数字支付时代——

谁来追责用户信息泄露

全球领先的数字支付技术公司Visa和新华社《经济参考报》日前在北京联合发布《数字支付安全与隐私保护中国大陆消费者态度调查报告》(以下简称《报告》)。《报告》指出,消费者在使用数字支付工具时最担心的并非向支付机构提供个人信息,而是"被商户泄露个人信息"以及"个人数据被转移至第三方"。数字支付监管应侧重于防范商户泄露客户信息;同时,金融机构和数字支付机构应加大力度,做好消费者教育沟通工作。

据悉,《报告》在中信银行信用卡中心的大力支持下,通过中信银行信用卡中心的技术平台,对来自北京、上海、广州、深圳以及其他地区的24387名个人消费者进行了问卷调查。

便利性是前提 安全性是根本

调查发现,消费者使用数字支付工具的主要是为了方便地完成支付,但个人隐私保护和安全防范机制,是消费者会否选择该种支付工具的决定性因素,商家的优惠促销并不是决定因素。

在选择具体使用何种数字支付工具时,59.6%的受访者选择"便捷"作为首要考察因素。其次,分别有8.4%、10%和10.4%的受访者会从"安全防范机制""信赖支付企业的声誉"和"健全的个人隐私及信息保护政策"的角度来考虑。只有6.4%和5.2%的受访者会从"商家广泛受理及促销活动"和"周围人士都在用"的角度来考察和比较。

《报告》认为,成功的数字支付工具是便利性和安全性的结合,便利性是前提,安全性是根本,是影响消费者是否会使用数字支付方式的关键因素,也是影响整个数字支付产业信誉的关键。消费者对数字支付安全性和隐私保护有着同等高的期待和需要。

Visa大中华区总裁于雪莉表示:"作为一家全球化的数字技术公司,'安全'已经成为Visa企业文化的DNA。我们始终倡导'负责任的创新',即不断在数字支付的便利性和安全性之间寻找平衡。"

中信银行信用卡中心副总裁张明表示,"我们一直高度重视数字支付的安全性,也非常关注对客户隐私的保护。为了顺应新技术和新业务的发展,中信银行信用卡中心搭建了云平台治理体系和自主可控的安全防护系统,组建独立团队,保护客户端、合作伙伴和内部系统的安全,推动支付安全体系不断完善。"

非接触支付最安全

《报告》指出,消费者对潜在隐私泄露渠道的关注程度存在较大差异。对"被商户泄露个人信息"这种隐私泄露方式非常担心的消费者比例高达67%,对"将个人数据转移到第三方"这种隐私泄露方式非常担心的消费者比例达到62%。而仅有38%的消费者担心"被支付机构获取个人信息"可能导致隐私信息泄露,明显低于前两种方式。

《报告》同时也发现,消费者作为非专业人士对金融机构和数字支付工具的认知,与真实情况存在一定的偏差,这反映出金融机构在消费者教育与沟通方面存在欠缺。金融机构应该就自身在保护消费者/持卡人隐私信息方面的投入与措施等方面,与消费者/持卡人保持有效沟通,并进一步做好相关教育工作。从消费者权益保护的角度看,对数字支付的监管,应侧重于防范商户可能成为泄露客户信息的渠道。

值得关注的是,在消费者眼中,"通过银行卡非接触式支付"安全度最高(68%),其次是"二维码支付"(67%)。而"基于设备终端的非接触式支付"的安全性排在第三位(60%)。此外,调查显示,在回答"常见的数据安全保障措施"时,消费者认为"收到实时交易信息"是最重要的安全措施。

加强消费者教育必不可少

《报告》认为,高支付环节安全水平和加强消费者个人隐私保护,不仅需要支付服务商采用更加先进的技术,开发产品与服务。同时,还应加强对消费者安全意识和隐私保护意识的教育,要针对不同性别、不同年龄、不同教育水平和收入群体的消费者提供具有针对性的金融产品和服务。

《报告》还认为,由于罪犯分子的手段变得越来越高明,支付机构必须通过技术创新、加强合作和完善业务流程等多方面的努力创建多层次的安全机制,以确保总能走在犯罪分子的前面。Visa公司大中华区总裁于雪莉表示:"我们必须动员、教育消费者,帮助他们建立自我保护意识。每个人都在系统安全方面负有责任——其中包括消费者自己,消费者必须成为支付安全解决方案的有机组成部分。只有协同合作,才能维护数字支付产业的信誉,从而推动经济与贸易的健康可持续发展。"

三分之二消费者个人信息被泄露

网络带来方便快捷的同时,个人信息泄露也成为不可忽视的问题。中消协日前发布的《2014年度消费者个人信息网络安全报告》显示,网络针对消费者个人信息"窃取"和"非法使用"的黑色产业链呈现爆发性增长态势,消费者因个人信息泄露造成的经济损失数目惊人。三分之二的消费者在接受调查时透露个人信息曾被泄露,六成被调查者认为,服务商暗自收集是个人信息泄露的最主要途径。

中消协副会长兼秘书长常宇指出,近年来个人信息泄露事件频发,对网民造成了金融资产和个人信息安全等多方面危害。

专家为此呼吁应尽快建立个人信息保护标准规制,规范行业企业在消费者个人信息的采集和使用,通过有效的技术手段提升消费者个人信息数据库安全,从源头上斩断伸向消费者个人信息的"黑手"。

去年年底至今年年初,中消协联合360互联网安全中心发起了"网民个人信息保护状况调查",调查结果显示,消费者对于互联网个人信息保护现状满意度低,将近六成的消费者选择非常不满意和不满意。

三分之二的消费者在接受调查时明确表示,过去一年内个人信息曾被泄露或窃取,有33.14%的受访者称,曾遭受过经济损失和人身伤害。

报告总结指出,不法分子非法获取消费者个人信息的形式主要包括无良商家盗卖、网络数据窃取、木马病毒攻击、钓鱼网站诈骗、二手手机泄露和新型黑客技术窃取等。中消协表示,一些掌握大量用户个人信息的商业机构由于管理不善,内部员工盗卖信息的事件时有发生。

中消协指出,我国未有统一、有效的法律制度作为保障也是不可忽视的因素,有必要尽快推动个人信息保护立法。

调查报告认为,要解决消费者个人信息泄露和滥用的"顽疾",最终还应回归法治轨道。应明确网络服务商的企业责任,明确互联网企业应承担的社会责任。制定颁布统一的《个人信息保护法》,对个人隐私权全面保护。

日前,『第四届互联网安全领袖峰会』在北京拉开帷幕。本届峰会的主题为『安全强驱动 数字新生态』,吸引来自国内外政府机构和互联网金融、智能汽车、物联网、智能硬件等行业的数百名顶尖网络安全专家与会。图为腾讯高级副总裁丁珂在大会上发言。

防止隐私泄露重在有效监管

近日,一项调查结果显示,88.9%的网友在电商平台购物过程中,表示有网购信息被泄露的经历。另一项调查数据则显示,有596位网友认为自己遭遇过网购信息泄露,占投票人数比例的71%。

上述调查结果并不出人意料。用户个人信息早已成为可资利用、有利可图的商业资源。从泄露隐私,再到传递信息、贩卖隐私,一条条高效率的利益链条不停运转。调查数据表明,只有不足6%的网友认为是自身原因导致的网购信息被泄露。在网友自我保护意识空前高涨的当下,盗取信息的手段如此高明、多样,让人失去了抵抗力。

泄露用户个人隐私固然有风险,但与收益相比,其犯错成本较为低廉。截至目前,我国还未制定专门针对个人信息保护的法律法规。但个人只有在隐私信息确实被侵犯,并发生了实际损害之后,才能主张侵权责任赔偿。在人们对互联网依赖日益加深的情况下,需要出台更便捷的法律保护措施。

尽管购物平台理应承担起保护用户信息的责任,尽管舆论认为许多平台并未做好本职工作,可是,又有多少平台为自身的不作为付出过惨痛的代价?

消费者权益保护法明确规定,经营者及其工作人员对收集的消费者个人信息必须严格保密,不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施,确保信息安全,防止消费者个人信息泄露、丢失。现实情况是,平台往往以各种借口将泄露用户信息的责任推卸给他者。

要确认信息泄露的责任主体,有赖于专业技术渠道和取证手段。广大网友虽心怀不满,但在体量庞大、财大气粗的购物平台面前,往往缺乏话语权。与其指望电商从业人员自觉提升素养,不如用强有力措施保障用户的隐私安全。相关法律法规能否得到细化,政府部门如何积极介入,进行有效监管,才是亟待解决的问题。

本版资料来源:新华网

工作简报 免费赠阅 编辑部地址:金坛区晨风路61号 新闻热线:82368015 82368022 在线阅读:www.jintannet.com 投稿信箱:jrjt002@163.com 常州信泰印务有限公司印刷