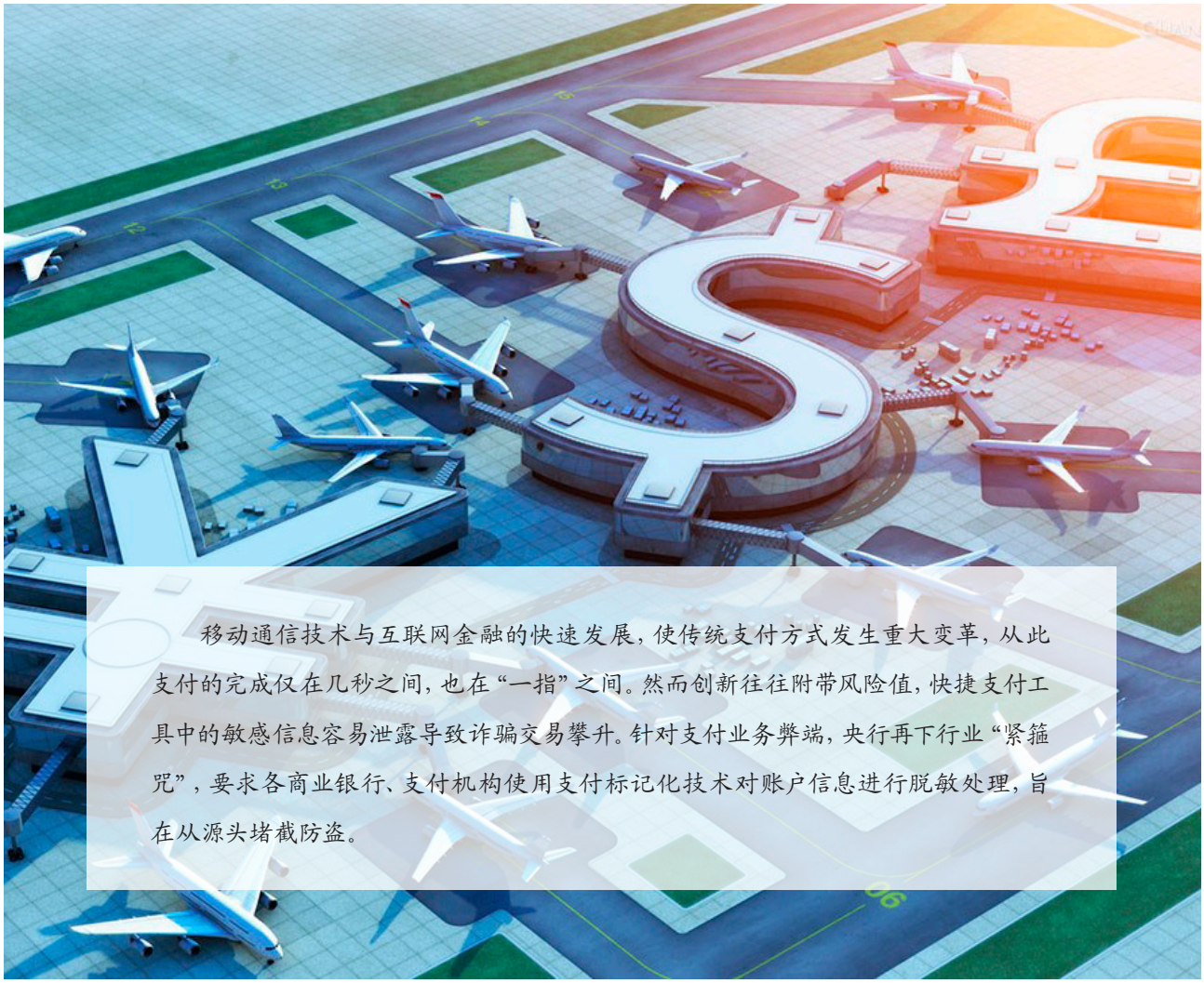
2016年 · 第9期
栏目编辑：王雪玉 E-mail:spytree99@163.com

支付风控新术上线

■ 本刊首席编辑 罗锦莉



移动通信技术与互联网金融的快速发展，使传统支付方式发生重大变革，从此支付的完成仅在几秒之间，也在“一指”之间。然而创新往往附带风险值，快捷支付工具中的敏感信息容易泄露导致诈骗交易攀升。针对支付业务弊端，央行再下行业“紧箍咒”，要求各商业银行、支付机构使用支付标记化技术对账户信息进行脱敏处理，旨在从源头堵截防盗。

创新附带风险值

现代社会支付技术变革第一步，应属现金支付向银行卡、电子支付的迁移。无纸化交易不但绿色环保，而且破除了交易主体之间的时空限制，实现不同维度的交互。随着移动互联网、大数据等新兴技术的不断推进，新一代电子支付手段更是体现了金融科技在民生服务的智慧性跳跃。

如今，中国移动支付市场已形成三股势力，一是以支付宝、微信为代表的互联网金融企业，深耕便捷的小额支付领域，应用场景广泛，民众依附性强；二是苹果、三星等与银联完成“站队”的硬件企业，自带数亿用户，与连接线下商户和银行的银联实现完美对接，利益互补；第三股势力便是迎着互联网金融的东风大胆创新的商业银行，作为金融业的龙头，它们在信用等级、支付结算、资金存管等方面具有独特优势。

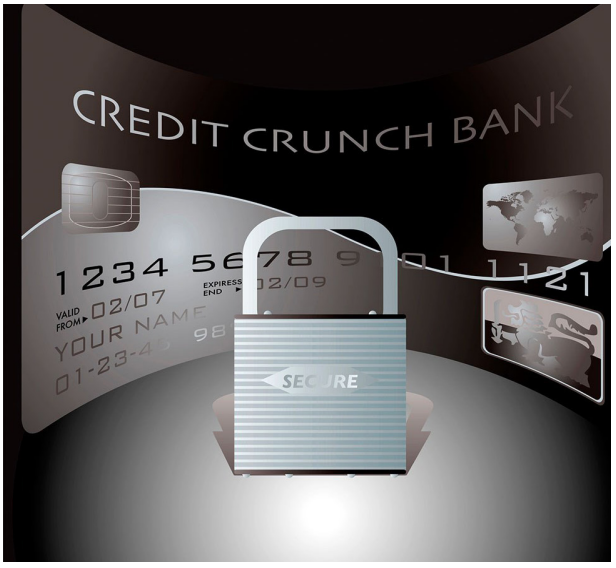
三股势力风云激荡，支付圈不断派生出新的交易方式，社会资金交易规模也在持续扩大。根据央行最新数据显示，截至2016年1季度末，全国共办理非现金支付业务2 267.97亿笔，金额888.28万亿元。其中银行卡发卡量高达56.58亿张，人均持卡4.15张；在电子支付方面，移动支付业务保持较快增长态势，实现交易56.15亿笔，支付金额达52.13万亿元，同比分别增长308.08%和31.05%。

资金交易规模如此庞大，业界又是如何保障其安全的呢？目前，业内已提供多种验证方式来降低交易欺诈的概率，以数据加密为主的账户安全保护、系统定期渗透性测试和端到端加密等，是保护账户信息安全的主要手段，但普遍存在局限性，有卡交易存在被侧录的可能，而无卡的电子支付因无须验证银行卡密码，不需要U盾、网银等多重验证，更是存在较大的安全隐患。其中，手机木马病毒成为移动支付的重大灾害。据腾讯报告数据显示，2015年新增的支付类病毒超过32.6万个，全年被支付类病毒感染的用户高达2 505万，据此推算，平均每天就有8万多人受到手机木马病毒的威胁。

支付标记化技术上线

显然，银行账户信息的传递和存储已成诈骗交易的一片沃土。此前，央行多次发文，要求加强多重身份验证，如为商业银行责任加码的“10号文”（即《关于加强商业银行与第三方支付机构合作业务管理的通知》），以及规范非银行金融机构的“43号文”（即去年底央行发布的《非银行金融机构网络支付业务管理办法》）。而就在今年6月，央行祭出了一份特急文件——《中国人民银行关于进一步加强银行卡风险管理的通知》（以下简称《通知》），要求各商业银行、支付机构、银行卡清算机构健全支付敏感信息安全内控管理制度，严控金融外包机构资质。《通知》还注明了敏感信息范围，包括银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等支付交易信息，从细节处着手保障每位持卡人的切身利益。

另外，《通知》要求，自2016年12月1日起，各商业银行和支付机构应使用支付标记化技术



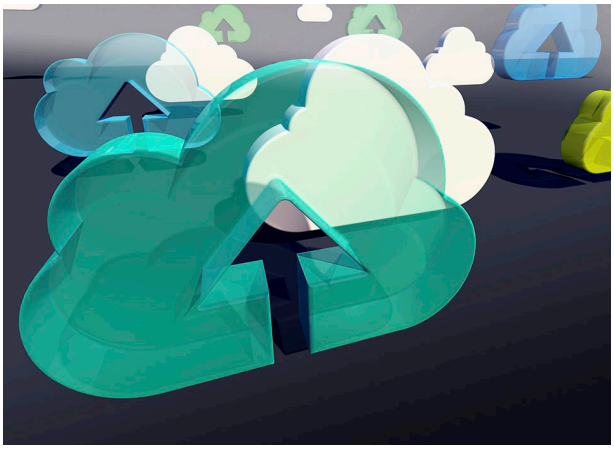
（Tokenization），对银行卡卡号、卡片验证码、支付机构支付账号等信息进行脱敏处理，并通过设置字符标记的域控属性，从源头控制信息泄露和欺诈交易风险。

纵览全文，我们在《通知》中发现了较为陌生的名词“支付标记化”。据了解，支付标记技术始创于2014年，是国际芯片卡标准化组织EMVCo正式发布的一项最新技术，原理在于通过标记（token）代替银行卡号进行交易验证。简单来说，就是在银行卡交易过程中，用替代值代替原始信息，如用支付标记替换卡号，用支付标记的有效期替换银行卡的有效期，而相应的替代值仅使用一次，且标记化可应用于跨行交易的整个环节。因此，即便交易信息遭第三方截获，也能避免因卡号信息泄露带来的风险。

根据标记化的覆盖范围和应用目的，支付标记化可分为收单端标记、发卡端标记和卡组织标记。交易过程起步时，由商户使用标记发起交易，经收单机构系统，被卡组织转换为卡号发送至发卡银行，发卡银行负责比对原始卡号，最终进行交易处理。

从上面的交易流程可以看出，支付标记化的最大优势体现在能从源头上对敏感信息进行处理，使持卡人的账户信息隐身于交易中。另外，支付标记化技术能够实现自主设置域控属性，所谓域控，即交易次数、交易金额、有效期、支付渠道等交易场景，支付标记化技术通过标记限定的使用场景，提升了支付安全性。并且它有灵活于传统银行卡的验证方式，通过个人身份信息和支付信息附加验证、风险等级评估等功能进行风险防控。

值得一提的是，支付标记不影响持卡人的交易体验，其业务处理均在后台进行，与日常支付行为无异，只有在部分交易场景中，显示在商户收据中的最后4位支付标记，才让持卡人感知到该标记的存在。



技术推动产业升级

基于以上优势，支付标记化将为保障支付交易安全、创新移动支付以及提升金融服务质量打开一片新的发展领域，至少在提高安全性的前提下，为一些快捷的支付体验赢得央行的“宽容”。

此刻不得不让人提起前几年被央行一度叫停的二维码支付。由于缺乏技术标准和安全标准，安全性薄弱一直是二维码支付的一块短板，但因为有足够便利的支付体验，即便被叫停的两年间，二维码支付并未销声匿迹，甚至在进一步扩大其支付生态圈。

显然，一味地叫停无法降低市场的活跃度，堵不如疏，央行深谙其道。近期，央行重开闸门，确认了二维码支付的市场地位，并表示将推动二维码技术标准和安全标准的制定。现如今，基于token的支付框架，能够让扫描的二维码数据生成交易密文，通过严格控制有效时间和标记次数，降低交易风险，为央行进一步推进二维码支付保驾护航。

而国内市场中，支付标记化技术已实现落地。去年，工农中建交等20多家商业银行联合发布的非接触式支付产品“云闪付”，便是搭乘了支付标记化技术的东风。

与传统借助银行卡芯片、手机SIM卡等实体介质不同，“云闪付”同时结合了支付标记化技术和HCE

（主机模拟卡片），以动态密钥、云端验证等方式保障支付安全。可以说，支付标记化技术推动了实体银行卡向无芯片银行卡的演变，为商业银行的金融创新历史翻页。而早在2013年，中国银联就启动了对支付标记化的技术研究，《中国银联支付标记化技术指引》已于近期出炉。

至于挺进中国市场的国际IT巨头中，苹果公司的产品Apple Pay，三星公司的Samsung Pay等，皆以支付标记化技术制定基于eSE（全终端）的移动支付方案，谷歌阵营中的Android Pay也不例外，相信很快便会在中国市场中看到它的身影。此外，银联、Visa、万事达等卡组织的云端支付方案也都使用了支付标记化技术。

国内的支付标记化技术渐入佳境，国外的标记化技术已相对成熟。

在发卡端标记方面，国外的发卡银行在新业务技术的发展推动下也逐渐转变了思路，以卡号标记化代替在磁条、芯片介质或手机安全单元中存储原始卡号与相关信息。目前，为适应移动互联网时代无卡支付的需求，西班牙、韩国等国家和地区的银行正在积极探索基于发卡端标记的产品。

在卡组织标记方面，Visa可谓该阵列的排头兵。在2014年，Visa接连放出三大招：完成了美国地区的发卡系统改造，在亚洲移动通信博览会上展出了使用字符标记化技术的移动支付产品，以及在Apple Pay中应用了该技术。

而在收单端标记方面，以美国为例，收单端标记在该地区的收单机构中已得到广泛运用。由于美国接连不断地发生持卡人账户信息泄露事件，这令商户面临重大的经济惩罚和法律制裁，他们希望不再保留持卡人卡号与有效期。为避免再次发生大规模的信息泄露事件，第三方支付行业数据安全标准（PCI DSS）作出紧急响应，要求必须对卡号与有效期进行强加密和标记化。基于政策需求，并结合行业的规范指导，良好的市场运作环境催生了一批提供标记化服务的安全厂商，如美国的RSA公司以及Visa的子公司CyberSource等。

此外，根据EMVCo关于支付标记化的生态系统，在不改变现有产业分工的前提下新增了标记申请方（TR）以及标记服务提供方（TSP）。标记申请方负责搜索持卡人卡号与有效期等相关信息，向标记服务提供方申请标记并将其返回相关方；标记服务提供方则负责生成支付标记、有效期和担保级别，并完成支付标记向卡号的转换。可以预见，以支付标记化为技术规范的支付产业，将培育出不同类型的标记申请方和标记服务提供方，在为收单业务与发卡业务提供强有力的支撑之余，也为产业带来诸如场景控制、身份认证、风险识别与分析等增值服务，推动支付各环节的发展与产业细化。FT