客源更多,辐射的地区更广。

“类似‘手机租借’放贷App,往往并不在应用商店上架,属于没有备案的非法应用。有的不法分子会通过App非法获取借贷人的通信录。如借款人到期后无法按约定金额偿还,不法分子便会通过短信、电话‘轰炸’持续骚扰借款人及其亲友,以‘软暴力’迫使借款人偿还高额利息。”上海市公安局经济犯罪侦查总队一支队队长程阳旭说。

程阳旭表示,不法分子以“实物租借和回收”巧立名目实施高利放贷的行为涉嫌非法经营罪,还可能催生寻衅滋事罪、侵犯公民个人信息罪等犯罪行为。此外,此类不法分子往往与其他黑灰产相勾结,为洗钱、非法集资、金融诈骗等其他违法犯罪活动提供便利。

## 手机、黄金、购物卡都可成“马甲” 小心“蒙面”高利贷!

“即申即放”  
“无需担保”

某非法放贷平台

高利贷

### 加强精准打击治理力度

业内人士认为,针对当前非法放贷出现的新变体,可通过“大数据+AI”进一步加强对违法放贷App的监测、预警、处置,同时加强跨部门协作,提高执法效率,对蒙面“高利贷”精准打击治理。

北京理工大学网络安全研究所所长闫怀志表示,从技术治理的角度来看,可以加强代码审查与监控,比如开发专门的技术工具,对一定范围内的App代码进行深度扫描,识别出潜在的违法功能和行为模式。

“手机操作系统提供方和应用商店可利用大数据分析和AI辅助识

别,加强对App的运行和用户反馈检测,识别出异常交易模式或高风险行为,快速识别出违法放贷等应用,从而阻止恶意App的安装和运行。”闫怀志说。

上海市公安局经侦总队相关负责人表示,警方已依托“专业+机制+大数据”新型警务模式,联合相关金融监管部门严厉打击、严密防范非法高利放贷等各类信贷领域违法犯罪,按照“个案到类案、类案到行业、行业到生态”的工作链路,紧盯高发突发领域,全面汇集数据资源,深挖上下游进行全链条打击。

上海警方提醒,市民群众要增强防范意识,如有资金需求,要通过正规渠道,向银行、消费金融公司等持牌机构申请贷款,切勿从非正规渠道进行高息借贷,以免造成经济损失、信息泄露等。

(据新华社)