

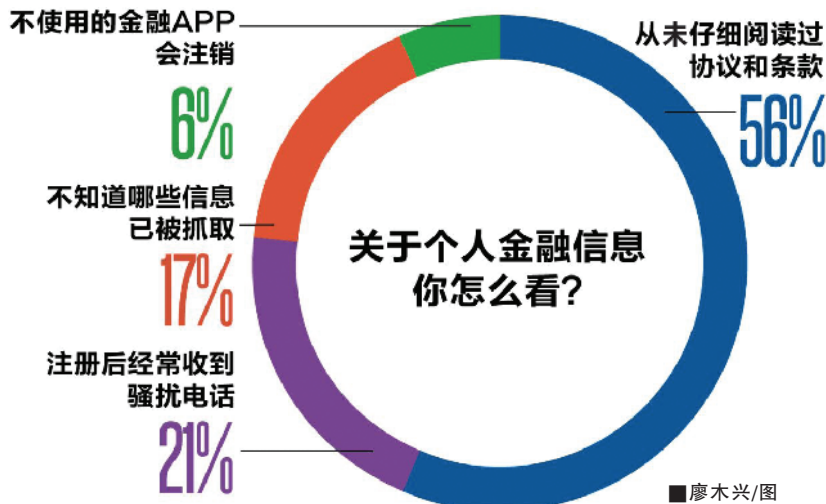
## 财经

# 个人金融信息迎来最严监管 别再让金融 APP 把你“卖”了

新快报记者调查发现:过半数网友从未仔细阅读过协议和条款

大数据高速发展的背后,不断暴露的数据隐私安全问题再次成为焦点。近期,金融标准化委员会下发了《个人金融信息保护技术规范》(下称《规范》)不仅对个人金融信息从敏感度进行了分类,还对个人金融信息在收集、传输、存储、使用、删除、销毁等各环节的安全防护提出要求。新快报记者在调查多家金融 APP 后发现,各家 APP 的隐私条款字数少则十几页多则几十页,大多数用户都是匆匆翻过然后勾选“同意”,根本不知道里面到底有没有“坑”。而记者的一项网络调查显示,超过半数的网友在注册金融 APP 前“从未仔细阅读过隐私条款”。

■新快报记者 许莉芸



## 你的个人金融信息到底有哪些？

去年以来,监管多次打击金融 APP 搜集用户个人金融信息乱象。这背后,根本原因在于用户与企业之间存在严重信息不对称的现象。新快报记者近日发起的一项关于个人金融信息的网络调查中,有超过 2 成的网友表示,注册金融 APP 后经常收到骚扰电话;近两成网友表示,不知道哪些信息会被抓取,抓取后又怎么被应用?是否被授权给第三方?这些信息他们基本没有任何认知。

“直接点击同意,没注意过协议条款。”有用户对新快报记者表示。然而,每次下载金融 APP 后,《用户协议》和《隐私条款》中都规定了大量的关于个人信息使用的规范和原则,如果用户不仔细阅读很有可能自己的个人信息被“卖”了。

对于很多用户而言,“蒙查查”的是他们连个人金融信息是啥都没搞清楚。

《规范》中,对个人金融信息进行了细致的分类,按照敏感程度从高到低,分别分为 C3、C2、C1。其中 C3 类别信息主要为“用户鉴别信息”,就是如何证明“你是你”?包括银行卡数据、卡片验证码、银行卡密码、账户登录密码、账户交易密码,还有指纹等鉴别用户的生物识别信息等。这类信息一旦遭到未授权查看,对个人财产安全危害最为严重;C2 类别信息则是识别用户身份和金融状况的个人信息,如支付账号、证件信息、手机号码、家庭信息、个人财产信息,还有用户鉴别辅助信息如动态口令、短信验证码等;而 C1 类别信息主要为机构内部使用的个人信息,与上述两种相比,这类个人信息敏感度较低,如账户开立时间、开户机构等。

“个人金融信息分级,利于行业对于用户关键敏感信息的使用、处理,也

给消费者隐私安全提供了证据。”有业内人士表示。不过,新快报记者在调查中发现,大多数金融 APP 均未对个人金融信息分类,少数 APP 也则只是简单粗暴地将个人金融信息分为“一般个人信息”和“敏感个人信息”。

“应该在具体场景中评估个人金融信息在其中的作用、可能遭受未经授权查看或未经授权的变更后所产生的影响和危害。”观韬中茂(上海)律师事务所合伙人吴丹君表示,比如在《规范》中表示,通过数据挖掘等技术可能在组合、关联和分析数个低敏感程度数据后产生具有高敏感程度的信息,因此,应对汇聚融合后的个人金融信息进行重新识别以确定类别。所以,个人金融信息要看具体使用场景,也存在大数据分析后低敏感度信息转化成高敏感度信息的可能性。

备信息也不影响正常的信贷业务。

此外,新快报记者发现大型集团公司旗下各子公司中个人信息共享是常态。如小米金融 APP《隐私协议》披露将与集团共享信息,“我们可能会向小米生态系统公司披露您的个人信息……小米生态系统公司可能不时与小米金融共享我们产品相关数据。”而根据近期国家标准化委员会下发的《信息安全技术个人信息安全规范》中规定,“不应通过捆绑产品或服务各项业务功能的方式,要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求。”有业内人士对新快报记者表示,“这意味着通过一个 APP,集团公司一次性拿到用户信息授权,能够应用到集团许多家子公司。”

权将共享的个人信息用于其他用途。”

从大数据行业来看,此规定也意味着此前行业中常见的各家金融机构与助贷、大数据公司合作抓取用户身份信息等数据的模式,并不合规。这将是大数据行业的又一重大打击。

“金融机构未来将加强第三方合作机构的资质审查,避免与非持牌机构开展涉及个人金融信息的业务合作,如征信、催收等。”业内人士对新快报记者分析表示。

链接

## 守护你的 个人金融信息安全

### 1 防止信息被过度收集,关闭非必要权限

一般而言,金融 APP 都是向用户申请开启权限来收集相应的个人信息。如“相机”权限用于拍照录像、人脸识别等;“位置”权限可以获取精准地理位置、基于位置的智能推荐等。在 APP 申请打开权限时,可根据其对目的的介绍或相关业务功能特点,简要分析和判断该权限是否与具体功能有关联。如果并没有关联则可以选择不打开该权限,如果 APP 强制要求用户提供无关权限,则需要考虑是否继续使用该 APP,防止个人信息被过度收集。

### 2 不使用金融 APP 时及时注销

根据新快报记者的网络调查,只有一成不到网友在不使用金融 APP 后会及时注销。由于很多用户在不使用金融 APP 后没有及时注销账户,个人数据也一直“躺”在账户中。一般而言,金融 APP 的“设置”功能中都有账户注销功能,点击注销的同时也要注意需要点击删除账户数据,才能确保个人金融信息被及时删除。

### 3 不要随意丢弃个人金融信息

广发信用卡相关人士提醒,用户应该注意不轻易泄露个人信息,不随意在网上晒照、发送地理位置;不要随意丢弃刷卡签购单、取款凭条、信用卡对账单等,如果一旦写错、作废的金融业务单据,应撕碎或用碎纸机及时销毁,不可随意丢弃,以防不法分子捡拾后查看、抄录、破译个人金融信息。此外,在提供个人身份证件复印件办理各类业务时,应在复印件上注明使用用途,如“仅供申报××信用卡用”,以防身份证复印件被移作他用。

## 遵循“最少且必要”原则

在注册各类金融 APP 之前,用户都需要同意《用户协议》和《隐私条款》,只要勾选“同意”则意味着条款中关于个人信息抓取、使用等各项规则。“2019 年是个人金融信息监管元年,今年可以说是合规元年。”有业内人士对新快报记者说。

实际上,去年因为 APP 超范围收集信息被监管点名的金融机构和互联网金融公司不在少数。去年底,央行向部分金融机构下发《关于发布金融行业标准加强移动金融客户端应用安全管理通知》中就规定,“在收集、使用个人金融信息时不得以默认、捆绑、停止安装使用等手段变相强迫用户授权,不得收集与其提供金融服务无关的个人金融信息。”

此前,北京市盈科(广州)律师事务

所律师徐进伟就曾对新快报记者表示,个人信息共享应遵从最少和必要的原则,否则一律不得采集和查询。《规范》中也提及,对于个人信息收集要采取“最少够用”原则。工行广东分行相关负责人也对新快报记者表示,应该按照“事先取得客户书面授权”“知所必需最小授权”原则,依法合规收集、保存、使用客户个人信息。“最大程度减少个人信息在 APP 中停留的时间,降低个人信息泄露的风险。”业内人士表示。

同时还要求收集个人信息类型应该与产品或服务的业务功能有直接关联。如拉卡拉 APP 的《隐私政策》中显示“信贷业务,需要位置信息、设备信息和其他必要信息,以完成交易”。但是位置信息和设备信息,与信贷业务并没有业务关联关系,即使没有位置信息和设

APP《隐私条款》中在授权第三方部分表示“与合作伙伴共享您的某些必要的个人信息”。到底是哪些“某些必要的个人信息”,并未做比较明确清晰的说明。“如果涉及到 C2、C3 类别信息,一旦与不规范的第三方合作则存在较大数据隐私泄露、被滥用等安全隐患。”有业内人士分析表示。

也有不少金融 APP 更新了相关规定。在京东金融 2020 年 1 月 9 日更新的《隐私条款》中规定,“我们只会共享提供服务所必要的个人信息,任何第三方无

## 第三方不能随便收集用户信息了

金融 APP 的《用户协议》中授权第三方收集、使用个人金融信息是惯常操作,也是存在个人信息安全隐患的“重灾区”。

依据《规范》的要求,企业不得委托或授权大数据公司、无个人征信牌照的征信公司收集 C2、C3 类别信息。由于这两类信息涉及鉴别用户身份、账户安全,敏感度更高,因此将无金融资质机构排除在外。

新快报记者在调查中发现,不少金融 APP《隐私条款》中含糊其词。如中邮钱包