从“刷脸”到“刷掌”，生物识别技术能否让支付更安全

在确保安全的情况下，“刷掌”成为支付验证的辅助手段之一。从探索到推广，“刷掌支付”还面临多重挑战和问题。

文 | 董希淼

继“指纹支付”“静脉支付”“刷脸支付”之后，“刷掌支付”也要来了。日前，“微信上线刷掌支付”登上社交平台热搜。“微信刷掌支付”小程序已上线，其开发主体为财付通支付科技有限公司。“刷掌支付”是将生物识别技术运用于支付领域的一种新尝试。在确保安全的情况下，“刷掌”可以成为支付验证的辅助手段之一。但“刷掌支付”从探索到推广，还面临多重挑战和问题，对生物识别技术在支付领域应用的规制也应进一步加强。

利弊两面观

近年来，技术创新与支付领域深度融合发展，支付机构和金融机构应用生物识别技术，纷纷推出相关产品和服务。借助人脸识别技术的“刷脸支付”，受到人们青睐。而目前备受关注的“刷掌支付”，也是将生物识别技术运用于支付领域的一种新尝试。

“伸手感应，识别支付”，“刷掌支付”由腾讯优图和微信支付合作推出。目前，腾讯已在部分地区推广“刷掌支付”，在授权场景中，可以通过手掌识别快速完成付款或者身份验证。用户开启该功能后，只需要伸手在掌纹识别区接受扫描，即可完成日常消费的支付。而早在2021年8月，微信就开始内测“刷掌支付”。当时，微信在公开回应中表示，“刷掌支付”仅为微信内部技术预研，尚无应用计划。直到日前，“微信刷掌支付”小程序上线，再度引发市场关注。

与此同时，腾讯科技（深圳）有限公司申请了多项与“刷掌支付”相关的专利及商标。“企查查”信息显示，腾讯已申请了识别模组及掌部生物信息识别设备、刷掌设备、识别设备和支付设备等专利。今年8月以来，腾讯已申请“微信刷掌支付”“微信刷掌服务”“微信刷掌”等多个商标。显然，腾讯在“刷掌支付”方面的探索并非一时兴起，而是从技术、专利、商标及场景等方面进行了全方位布局。

全球支付科技发展趋势

> 资料来源：安永智库

亚太市场销售点支付方式

	2021	2025
数字钱包 / 移动钱包	44%	56%
信用卡 / 签账卡	19%	17%
现金	16%	8%
借记卡	15%	14%
零售商 / 银行分期付款	4%	3%
预付卡	2%	1%
先买后付	1%	1%

> 资料来源：worldpay

不可否认的是，“刷掌支付”具有一些独特的优势。与其他应用人脸、指纹、静脉等生物识别技术的支付方式不同，“刷掌支付”有两个突出的特点：第一，可以在应用生物识别特征识别时加入人的主观因素，例如可设置不同的手势，使得“刷掌”的个性化和安全程度更高；第二，人们外出戴口罩已成为普遍行为，“刷掌”比“刷脸”更方便，并有助于降低病毒传播的风险。在确保安全的情况下，“刷掌”可以成为支付验证的辅助手段之一。

但是，单纯从技术本身看，“刷掌支付”

单纯从技术本身看，“刷掌支付”的大规模推广应用仍然面临着硬件环境和场景选择的双重约束。

“刷掌”技术在提升支付服务便捷性的同时，同样存在一些已知或未知的风险，技术的安全性和系统的可靠性需要进一步验证。

的大规模推广应用仍然面临着硬件环境和场景选择的双重约束。从硬件环境看，“刷掌支付”需要专用的刷掌设备，这是“硬约束”。尽管腾讯方面提供刷掌设备，但设备从生产到铺设、商家从接受到学习都需要时间，设备成本是否会转移到商家以及终端用户目前也并不明确。从场景选择看，“刷掌支付”主要应用于线下场景，这是“软约束”。在科学精准防控二十条措施公布之后，疫情防控政策不断调整优化已经成为趋势。如果经济社会回归正常，公众摘下口罩，“刷掌支付”相比“刷脸支付”的优势也将变得不明显。对用户而言，在众多支付验证方式中，“刷掌支付”是否真的方便还有待验证。

应用须审慎

技术是一把双刃剑，就支付领域而言，新技术的应用往往伴随着新风险的产生。据媒体报道，北京市民李红（化名）被诈骗人员骗走了交通银行账户中的将近 42.9 万元，这一事件暴露出交通银行的人脸识别技术存在严重漏洞。报道显示，李红被骗当天共有 7 次操作涉及人脸识别，均显示识别成功通过，其中 1 次为借记卡申请、1 次为登录密码重置、5 次为大额转账，除了第一次不涉及活体检测，后 6 次操作“活检结果”均为成功。虽说掉入诈骗分子的圈套是造成李红被骗的主要原因，但 IP 地址显示为我国台湾地区的诈骗分子，居然 6 次顺利通过交通银行的人脸识别比对。据报道，除李红之外，还有多位交通银行用户也有过类似遭遇，被骗资金总额超过 200 万元。

而“刷掌”技术在提升支付服务便捷性的同时，同样存在一些已知或未知的风险，技术的安全性和系统的可靠性需要进一步验证。

一是信息泄露风险。生物识别特征具有唯一性，一旦泄露则后果严重。不法分子或可在公共场所非法获取用户掌纹等信息，导致基于掌纹的身份认证系统可被轻易绕过。账户密码被盗尚且可以修改，掌纹信息被盗可能难以找回。

二是算法漏洞风险。目前，活体检测等算法仍在快速迭代，识别通过率、误识率等关键指标相互关联、难以兼顾，且容易受到外界环境因素干扰。其中可能存在隐藏的未知漏洞，一旦被不法分子发现并利用，将产生系统性风险。

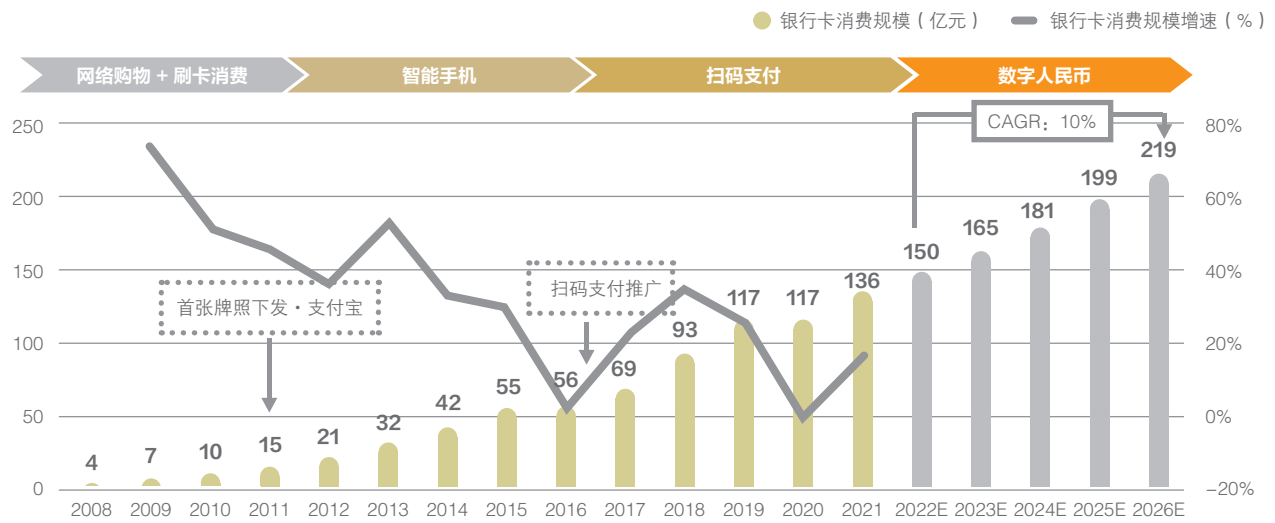
三是假体攻击风险。在人脸识别中，不法分子通过照片、视频、高仿面具等手段，仿冒用户人脸进行 2D 或 3D 攻击，屡见不鲜。在“刷掌支付”应用中，假体攻击等新型攻击手段是否还会出现，需要进一步观察。

而且，当下一些金融机构和支付机构自认掌握（或引进）了一些先进的生物识别技术，满足于提升用户体验，而未充分评估和防范风险。这种不审慎的行为，给金融业务埋下了风险隐患。过度的便捷往往给不法分子带来可乘之机，通过远程、非接触方式，在用户本人毫无察觉的情况下“无声无息”地获取用户的生物识别信息，加上手机号码作为用户社交工具也极易被获取，因而很可能导致“隔空盗刷”问题出现。

共筑安全线

无论是央行公布的《金融科技发展规划（2022—2025 年）》还是银保监会公布的《关于银行业保险业数字化转型的指导意见》，都对坚守安全底线、防范技术风险提出了明确要求。今年 10 月，央行公布《金融领域科技伦理指引》，对金融领域开展科技活动需要遵循的守正创新等七个方面，提出了价值理念和行为规范。由于互联网的虚拟化、金融服务的数字化、参与主体的多样化，当前金融科技风险呈现出蔓延速度快、隐蔽性强、潜伏期长、外溢效应明显等特点，支付机构和金融机构在敏感信息

第三方支付的发展历程与规模



> 资料来源：ifind，招商证券整理

保护、客户资金安全等方面面临较大压力。

因此，无论是支付机构还是金融机构，在应用生物识别技术时，都应把安全性放在第一位，以最严格的标准审慎对待风险，在确保安全的前提下合理审慎应用。从技术的层面看，应采取数据脱敏、隐私计算、分散存储等多方面措施，保障生物识别技术安全应用。下一步，支付机构、金融机构应正确把握安全与发展、风险与创新的关系，认真落实相关要求，确保新技术、新产品安全合规，并在充分告知风险的情况下为消费者提供多种选择。如果由于新技术不当应用给消费者带来损失，应主动承担相应的责任。

生物识别技术在金融行业的快速发展和应用，引起全球范围的普遍关注，呼唤更全面完善的法律规制和技术标准。在我国，《网络安全法》《数据安全法》《个人信息保护法》构建了个人信息保护的“三驾马车”，应加强法律执行的检查和处罚力度，确保各方在法律框架之下依法合规行事。2018 年 10 月，我国金融行业首个生物特征识别安全标准《移动金融基于声纹识别的安全应用技术规范》公布。金融管理部门应加快出台并不断完善生物识别技术在支付领域的应用规范、技术标准等，推动各类参与主体提高认识、增强能力，共筑支付安全防线。消费者则要理性看待技术创新和应用，增强识别和防范诈骗的意识与能力，妥善保护个人敏感信息，降低信息和隐私泄露风险，守护好“钱袋子”安全。

（作者系招联金融首席研究员、复旦大学金融研究院兼职研究员）