# 注册时，用新手机号直接进入了陌生人账号

## “二次放号”给新旧号码主带来的那些困扰

□ 本报记者 韩丹东

“刚换的手机号，我在注册网盘账号时，直接进入了陌生人的账号，里面有别人的家庭照片、工作文档，甚至还有合同扫描件。”北京市民李先生向记者吐槽说。

李先生的遭遇，是电信运营商“二次放号”背后诸多隐患的一个缩影。

“二次放号”是用户注销或停用手机号，运营商在经过一段“冷冻期”后，将该号码重新投放电信市场，供新用户办理。与此同时，随着手机号成为各类平台的主要注册与登录凭证，由此带来一些不便：号码新主人被前主人绑定的各类业务骚扰，前主人的个人信息因未及时解绑而面临泄露风险等。

### 新办号码收到催收信息

北京市民王女士最近经历了一次“烦恼连环套”，起因则是一个手机号码。

2025年8月，王女士新办理了一个手机号码，使用一段时间后，突然有一天收到某网贷平台的一条催收短信“某某（手机号前主人姓名——记者注），你的贷款已逾期3个月，欠款金额5000元，请及时还款，否则将影响征信”。

她起初以为是一条诈骗短信，未予理会。但随后催收电话接踵而至，甚至有催收人员发送“威胁性言论”短信，声称要“上门催收”。

意识到问题严重的王女士马上联系网贷平台客服，才知道手机号前主人确实在该网贷平台贷款，绑定的正是这个手机号码。

王女士多次联系网贷平台客服，提供了自己的身份证、手机号办理凭证等材料，耗时二十多天平台才确认该手机号已易主并停止了催收。

“我那段时间天天焦虑，担心这件事影响自己的征信，还得跟家人、朋友解释，太折腾了。”王女士无奈地说。

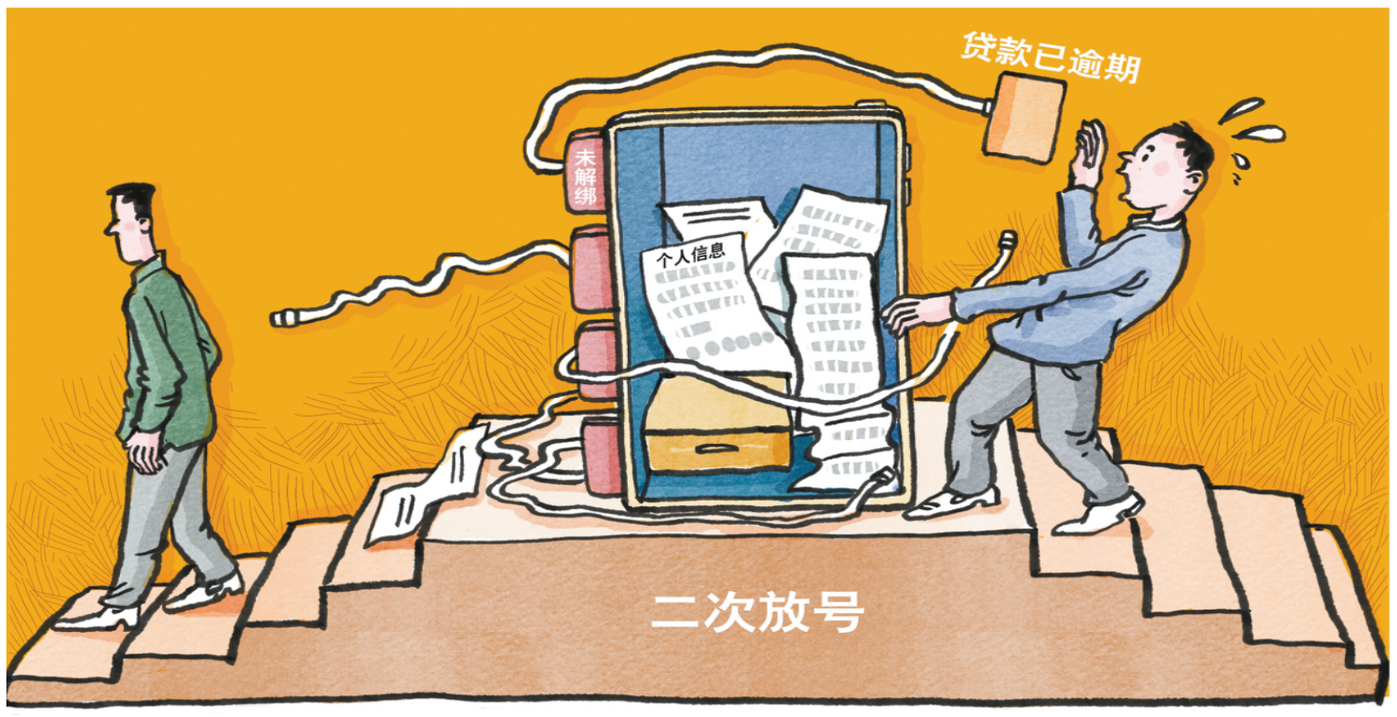
与王女士的烦恼不同，手机号前主人则面临个人信息泄露的风险。

2022年，天津市民赵先生因工作调动，注销了使用多年的手机号码。2023年春节期间，他突然收到前同事的消息，对方称：“你的网盘账号怎么在发陌生信息？”赵先生这才意识到，自己的网盘账号绑定着此前使用的手机号码。

“我登录网盘发现，里面的工作文档、客户资料都被人看过。”赵先生说。他立即联系网盘客服申请冻结账号，但客服表示，他不是网盘绑定手机号的主人，无法通过验证码验证身份，只能通过提供大量的历史使用记录、身份信息等材料进行验证，并且需要经过多轮审核才能冻结。

“经历半个多月才解决问题，在这期间不知道有多少个人信息被泄露了，想想都后怕。”赵先生感慨地说。

在进一步采访中，记者随机走进某运营商北京一家线下营业厅，告诉工作人员打算“办理一个新手机号”。工作人员向记者推荐了多款“尾号吉祥”号码，记者随机选择了一个尾号为“99”的手机号码，办理了基础套餐。




随后，记者登录某网盘页面，在相应窗口输入手机号并获取验证码后，点击“登录/注册”，页面直接跳转至一个已登录账号，并未出现“新用户注册”选项。该账号内存储大量个人资料，包括家庭合影等。该账号的昵称是“张先生”，个人资料页显示绑定的手机号码正是记者刚办理的这个，绑定时间为3年前。

之后，记者联系该网盘客服，申请注销该账号或解除手机号绑定。客服表示，由于账号内有大量数据，且无法核实记者是否为该账号的前主人，只能通过“账号申诉”流程处理，且需要提供前主人的身份信息。记者刚拿到这个手机号码，无法提供相应信息，此事只能作罢。

记者还发现，这个手机号码在多个平台注册过相关账号，因此无法注册新账号。

此外，记者在使用这个手机号期间，还持续收到各类骚扰信息，包括房产中介的推销电话、培训机构的广告短信、号码前主人的亲友来电等，每天至少接到几通电话都与前主人有关。

### 用户忽视解绑所有平台

就遇到的这些问题，记者分别联系三大运营商的客服进行咨询。

三大运营商客服解释说，用户主动注销手机号后，该号码并不会被立即重新投放市场，而是会经历一段“冷冻期”。

关于手机号码“冷冻期”的时长，三大运营商客服的表述基本一致，最长90天后会重新投放市场，具体时长会根据地域差异而有所调整。

有客服表示：“用户注销手机号后，号码会进入‘冷冻期’，一般情况下是60天，最长不超过90天。‘冷冻期’结束后，号码会被系统自动释放，重新进入‘号码池’，供新用户办理。”

该客服还说，如果号码进入双停（手机无法接听和拨打电话）状态，相当于停机，则60天后进入“冷冻期”，再过90天后进入市场售卖。

“在‘冷冻期’内，号码主人可以申请恢复使用，若无人申请恢复使用，号码将被重新售卖。如果用户在‘冷冻期’内申请恢复使用，可以携带身份证前往线下营业厅办理，需要交纳一定的手续费。”该客服说。

一个随之而来的问题是，记者新办理的手机号被前主人注册了网盘账号，想注销但又不能注销，该怎么办？

对此，客服表示：“我们可以协助您解除该手机号在我们自有平台的绑定，但对于第三方平台的绑定，我们没有权限处理，需要您联系对应的平台客服解决。”

记者了解到，三大运营商均推出了“号码注销前解绑指引”服务，用户在注销手机号时，工作人员会提醒用户及时解绑第三方平台的绑定，并提供一份常见平台的解绑流程指引。但记者在采访中发现，不少用户在注销手机号时，并未意识到需要解绑所有平台，或者因绑定平台过多而有遗漏。

“注销手机号码时，客服确实提醒要解绑第三方平台，但我以为只用解绑少数几个常用的平台，忘了解绑不常用的平台。”赵先生说。

此外，对于号码前主人而言，一旦手机号被注销，再想解绑第三方平台就变得异常困难。“手机号码注销后，很多平台的解绑需要接收验证码，没有验证码无法完成解绑，或者按照客服要求提供各种证明材料，流程复杂，耗时耗力。”赵先生无奈地说。

### 扩展一键查询解绑服务

根据公开信息，为解决用户手机号码注销后解绑相应平台问题，中国信息通信研究院推出了便捷的“手机号注册账户一键查询解绑服务”，但由于一些小众平台尚未接入，此项服务仍存在“遗漏地带”，用户需自行联系处理。

工业和信息化部还组织中国信息通信研究院、电信运营商等打造技术服务平台，建立跨行业协同机制，用户可以通过电信运营商官方焕新服务，快速解绑手机号码开户前绑定的应用。

面对“二次放号”带来的解绑问题，号码现主人、前主人通常不了解该如何解决，运营商是否应该对此负有责任？

据了解，当用户遇到问题时，运营商往往以“无法介入第三方平台”为由拒绝承担责任，相关平台则以“用户未及时解绑手机号”为由推诿。

记者联系某平台客服，反映手机号码前主人信息泄露问题时，客服表示：“我们的账号注册与登录均通过手机号验证，用户注销手机号后，应当及时主动解绑账号，若未解绑，导致信息泄露，责任在于用户自身，与平台无关。”

而运营商则表示：“我们已在用户注销手机号时提醒过解绑第三方平台，尽到了提醒义务，后续出现的问题与我们无关。”

“我办理的号码不能注册某平台，因为显示号码已注册。我向12315投诉过某平台，对方表示需要提供号码前主人的身份信息才能处理，我不可能做到；之后又投诉运营商，运营商则称已尽到提醒义务，无法进一步解决。”王女士的经历，折射出当前“二次放号”机制下用户维权的现实困境。

漫画/高岳

用户遭遇“二次放号”个人信息保护问题 专家建议

# 修订电信条例明确运营商及平台责任

□ 本报记者 韩丹东

在移动通信服务普及的当下，手机号已不仅是通信工具，更是个人身份核验、账号注册、金融交易的核心载体，而“二次放号”这一行业常规操作，正逐渐成为个人信息保护与用户权益维护的风险洼地。记者在采访中发现，号码前主人未解绑账号导致的信息泄露，号码现主人遭遇前任债务催收与业务扣费、跨平台解绑无门等一系列问题接踵而至。

围绕“二次放号”行为的法律责任边界，记者采访了华东政法大学教授高富平、北京大成律师事务所高级合伙人邓志松、北京市盈科律师事务所高级合伙人邱跃。

### 明确相关主体法律责任

“二次放号”从技术层面看是号码资源的循环利用，但其衍生的风险却涉及个人信息安全、财产权益安全等多个领域。

在邓志松看来，“二次放号”带来的问题呈现双向性。对号码前主人而言，若未及时解绑账号，极易出现信息泄露、账号被现主人登录的情况；对现主人来说，更易遭遇前任用户关联的债务催收、莫名业务扣费，甚至可能因前主人的不良记录影响自身名誉。

对此，高富平认为，问题根源在于规则层面的缺失。“二次放号”的核心矛盾是号码流转后，号码前主人与现主人的账号绑定关系未被有效切割，进而引发一系列问题，但目前却没有相关规则予以规范。

受访专家认为，面对“二次放号”引发的各类纠纷，明确号码前主人、运营商等相关主体的法律责任，是化解矛盾的关键前提。

在号码前主人的责任认定上，受访专家均认可其需承担相应的审慎管理义务，但责任范围与程度存在细化区分。

高富平认为，手机号在注销或停用之前，号码前主人应当负有对注册账号及时解绑、注销的注意义务，从法律角度出发，这种注意义务是前主人的自力救济，也是前主人基于自身信息管理的基础责任。

在邓志松看来，根据民法典规定，要求个人信息处理活动遵循合法、正当、必要原则，并采取相应安全措施。一般而言，前主人对自身账号和高风险绑定关系负有合理注意义务，若其明显疏忽导致信息泄露，在与平台、运营商的纠纷中，平台、运营商通常因其过错而被减轻责任。

邱跃认为，前主人未解绑账号导致信息泄露还可能承担相应侵权责任，如对被泄露信息的联系人赔礼道歉、赔偿损失等，前主人责任边界应限定在其可预见、可操作、可避免的范围内，手机号二次投放造成信息泄露时，前主人是次要责任，平台和运营商是主要责任；如果信息泄露和手机号无关，是新主人的恶意行为造成，或是平台安全漏洞造成，前主人可减轻或免除责任。

### 运营商应尽到提醒义务

运营商作为号码流转的核心主体，其义务与责任的界定是“二次放号”纠纷中的焦点问题。

高富平认为，运营商应当尽到提醒义务，即告知新主人，该号码为二次投放号码，请其注意该号码关联第三方平台账号等，不仅如此，从提升服务质量和信息安全的角度，运营商也应当增加注意义务。同时，运营商的业务范围属于自我管理范畴，无需加强其在用户注册账户方面的管理。

邱跃认为：“虽然运营商无权强制解绑第三方账号，但这并不能免除其在风险防控中的提示义务，因为运营商没有向新老用户提示风险，所以需要为其未尽到提示义务的过错承担补充责任，即在直接侵权人无法赔偿时，运营商在其过错范围内承担相应责任。”

平台作为账号服务的提供方，其安全机制与解绑流程的合理性，也直接影响“二次放号”风险的防控效果。

在高富平看来，平台应加强验证手段，如动态验证、IP地址检测等，避免单一验证手段，以避免“二次放号”产生的后续影响。

邓志松分析认为，“平台的安全机制是否达到‘必要安全措施’要求，需要基于与所涉及的个人信息对个人的人身、财产安全的影响进行综合判断，单纯依赖‘手机号+短信验证码’的登录方式本身并不违法，但对涉及大量个人信息或财产安全的场景，如果仅采用单一验证手段，发生信息泄露时容易被认定为安全措施与风险不匹配。”

他认为，实践中，金融及支付类平台通常在短信之外叠加密码、身份证信息、人脸识别等多途径验证，以防止“二次放号”情况下轻易登录号码前主人账户，是一种非常好的措施。但对于一些普通平台，无论是从消费者使用习惯还是从必要性来看，在无异常发生的情况下，如在“手机号+验证码”基础上增加多种方式认证才能解绑手机号，一方面可能被认为平台变相阻碍用户行使“撤回同意”的权利；另一方面，也会给服务提供商增加过多的安全保障义务。

邱跃的观点是，多数平台仅支持“手机号+验证码”登录违反了“必要安全措施”的要求，平台处理个人信息时，应采取措施保障个人信息的安全，“必要安全措施”不仅包括加密传输、防火墙等技术，也包括身份验证机制的合理设计。

### 在法律法规中予以规范

针对“二次放号”引发的种种问题，受访专家均认可需要完善现有相关规定，细化各方主体义务。

高富平建议，将来在修订电信条例时可以明确运营商的注意义务。

邓志松提出，目前，民法典、个人信息保护法、消费者权益保护法、电信条例等法律法规均对个人信息保护与电信服务作出一般性规定，但并未专门规范手机号码“二次放号”，也缺乏针对号码回收“冷冻期”、历史绑定统一查询与解绑机制、账号休眠制度以及责任分配的具体规则。

“因此，从风险管理和成本可预期性考虑出发，有必要将‘二次放号’纳入法律法规中予以规范，细化运营商在销号、过户、‘二次放号’前后的告知、清理义务，明确平台接入统一解绑接口、提供多元验证方式和账号休眠机制等义务，同时对运营商、平台、号码用户之间的责任分担予以清晰划分。”邓志松说。

邱跃同样认为：“需要在现行立法中以专门条款明确运营商、平台的强制性义务，比如运营商在号码回收前，向原用户发出两次以上有效提醒；新号码启用前，应向新用户提供绑定平台清单；大型平台必须接入国家平台并支持一键解绑；建立账号休眠和自动清理机制等。”

在他看来，还需要强调在将来修订个人信息保护法时明确各方义务，比如明确“二次放号”信息解绑的各方义务。

在平台技术验证层面，受访专家均主张丰富验证方式，实现安全与体验的平衡。

高富平认为，平台应加强验证手段，如动态验证、IP地址检测等。

邓志松则给出了验证方案建议，在云盘、社交账号、支付、网银等高风险场景，可以实施登录密码或历史密码校验、身份证号和姓名等静态信息比对、人脸或指纹等生物识别、对常用地址或收货信息的行为特征核验等。还需要有“分级验证+风险感知”的平衡思路，对日常、低价值操作维持相对简洁的登录流程；可以考虑只有在检测到疑似“二次放号”、频繁更换设备、跨地区登录或修改关键信息时，才触发更严格的多途径认证。

在维权层面，邓志松认为，针对“二次放号”导致信息泄露的维权问题，明确责任主体是有效行动的前提。受害者通常可能向三类主体主张权利，即直接盗用信息的行为人、相关平台服务提供者、电信运营商。

在他看来，向盗用信息的主体追责，需证明该主体确系信息使用者，其行为构成“盗用”、造成了实际损害；向平台服务提供者追责，核心在于证明平台安全机制存在缺陷或应对不力，需准备的证据包括账号归属证明、异常情况证据、损害结果证明，此外，若能证明其已就账号异常通知平台，而平台未及时采取冻结、阻断等有效措施，导致损失发生或扩大，将强化对平台过错的认定；向电信运营商追责，重点在于证明运营商未履行法定的提示与管理义务，关键证据包括能证明“二次放号”事实及运营商知情的材料、证明其未清晰告知风险的证据、证明违规销售号码等行为的相应证据。

用户自身的操作规范也至关重要。

邓志松提示说，准备注销手机号的用户，宜先通过“一证通查”核对名下电话卡和关联账号数量，再对云盘、支付、网银等重点平台逐一更换预留手机号或注销账号，并关闭依赖原号码找回密码等功能后，再向运营商申请销号；新办理“二次放号”的用户，则可在开卡后尽快使用“二次号码焕新”服务，对号码前主人绑定的主流应用进行排查和解绑，遇到陌生验证码或异常订单时及时联系平台核查。

北京朝阳检察院发布白皮书指出金融犯罪呈现组织化专业化特征

# 有涉案公司专门设立法务部规避风险

□ 本报记者 张雪泓

3年时间内，在未经国家主管部门批准的情况下，王某等10人自建“第四方支付”平台从事实时在线支付结算业务，为境外赌博网站等非法支付结算金额2900余万元。王某等人通过控制大量银行账户在短时间内快速流转资金，在国家金融监管体系之外形成“体外循环”，成为违法犯罪资金的输送通道，严重扰乱了金融管理秩序。

近日，北京市朝阳区人民检察院发布《金融检察白皮书（第九辑）》（以下简称白皮书），其中披露了这起入选北京市检察机关助力防范化解金融风险典型案例的案件。检察机关依法提起公诉后，法院以非法经营罪判处王某等10名被告人有期徒刑5年至1年6个月不等，并处相应罚金。

白皮书显示，近两年，朝阳区检察院共受理各类金融犯罪案件1107件3002人，其中非法集资类犯罪案件达991件2591人（包括非法吸收公众存款罪和集资诈骗罪），但总体发案趋势有所缓解。非法经营罪（金融业务）呈现增长态势，主要涉及非法经营证券、非法放贷、非法买卖外汇等领域。

据介绍，金融业是朝阳区的重要产业，截至目前，全区汇集超过1800家金融机构，其中外资（合资）金融机构达400家，数量占全市的三分之二以上。基于金融风险点多面广的特点，朝阳区检察院整合优势资源，从严打击金融犯罪。

朝阳区检察院副检察长胡静介绍说，金融犯罪手段伴随着技术发展不断“升级换代”，不法分子借助新概念、新技术或者利用合法交易外观掩盖非法实质，犯罪隐蔽性更强，防范和打击难度加大。如信用卡诈骗罪，传统“恶意透支”型犯罪基本消失，取而代之的是“隔空盗刷”。此外，金融犯罪组织化专业化程度高，犯罪链条更长。以非法集资案件为例，该类犯罪一般以公司形式开展运作，公司层级分明，部门齐备，为激励员工设有KPI考核等绩效机制。部分涉案公司还专门设有法务部以规避法律风险。公司一旦爆雷，涉案人员众多，导致案件办理周期长，司法成本投入巨大。

胡静介绍说，不法分子为逃避侦查，实现非法资金合法化，洗钱手段日趋多样化，呈现“线上+线下”并行、传统手段与非传统手段交织的特征，导致资金流向更加复杂，追赃挽损难度进一步提升。非法集资与网络传销、信用卡诈骗与电信网络诈骗、贷款领域犯罪与相关职务犯罪等相互交织，导致风险叠加扩散。

白皮书显示，面对复杂态势，朝阳区检察院坚持依法严惩与源头治理并重，全面审查涉案资金流水与电子数据，全链条打击洗钱等下游犯罪，办理洗钱案件20件95人，追赃挽损总额超过10亿元。通过研发非法金融活动“烽火台”大数据监测预警平台，实现对辖区金融风险进行动态监测。平台启用以来，已累计研判风险企业8批62家，推动刑事立案5件，118名犯罪嫌疑人到案，助力追赃挽损超10亿余元，推动金融治理模式从事后打击向事前预警转变。

据了解，为破解海量数据审查难题，朝阳区检察院参与建设“北京市资金电子数据分析技术检察应用联合实验室朝阳工作室”，形成“办案人员+检察技术人员+研发团队专家”的协同模式。工作室成立以来，累计分析案件103起，处理交易流水2000余万笔、总金额达7000余亿元，在办理非法支付结算、新型盗刷信用卡等复杂案件中精准查明资金流向方面，发挥了关键作用。