“金融知识进万家 龙的传人用龙卡”

——安全用卡，防范诈骗

近几年信息技术的进步，让信用卡无论是在形态上还是在使用方式上都得到更进一步的发展：出现了更新颖的信用卡类型、更灵活的刷卡方式、更开阔的使用场景、更加人性化和个性化的使用体验。但是，信用卡在给消费者带来便利的同时，风险也相伴而来，尤其是欺诈风险，随着信用卡功能从最初的单一刷卡，发展到现在可广泛应用于人们生活的各个方面，欺诈风险的形态也呈现出多样化趋势。

一、信用卡欺诈风险类型

（一）冒用他人真实身份取得信用卡后进行盗刷

1.伪冒申请。持卡人的真实身份证件被伪冒人冒用，或伪冒人使用伪造、变造的身份证件骗领并使用信用卡。

2.未达卡。持卡人的信用卡在邮递寄送过程中被伪冒人截获并冒用。

3.账户转移。伪冒人假冒持卡人名义，变更持卡人在银行预留的手机号码、账单地址等重要信息，欺骗银行补发信用卡并冒用。

（二）窃取信用卡信息后进行盗刷

1.网络伪冒。持卡人信用卡信息被伪冒人窃取，并通过网络等方式冒用。

2.伪卡盗刷。伪冒人通过窃取、收买等手段非法获得他人信用卡信息，伪造虚假的信用卡并使用。

3.遗失被盗。持卡人卡片被伪冒人拾获或窃取并冒用。

二、养成良好用卡习惯，安全从点滴做起

面对形态多样的欺诈风险，银行会从各个方面努力提升信用卡的安全防护措施，让您能够安全放心的使用信用卡。同时，对于您来说，养成以下良好的用卡习惯，也可以最大限度防范欺诈风险的发生:

（一）您应直接到银行网点、或登录银行官方网站申请信用卡，不要将个人资料信息随意提供给银行工作人员以外的其他人员；在办理信用卡各项业务需提供个人材料时，最好在材料中标明“仅限于办理XX银行信用卡业务使用”字样。

（二）建议您在使用信用卡时要设置交易密码，不要图方便好记而将自己的生日、身份证件号码、简单数列（111111、123456）等设置成密码，并且最好将交易密码和信用卡自助业务的查询密码设置为不同密码。

（三）您在ATM机上使用信用卡进行余额查询、取现等业务时，要留意ATM机是否有插卡口不规整、插卡口外有异物粘连等异常情况，一旦发现异常请停止使用，并及时向银行反映。在输入卡片密码时，应注意用手遮挡数字键盘，避免密码被不法分子安装的摄像头摄录。

（四）您在商户进行刷卡消费时，要让卡片始终在自己

的视线范围内，防止收银员通过非法装置窃取卡片信息；在输入密码时，也应尽可能用身体或另一只手遮挡数字键盘后再输入密码，避免密码被他人窥视。

（五）您应选择信誉好、运营时间长的网站进行网购。最好直接从官方网址进行登录，不要随意点击不明链接、悬浮窗口、或电子邮件/短信等方式提供的网址，避免进入虚假的钓鱼网站。不要在公共上网场所登录网上银行、进行网上交易或输入个人信息，以避免卡号及密码等信息被他人盗取。

（六）您在境外网站进行支付时，应尽量选择支持信用卡3DS支付验证服务的网站，并在支付时保持手机畅通，用于接收手机动态验证码，确保交易安全。

三、关注用卡情况，防范从细节做起

除了养成良好的用卡习惯之外，您对信用卡的使用情况要保持关注。如果发现有异常情况，应在第一时间采取相应的安全保护措施，这样不仅可防范自身的财产损失，还可为银行和司法机关后续调查提供有利的帮助。

（一）您申办银行信用卡成功获得出卡短信后，应及时关注卡片邮寄情况，如果长时间（一般10天以上）仍没有收到卡片，可以根据银行短信告知的挂号信单号到附近邮局查询，或者致电客服中心进行查询。

（二）您如果发现自己的信用卡遗失，应在第一时间致

电客服中心对卡片采取挂失等管控措施，及时防范可能出现的信用卡被盗刷风险。

（三）您如果接收到银行发送的异常交易短信提示，或通过账单查询发现自己的信用卡可能被盗刷了，应第一时间致电客服中心反映，并在就近的ATM机上通过查询余额等方式确认自己当时所处的位置，以便于后续调查。

（四）您如果接到银行工作人员电话，询问某些具体交易情况时，请配合工作人员进行确认，一旦发现自己并没有使用信用卡进行该交易，请及时反映，并在就近的ATM机上通过查询余额等方式确认自己当时所处的位置。

（五）您如果发现自己的手机出现异常停机的情况，要及时致电电信运营商了解情况，并同时致电银行，查询自己名下的信用卡是否有信息更改和交易发生，一旦发现异常要立即向银行反映，采取必要的管控措施来防范可能出现的风险。

（六）为保障您账户信息安全，对于某些曾经在高风险商户刷卡，可能存在信息泄露风险的持卡人，银行会通过电话或短信形式提醒您换卡，并提供免费换卡服务，请您积极配合工作人员进行相应操作。

（七）您要认准银行发送短信的官方号码，如果收到非银行官方号码发送的短信，要求提供个人信息或联系非银行官方客服电话的，均为虚假诈骗信息，不应理会。

（八）您如果接到自称“卖家”、“网站客服”、“银行工作人员”、“政府机关工作人员”等的电话，以银行系统问题、网站升级、购物退款退税等名义要求您提供信用卡卡号、有效期、安全校验码（CVV2）、短信动态验证码等信息的，一定不可相信。如已向他人泄露了个人信息的，应立即致电建行客服中心。