随着支付交易形态日益多元，金融和通信、互联网等产业之间融合加深，线上欺诈的攻击对象也从金融机构、持卡人扩展到商户网站、手机运营商。下一步在加强对信用卡产业链配套规范体系建设的同时，还应尽快出台针对移动支付、二维码支付等创新业务的相关管理细则，形成制度规范。

当线上支付为消费者带来全新体验的同时，其因信息泄露导致的欺诈风险也在迅速上升。中国银行业协会近期发布的《中国信用卡产业发展蓝皮书（2014）》显示，伪卡、虚假申请、互联网欺诈、失窃卡、账户盗用是信用卡最突出的五大欺诈类型，其中互联网欺诈呈现快速增长态势，2014年欺诈损失金额为2245.4万元，比上年增长59.1%。

支付信息如何泄露

业内人士表示，互联网欺诈的关键环节是获取支付数据与信息。随着支付交易形态日益多元，金融和通信、互联网等产业之间融合加深，线上欺诈的攻击对象也从金融机构、持卡人扩展到商户网站、手机运营商。

“常见手法有三种，一是利用手机运营商管理漏洞，通过伪基站发送钓鱼链接；二是通过木马、黑客技术攻击商户网站，获取支付订单信息；三是以退货、网银升级等理由骗取持卡人的银行卡卡号、动态验证码等支付信息。”中国银行业协会银行卡专业委员会相关负责人介绍。

北京某事业单位员工晏玉回忆，今年8月她曾收到号码为10086的短信，称“未兑换的话费积分即将清零，请及时登录10086zem.com下载客户端兑换216.8元礼包（中国移动）”。“我当时以为是中国移动的客服电话，就按照要求登录，输入了银行卡号、身份证号、支付密码，随后卡片就被盗刷了3000元。”晏玉说。

“这是典型的伪基站冒充手机运营商发送诈骗信息，诱骗持卡人登录钓鱼网站窃取信息然后盗刷。”中国工商银行牡丹卡中心内部人士表示，保管个人账户信息十分关键，尤其是快捷支付时的核心信息“短信验证码”，银行在任何时候都不会向持卡人索要密码等相关信息。

该人士表示，与钓鱼网站原理类似，有些诈骗手法是以网银升级、系统升级等名义诱骗持卡人登录虚假网址，进而骗取信息。

值得注意的是，信息泄露的途径还在向商户网站扩散。中国银行业协会银行卡专业委员会相关负责人介绍，去年以来，在全球范围内已陆续发生多起黑客、木马攻击

网站窃取支付订单的案件。

金融机构如何应对

虽然支付信息泄露的可能途径涉及金融机构、通信、电商等多个主体，但作为网络支付市场的主要参与者，金融机构在创新防控技术、应对信用卡互联网欺诈方面大有可为。

业内人士介绍，从技术手段看，为了防止支付信息在传输过程中被窃取，多家商业银行在线上远程支付的过程中选择采用令牌技术。借助该技术，持卡人正在交易的16位账号在传输过程中有了一个数字化的令牌“替身”。

“从工行HCE云支付信用卡的运行过程看，工行搭建了一个云端服务器，用以存储海量的银行卡账户信息，在客户的手机APP中仅存储令牌作为银行卡的替身，也就是不在客户手机里显示真实的卡片信息，而是让云端服务器与客户手机APP实时交互，完成信用卡在客户手机端的发卡交易、密钥下载、身份验证等一系列过程。”工行牡丹卡中心总裁栾建胜说。

除了技术升级，部分银行还推出了“交易开关”服务。以广发银行为例，目前该行已针对境内无卡交易、港澳台交易、境外交易、交易限额管理等推出了开关功能，持卡人可以自主设置交易开关。

“作为日常保障，各行应重视对网络异常交易的实时监控，有条件的可建立专门部门或团队。”工行牡丹卡中心内部人士表示。

联手打造安全用卡环境

由于网络支付市场参与主体日益多元，中国银行业协会银行卡专业委员会建议，除了金融机构，产业各方主体应携手合作，尤其应深化警银、银法合作。

目前从监管法规层面看，信用卡支付行业的监管和风险防控体系已初步建立。中国银行业协会银行卡专业委员会认为，下一步应加强对信用卡产业链配套规范体系的建设，同时，还应尽快出台针对移动支付、二维码支付等创新业务的相关管理细则，形成制度规范。

从产业各方主体合作的角度看，该委员会建议各金融机构应深化与互联网企业、通信、公安、工商等机构的合作。“比如与通信部门合作开展互联网不良信息清扫，与工商部门合作严查非法套现广告、空壳公司的注册行为等。”该委员会相关负责人说。

“治理信用卡互联网欺诈尤其要重视警银、银法合作。”上述负责人表示，金融机构今后可在案件监测预警、执法协作等环节加强与公安经侦部门的联动，同时与司法部门合作，维护金融债权。具体来看，可建立司法协助网络工作平台，将人民银行、各商业银行、公安、法院、工商局等各类机构的数据整合起来。

“监管方为行业提供良好政策的环境，卡组织做好交易清算、受理环境建设等基础工作，商业银行应在贯彻政策、控制风险的基础上积极创新。”中国银行业协会专职副会长杨再平说，各方应在实践过程中不断规范网络支付的产品标准、行业规则和监管制度，共同打造安全的用卡环境。