【互联网账户安全实践】蚂蚁金服曹凯：

支付宝互联网账户安全实践

（本文选自微金融 50 人论坛演讲汇编系列之一：微金融的基础设施，独家推出，转载请注明出处）

无可否认的是，系统的效率往往取决于机制和技术，机制和技术的进步也会带来效率的提升。同样在很多时候，机制和技术本身不是孤立的，技术的进步往往会带来机制的变革，而机制的变革又会推动技术的进步。我们在一个大的互联网安全系统当中，在安全效率和效果当中不断地推动支付宝的互联网账户安全的进步和平衡，其中有技术的部分，也有机制的部分。

通过支付宝的实践我们发现，账户安全涉及端、管、云整个体系，单纯的从端很难解决账户安全的问题。云的环节、云和端之间、管道的传输中也存在安全问题，需要我们不断地解决和管理安全的风险点。另外，在端管云的基础上可以补充一个生态的概念。在支付宝的安全实践中，我们发现生态的安全已经开始对互联网账户造成威胁。比如，现在存在

大量的“网络拖库”现象——对于不同的互联网账户，比如游戏账户和互联网金融账户，用户可能使用相同的账号和密码。这样，当别人的账号密码库存在安全问题被拖造成信息泄露的时候，可能会影响支付宝的账号安全，这就是生态问题。再比如，线下生活当中见到的电信欺诈案件开始转移到互联网的环境中，犯罪分子开始利用网络为依托实施诈骗。在这样的案件中，用户把所有基于信息的安全手段（不管是密码、数字证书还是其他的交易保障）都告诉给了犯罪分子，并在被欺骗的前提下配合犯罪分子完成了整个盗用过程。这些都是网络安全生态新形势下互联网账户面对的两种严重的威胁形式。因此，在安全中除了要考虑端管云的体系之外，我们也要考虑生态安全恶化带来的威胁。如何保障生态安全是我们需要思考的课题。

下文主要探讨两个部分：支付宝账户安全体系理念和实践以及我们在这个过程中遇到的挑战和思考。

一、支付宝账户安全体系理念和实践

从安全的角度，我们一直认为支付宝最核心的能力不是有余额宝，不是有很多第三方支付的产品，也不是有淘宝的海量交易，而是我们能够控制账户可能会遇到的风险。以不严格的方式估算，支付宝的账户安全体系保障资金有可能达到近万亿（余额宝现在有五千亿，还有大量的和支付宝账户绑定的银行账户以及用户沉淀在支付宝账户中的资金）。由此看来整个支付宝安全体系需要保护的资金量非常大，所以账户安全一直是支付宝要解决的重要问题。

个人认为账户安全包括两部分：一是很多传统的技术和思想关注的账户的基础安全，二是怎么利用互联网大数据和智能化的方式和思想去管理风险。比较早期的安全理念更多是偏重于入口的认证，比如怎样去设置一些物理的介质标识或是保护用户的身份和账户，怎样通过一些指定的客户端、卡片或者日常的对介质的管理设置准入门槛来保护身份安全，同时在入口的端上做控制，即根据入口控制。这是最早的是计算机等级保护思想的延伸，这种安全思路对网络银行的发展起到很大的推动作用。然而，这种基于入口控制的传统账户安全体系思想在现有的体系下越来越不适用。移动互联网实现以后，基于介质的、传统的方式由于用户在使用上的体验不够便利，变得可能会阻碍交易的进行，而与此同时，商户等主体获取用户的成本越来越高。据不完全统计，一个 B2C 的商户获取新用户的成本接近两百到三百元。所以支付宝账户安全体系需要平衡这种安全的效率和效果，在保障效率的同时达到安全的高强度效果；需要强调综合的安全风险管理，而不仅仅是入口的管理；需要弱化传统介质保障，通过数字化手段（包括可信的体系保障以及数字安全加密的一些机制）增强安全性；需要强调安全与企业业务并重，满足企业对业务安全的诉求；也要强调通过云和端的协同、强化安全管理。

支付宝这一套安全体系的背后是这样的一个思考：不管是早期的支付宝还是现在的蚂蚁金服，我们希望主动承担微小的风险，并通过互联网的思想和技术全面管理风险，把最终的风险收益和业务的便利带给用户和商户；我们希望在整体社会或者整个支付宝的平台体系当中，大幅度降低交易成本、提升用户体验。

做好互联网账户安全需要满足两个层面的诉求，我们可以推而广之把它放到社会或者公共安全上。一是安全效果，即安全度，它回答的是实际上是否安全的问题。二是安全感，即用户对安全的感知，它来自于用户体验层面。如果只有安全效果没有安全感知，那么没有人敢进行正常的交易活动。安全度要求我们满足三个核心的诉求，第一是提升防御能力、减少短板。黑客、盗用或者威胁都会找短板突破，一旦出现短板，其他部分做得再好都无济于事。第二是快速响应和灵活管控的能力。威胁越来越多来自于生态或者系统内生风险，快速、灵活的管控能使危险第一时间被堵住，从而降低风险造成的损失。第三是提升攻击成本、降低攻击损失。从经济学的角度，成本收益是一切经济活动的原动力，欺诈与盗用活动也是如此。只有在付出的成本小于收益时，人们才会有行动的动机。如同刑法对于犯罪的惩处在社会和公共安全中起到的作用，对于账户安全的威胁，我们要做的是减小犯罪的收益、增大惩罚的力度。

支付宝的安全体系是多层次的闭环的安全体系。我们把一个用户的正常业务过程按照不同的安全层次或者风险控制的场景进行多层次的控制，形成一个闭环的反馈体系。第一个层面是终端和系统的用户保护体系。用户在网站和手机上进行交易的时候，我们会通过一些端层面的控制保障环境安全。同时，我们在网站有一层系统安全的保护层，用于检测危险、解决外部的攻击和威胁。据不完全统计，支付宝网站每天可以检测到并保护的威胁超过几十万次，可见网络的生态已经是非常严重的问题。第二个层面是身份认证，即在账户登陆时识别、匹配用户的身份。我们通过认证和管理体系，利用大数据等技术手段来完成对用户的身份识别。第三个层面是风险识别。在风险识别过程中，支付宝会在后端帮助用户做操作和交易行为的风险识别与评估。对于那些比较敏感的业务操作，比如说输入密码，或者修改密码，或者包括支付，支付宝有一套风险识别和风险控制体系进行分析。

第四个层次是风险控制环节。一旦在识别过程中发现风险就会进入风险控制环节。支付宝会根据不同的风险程度，控制交易的额度、做出权限和交易灵活度的限制。

针对风险很高的交易，我们有一个核查和分析的环节。支付宝积累了非常多的公安分析案件的经验，能够根据大量的数据、场景和分析对用户进行核实。如果构成案件，我们会做出补偿并做深度的核查，找出潜在的风险；如果不构成案件，我们会作出反馈并不断地调整策略，避免打扰用户。最后，会员的损失风险由支付宝来承担，让用户无忧。

除了刚才的技术体系、风险的管控和账户安全的基础体系之外，我们还有一个机制上的保障——全流程的安全与风险控制体系。很多风险不仅仅来自于技术、密码的窃取，也不仅仅来自于用户不安全的习惯，同样来自于内部操作和运营上的风险。**通过研发、运营、监控、运维等环节中全流程、不同的安全策略和机制可以有效解决风险的问题。另外，支付宝也建立了一支蓝军团队，通过模拟盗用者的行为以及基于蓝军和红军的攻防互动来提高我们的安全能力。**

支付宝的风控体系发展了十年。到 2013 年，这套实时风控体系进入到第四个版本，因此，我们把目前正在使用的这个安全体系叫做第四代安全技术架构。

第四代安全技术架构主要解决的是面向未来的账户的技术安全能力。它具有以下特点：第一，采用大量云计算技术，不仅仅靠支付宝单点布防，也在生态层面布控。第二是海量的实时数据计算和服务能力。云计算能力是互联网上数据处理能力的一个典型表现，它使得在单一系统中难以完成的海量实时计算成为可行，并能够在更短的时间里发现和处理更多的复杂数据。第三是大数据驱动的个性化和自动化的风险管理与运营，用数据去做运营和预测。第四是尽早发现风险的征兆，快速识别、预警和布防。第五是充分利用移动互联网端的作用，强化端在风控体系中的识别和布控作用。第六是基于生物特征的认证。由于技术的进步，人的指纹、脸部、掌纹，甚至是签字、敲击键盘的习惯都可能进行分析，从而能够用来更好地保护我们的账户安全。最后，它能够有效整合业务安全、系统安全、应用安全、信息安全以及风险控制等多种能力，构建一个多层次的有机安全体系去保障账户的安全。经过不断的实践和改进，现在支付宝由于风险造成的损失率低于百万分之五，概率堪比赢得乐透大奖。

二、支付宝账户安全体系建设的思考

在支付宝安全体系建设过程中，我们也看到了一些问题、遇到了一些挑战，需要整个经济体系和行业共同面对。第一是不断恶化的网络安全生态给互联网账户安全造成的威胁。在别的网站被拖库以后，支付宝可能就要遭受威胁。虽然我们能够实时检测和捕捉这种行为，，但这种状况成为了行业共同的风险。第二是部分传统犯罪模式开始向网络转移。第一类情形是犯罪分子骗取用户的支付宝密码和短信交易码或者直接将用户账户里的资金骗到他的账户上，这类行为严重威胁到了账户安全。第二类情形是网络上出现的“黑社会”。例如，典型的“恶意差评师”是通过恶意差评敲诈勒索商户，其性质无异于“收保护费”。第三类情形是恶意抢拍。一些竞争对手或者别有用心的人，会把商户进行闪购的商品抢拍下来却不确认收货或者填写假地址，干扰商户的经营，以此来敲诈商户。第三是互联网模式下的分工协作使得网络犯罪门槛降低并催生黑色产业链。有这样一个案例，一对开手扶拖拉机的农村夫妇听说网上来钱快，就到论坛和社区买了一些打电话骗人的剧本和电话号码。他们每半个月换一个剧本，通过这样的诈骗每个月收入一万多，甚至超过了原来开拖拉机的收入。将近半年之后，他们由于诈骗被捕。原本是两个普通的开拖拉机的老百姓，由于从网上学到这些歪门邪道的门槛很低，才有了这样的悲剧。互联网模式下的产业链分工精细、效率很高。互联网在改变传统行业的同时也在改变黑色产业。第四是网络条件下的数字化犯罪和打击与取证采信越来越困难。网络犯罪的侦破成本很高，网络犯罪没有任何时间、地点、人的限制，并且它的门槛很低而警力有限。现在支付宝一天的交易超过七千万，即使是百万分之一的概率也会有几十个案件。虽然警方内部有自己的案件侦破机制，但是解决的毕竟是线下的问题。支付宝基于大数据有一整套的用户轨迹的记录，可以非常方便地进行犯罪分子作案轨迹的实时记录和取证。这一记录短的可以保持 14 天，长的可以根据央行的要求保持三年甚至更久。但是目前没有标准指明我们掌握的证据是否能被公安机关采信，这会让立案变得困难。第五是现有的法律体系下针对电子商务和创新型互联网金融企业的业务安全保护、犯罪打击和量刑缺乏标准。针对现在的互联网金融企业犯罪可能就是按照一般犯罪的标准量刑定罪，而不是针对金融企业的量刑定罪，无法达到有效震慑犯罪分子的目的。怎样提升犯罪成本，对犯罪进行严厉打击是需要思考的一个问题。

三、我们的建议

经过不断的努力，支付宝的被盗资金损失率目前已经低于百万分之五，移动支付的损失率甚至更低，相应的，这样的风险控制水平下对用户的打扰也非常低，小于千分之一。无可否认的是，由于光晕效率，个别案例给广大用户造成一定的担忧，这些负面声音，也在引发大众对于互联网账户安全的质疑。支付宝做过不少用户调研，虽然已经实施了很多

年的用户损失赔付保障，但仍然有一个有意思的回复是说，对于支付宝安全不太放心的主要原因在于“支付宝没有柜台，如果出现问题没有地方申诉”。可见中国的用户是缺乏安全感的、也不清楚如何合法合理获得安全保障。不管是传统金融还是互联网金融，我认为整个产业对用户的保障还不够，以至于用户仍有安全方面的顾虑。支付宝对互联网的资金损失做全额赔付，但是这还没有形成行业标准。这一做法应该慢慢成为行业标准，让中国的老百姓和消费者在互联网的账户使用中有安全感，这是我们要继续努力的方向。