《银行卡法律风险管理》课程培训大纲

前言：

随着银行卡业务的迅速扩张和竞争的日趋激烈，全国各地有关银行卡方面的投诉、纠纷、案件频发，银行卡业务风险处于多发、高发期。为此，银监会对当前银行卡业务风险进行了专门调查分析，并提出了相应的防范建议。银监会先后发布了授信尽职、外部营销、银行卡安全管理等一系列规范性文件和风险提示，各银行机构应查漏补缺，进一步建立健全内控机制，根据银行卡种的属性、业务种类及其风险特点制定相应的业务规章制度和操作程序。银行卡发卡银行应从各类风险事件中吸取教训，建立有效的内部监督机制，确保内控制度的落实，把银行卡业务的审计工作纳入到银行内部审计工作的整体计划中，结合案件专项治理工作，建立合规风险管理的长效机制。

授课大纲

一、基础知识

1. 银行卡风险的定义

经营或参与银行卡业务的机构在银行卡业务运营的过程中，以及单位和个人在申领、持有和使用银行卡的过程中发生损失的不确定性。

2. 银行卡风险类型

按照银行卡风险表现形式可划分为信用风险、欺诈风险、操作风险和合规风险等四类。

3. 银行卡产业链各参与主体面临的风险

在银行卡业务中，持卡人、发卡机构、特约商户、收单机构、银行卡转接清算机构及第三方专业化服务机构等业务参与主体，共同构成了银行卡的生态产业链。同时，因为角色和职能的不同，各参与主体在

银行卡业务开展过程中面临和承担的风险及责任也不同。

4. 银行卡风险管理的几种主要策略

五种主要策略:1、风险承担。2、风险预防。3、风险分散。4、风险规避。5、风险转移。

5. 银行卡业务参与主体的风险管理流程

大多包括以下四个步骤：一是结合银行卡业务的整体发展战略制定明确的风险管理政策和目标。二是对风险进行识别、评估和衡量。三是制订并实施管理风险的策略和方法。四是对风险管理的评价和反馈。

二、发卡信用风险及防范

信用风险是信用卡发卡机构面临的最主要的风险，由此导致的坏帐损失不仅会直接降低银行利润，而且会使监管机关对信用卡发卡机构提出更高的资本准备金要求，进一步提高发卡机构的经营成本。强大的信用风险管理能力是信用卡发卡机构的核心竞争力之一。

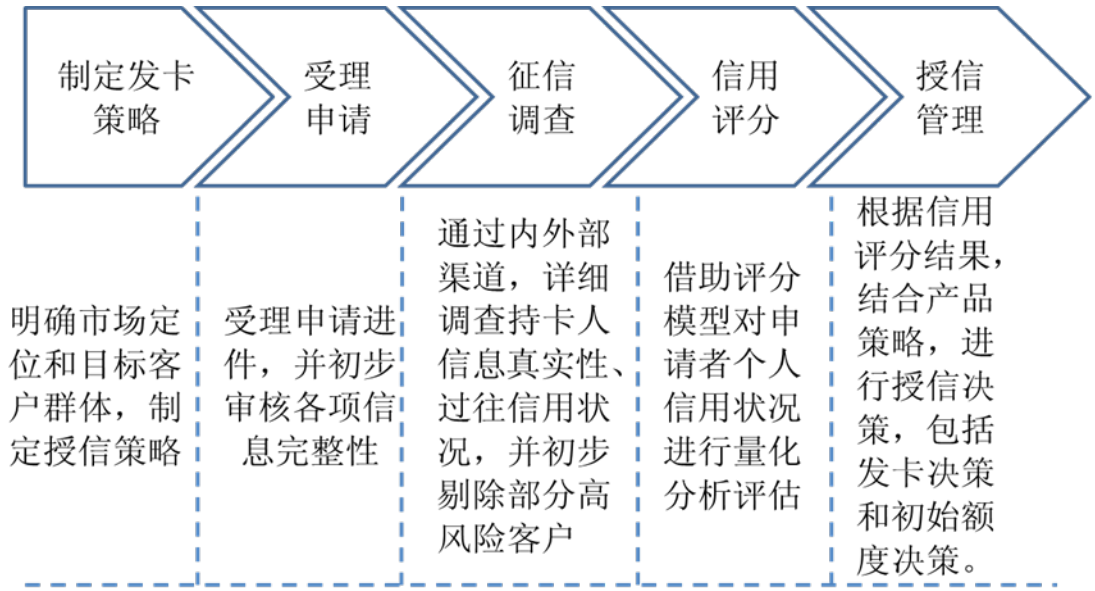
1. 发卡机构信用风险管理

信用风险管理贯穿于信用卡业务生命周期各个环节，建立完整的信用卡信用风险管理体系，并借助量化分析技术和手段，实现精细化和自动化的信用风险管理，以提高风险决策效率，降低管理成本。

6. 信用风险管理主要内容

信用卡信用风险管理工作贯穿于信用卡业务的生命周期，包括信用卡审批管理、贷后额度调整和交易授权管理、催收与呆坏账管理、信用数据分析等方面。

1） 信用卡审批基本流程



2） 贷后额度调整和交易授权管理

一是对授信额度的动态调整和管理；二是针对日常交易的授权管理，特别是对于拖欠账户的交易授权管理。

3） 催收管理

发卡机构的核心竞争力之一，代表了发卡机构控制最终风险损失的能力。催收能力强的发卡机构可以拓展风险相对较高的客户群体，从而获取更多的利息和手续费收益。

三、发卡欺诈风险管理

银行卡欺诈风险是指不法分子通过各种欺诈手法窃取持卡人卡内资金或信用额度而导致的风险。

1. 发卡欺诈类型

一个完整的银行卡生命周期包括了卡片申请、卡片发行、卡片日常管理、卡片挂失/到期处理等基本阶段，都有可能发生银行卡欺诈。根据欺诈发生的不同阶段，可初步划分银行卡发卡欺诈风险的类型：卡片申请环节----虚假申请；卡片发行环节----未达卡欺诈；卡片日常管理环节----失窃卡、伪卡、非面对面欺诈等类型；卡片挂失环节----账户盗用欺诈。

7. 信用卡主要欺诈类型及风险防范

1） 虚假申请欺诈防范

审批环节、交易监控环节、催收环节采用相应的防范措施和监控措施。

4） 伪卡欺诈防范

1、添加卡片校验码（CVN）、2、增加其他交易验证要素、3、 加强交易监控

5） 未达卡欺诈防范

1、加强卡片寄送环节安全管理。2、 加强卡片激活环节身份验证。3、 加强交易监控。

6） 失窃卡欺诈防范

1、为卡片设置交易密码。2、及时止付，控制欺诈损失扩大。3、加强交易监控。4、提升持卡人安全用卡意识，及时关注账户交易变化情况。

7） 账户盗用欺诈防范

1、加强持卡人更新信息环节风险防控。2、加强换发/补发卡环节风险防控。3、加强交易监控。4、提请持卡人密切关注卡片及账户交易变动情况。

8） 非面对面欺诈防范

1、加强业务开通身份审核。2、加强业务定制风险防控。3、提高交易验证强度。4、加强交易限额管理。5、加强交易监控。6、加强持卡人个人身份信息管理。7、加强持卡

人宣传教育。

8. 借记卡主要欺诈类型及风险防范

目前国内借记卡欺诈主要表现为欺诈转账，损失金额在借记卡欺诈总损失金额中的占比超过 80％；其次是伪卡欺诈，特别是境外的大额伪卡欺诈案件也是近年国内借记卡欺诈的突出风险类型之一。

1） 电信欺诈转账防范

1、加强个人银行开户及开通业务功能环节的风险防控

2、加大对银行柜面转账交易的风险核查力度

3、做好客户身份资料及交易记录保管工作

4、加强可疑交易监控

5、加强持卡人宣传教育

9） 借记卡境外欺诈风险防范

1、加强借记卡境外交易授权管理

2、建立大额交易监控机制

3、建立借记卡交易限额管理机制

4、建立 7×24 小时应急处理机制

四、收单风险管理

银行卡收单（简称“收单业务”）是银行卡交易体系运作的重要环节，主要包括 POS 收单和 ATM 收单两大类,随着技术的发展,越来越多的创新业务收单也被用户应用.

1. POS 收单业务风险及防范

1） 有哪些风险类型？

1. 商户信用风险
2. 商户虚假申请
3. 商户套现
4. 终端违规移机

5. 合谋伪冒交易

6. 侧录（盗取账户信息）

7. 商户违规受理

8. 复制（伪冒）POS 终端

9. 欺诈性联机退货

10） POS 收单业务防范

收单机构应建立起覆盖收单业务事前、事中、事后的全流程风险管理体系，在商户拓展、商户审核、商户签约、商户日常管理、交易监控、机具管理、案例调查处置等收单业务各环节建立起体系完备、措施有力的风险管理制度。同时收单机构应通过不断完善收单风险监控系统、加强人员培训、严格制度落实等手段实现收单风险的全流程管理。

9. ATM 收单业务主要风险点及防范

风险类别	风险点
现金安全	改装出钞口盗取现金 假币置换 加钞过程安全风险
银行卡安全	假读卡器/假门禁侧录磁道信息 设置钓钩/假卡调包盗卡
持卡人安全	取现后盗窃或抢劫 围观诈骗
交易信息和密码安全	密码被窥视或偷摄 假键盘记录密码 凭条信息泄漏
ATM 物理安全	盗取整机/假 ATM 非法改装和破坏安全装置 张贴欺诈性告示
ATM 软件系统安全	篡改 ATM 后台程序， 利用 ATM 键盘侵入主机程序等

ATM 安全的范围涉及到现金安全、银行卡安全、持卡人安全、交易信息和密码安全、ATM 物理安全、ATM 软件系统安全六大方面，更多创新技术和安全解决方案正处于从研发到投入使用的各个阶段。收单机构应从硬件配置、软件开发、人员培训等各方面加大投入，加强对常见欺诈类型的防范。

10.互联网支付特点及风险防范

1）互联网支付风险点：交易双方身份不确定性所导致的持卡人被伪冒交易

2）对于互联网欺诈的防范，可以从以下方面进行：

1.加强商户和成员机构侧敏感信息管理

2.完善商户和成员机构侧风险监控机制

3.同样注意要加强持卡人安全教育

11.移动支付风险防范

1） 发卡类产品主要风险：

1、虚假申请（以他人身份信息申请并下载他人金融应用）

2、伪卡风险（移动支付发卡产品比较传统磁条卡，被侧录的风险较小，因此伪卡风险目前极小）

11） 收单类产品主要风险：

1、账户盗用（常见于收单类的无卡模式，因为不需要卡片出现，只要窃取了卡片信息，骗取了持卡人的短信动态码，即可实现盗刷）

2、账户信息泄漏（客户端输入 PIN/有效期/cvn2 等，可能存在被第三方截获的风险）

3、侧录磁条卡（通过类 square 产品窃取磁条卡信息）

4、钓鱼网站（和传统 PC 的线上支付一样，通过手机上网支付可能发生钓鱼网站的风险）

12） 风险防范建议：

发卡侧：

发卡机构应对移动支付的交易进行有效识别，并设置相应的监控措施（限额管理、频率管理、异常监控等）；

开展有卡模式的发卡机构，对持卡人空中下载金融账户的模式，应设置完备的身份审核和管理制度，并对金融应用申请下载、锁定解锁、注销各环节的全生命周期进行风险防控。银联已制定发布了相应的智能卡

产品风险防范指引，可供发卡机构参考；

同时发卡机构应开展对持卡人的教育，做好安全交易宣传。

收单侧：

收单机构应谨慎发展移动支付商户，特别是涉及虚拟物品的商户，需设置严格的准入制度和监控措施（包括但不限于限度管理、频率管理、异常监控等）；

联合商户建立货物拦截机制，对发生欺诈交易的货物实时拦截，挽回损失。

做好账户信息安全工作（可参照银联《银联卡收单机构账户信息安全管理标准》）；

对个人支付的类 square 产品应建立实名登记制度，并限制每个终端能绑定的卡片数量，避免持卡人将个人支付终端用于商户终端。

持卡人：

提高警惕和账户信息安全保密的意识，不泄露账户信息，包括短信动态码；

避免打开不信任的网页和客户端，不在不安全的页面输入账户信息；

出现欺诈事件及时向发卡行和警方反应，及时挂失卡片，避免损失进一步扩大。

五、转接清算风险

1. 银行卡转接清算机构主要面临国家风险、清算风险、系统操作风险、项目风险，品牌风险、合规风险、国际汇率风险。

1. 清算机构的风险管理

对成员机构的信用风险管理, 对成员机构的清算风险管理

六、账户信息安全管理

1. 管理内容

在传统的面对面交易过程中，卡片有效期、银行卡磁条信息、卡片验证码、交易密码（PIN）是账户信息安全管理的核心内容，而随着银行卡互联网支付、电话支付、移动支付等创新业务的快速发展，非面对面业务中与银行卡交易相关的用户身份验证信息，如用户注册名、密码、真实姓名、证件号码、联系方式等，也逐步成为账户信息安全管理的重要组成内容。

12.账户信息安全管理的重点内容

（1） 建立账户信息安全管理制度体系

（2） 人员及组织管理

（3） 访问控制

（4） 账户信息生命周期安全管理

（5） 系统安全管理

（6） 账户信息风险事件应急处理

（7） 账户信息风险安全合规评估

七、银行卡反洗钱

1. 一般犯罪分子利用银行卡洗钱可以分为三个阶段：

（1）资金放置阶段。

（2）资金转移阶段。

（3）资金归集阶段。

13.银行卡洗钱的主要手段

（1）利用银行存款的资金转移进行洗钱。

（2）利用虚假资料进行信用卡欺诈的洗钱风险

14.商业银行的反洗钱工作

作为银行卡业务的主体，须在客户身份识别、大额和可疑交易报告、客户身份资料和交易记录保存等

三个方面合规开展反洗钱工作。

15.银行卡转接清算机构的反洗钱工作

对于成员机构或其指定代理机构未能遵守反洗钱的要求，银行卡转接清算机构可根据当地法律对会员或指定代理机构施加条件或要求其采取补充措施，这些措施一般包括：

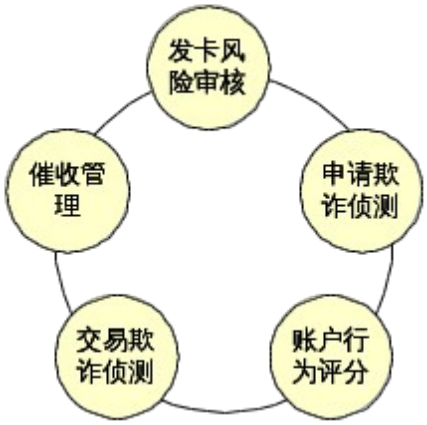
- 实施补充的政策、程序或控制措施
- 终止商户或持卡人协议
- 终止代理机构协议
- 终止成员资格
- 罚款或给予处罚

八、银行卡风险服务与安全技术

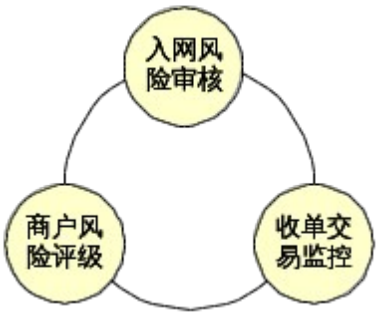
1. 银行卡风险管理系统

发卡业务风险系统往往由多个不同的风险子系统或风险模块组成

发卡业务风险系统构成



收单业务风险系统构成



16.银行卡风险管理技术

包括卡片防伪技术、身份验证技术、银行卡信息加密技术、终端安全技术、欺诈侦测技术、信用评分技术等。