在今年春节我前往墨西哥的一次旅行中，我的交通银行标准白金卡被盗刷了。在我收到第一次盗刷提醒的短信之后，我就向交通银行打电话挂失卡片。好在当时卡内的额度不多，盗刷者在进行了多次尝试之后依然没有刷掉我卡上的额度。

除了只能更换卡片进行消费之外，此次盗刷并未对我的信用卡使用造成任何影响，我也没有因此收到损失。

交通银行标准白金卡是一张磁条卡，交易方式在海外大多是采用磁条+签名的方式，极少数POS机会要求密码的验证（走银联通道或识别出是由中国地区发行的信用卡）。

虽然现在芯片卡已经进入了普及的阶段，但如果出国去很多地方刷卡，我们会发现商户还是不支持我们手里的芯片卡，最方便的刷卡方式还是刷磁条，这是为什么呢？

芯片卡的接受程度与商户POS机是否支持你的芯片有很多的关系。在市场上有两种芯片卡标准，一种是国际上应用较多的EMV标准，一种是央行的PBOC2.0标准。而除此之外，也跟北美地区芯片卡普及速度过慢有关系。

由于安全性问题，欧洲地区早在数年前就抛弃了传统信用卡磁条读卡+签名的验证机制，而在包括美国在内的北美地区，虽然芯片卡已经开始大量发放，但在刷卡机的支持上，由于利益驱使停留在磁条卡年代。

可以说，美国当前的信用卡和借记卡技术已经落后于欧洲达到数十年之久。

VISA的全球支付系统风险负责人RL Prasad表示，虽然信用卡上只有一个磁条，但磁条里面主要包括有三条轨道，三个轨道都可以写数据。其中轨道1和轨道2是最为重要的，所有的核心信息，比如持卡人的姓名、卡号、有效期和安全码都存储在这两条轨道上。

轨道3并非经常使用，主要用于高级的详细信息，比如该卡可以适用于哪些货币。但出于付款的目的，主要信息大多只存在于在前两个轨道上。

“传输该数据涉及多方，当消费者在商店中刷卡时，POS机会读取轨道中的数据并将数据传输给收单机构，” Prasad说。 “收单方将数据发送给发卡方，最终确认付款。

传统银行卡的磁条技术相对简单，磁条信息易被复制，通过使用磁条信息盗录装置复制银行卡磁条信息，再通过针孔摄像机在自助机终端上偷录持卡人密码就可以伪造磁条银行卡，从而盗刷持卡人的卡内资金。

而芯片卡则是在卡片正面嵌入了一小块金色的智能芯片。这块芯片实现了硬件升级，完善的密钥体系、脱机认证、联机双向认证等更是保障了卡片的防伪性及交易的安全性。芯片卡因为在芯片里嵌入了一个证书，每个交易都要通过这个证书才能完成，大大提高了卡被复制、盗刷的难度，从而提高用卡安全性。

“数据传输的方式很重要，磁条的记录都是静态数据，这意味着盗刷者只要专用的读卡器就可以在你刷卡的过程中神不知鬼不觉的复制你所有数据，通过复制的数据新建卡拿到可以套现的地点进行盗刷。

由于磁条上的数据都是静态的，因此复制出来的假卡，理论上来说和真的一模一样。

之所以芯片卡开始普及，也是为了降低盗刷的风险。芯片卡所存储的数据都属于动态数据，只要客户插入芯片卡，就会产生新的数据，“这也意味着克隆芯片卡非常困难。

根据Visa的最新数据，超过75%的美国店面现在接受芯片卡，Prasad表示芯片卡的接受度将会继续提高。不过，他也指出磁条技术不会消失。“我们看不到磁条完全消失，”普拉萨德说。“虽然目前世界某些地区，芯片卡的采用率已经超过90%，但认为磁条卡还会将继续使用一段时间。”

普拉萨德指出，由于更换刷卡机需要一定成本，部分中小商户可能无法及时更换。与国内的二维码移动支付已经普及不同，在北美地区，刷卡交易类型中最大的是加油类商户，也就是自助加油机。

此前自助加油机上的刷卡机经常被盗刷者加装磁条卡复制器，从2020年10月开始，盗刷责任将从发卡行转向到收单方，所以北美地区的自助加油机也将全面支持芯片卡。

如果您担心在下次刷卡时可能会被盗刷，建议你采取其他的安全措施。Prasad也在推广Visa全新推出的移动位置确认技术。说老实话，使用芯片卡并输入密码进行操作，可以避免90%的盗刷风险。

之前你在境外出行的旅行中，遇到过盗刷吗？