金融信贷个人信息泄漏风险评估与防范策略研究

徐金梅
泰国格乐大学

摘　要：随着金融信贷业务的发展，个人信贷信息的泄漏风险逐渐凸显。金融信贷业务本身就涉及大量的个人敏感信息，如个人身份证号码、银行卡账号、信用记录等。这些个人信息一旦被泄漏，可能导致个人面临诈骗、资金损失等风险，不仅给个人造成损失，也对金融机构的声誉和信誉造成负面影响。于是本文对金融信贷个人信息泄漏风险进行研究，首先通过对金融信贷个人信息泄漏风险的后果进行介绍，分析该风险对金融业和个人的影响。其次探讨金融信贷个人信息泄漏风险评估的方法，最后提出金融信贷个人信息泄漏风险的防范策略。以帮助金融机构和个人有效应对个人信息泄漏风险。

关键词：金融信贷；个人信息泄漏；风险评估；防范策略
【DOI】10.12252/j.issn.2096-6288.2022.11.111

引言

随着互联网和信息技术的快速发展，金融信贷领域的个人信息泄漏风险日益增加。金融信贷涉及大量个人敏感信息，如身份证号码、银行账号、财产状况等，一旦这些信息泄漏，个人将面临诈骗、盗窃身份和财产损失等风险。个人信息泄漏风险的背后是多种因素导致的，首先，金融信贷行业的信息安全意识和技术水平相对较低，容易遭受黑客攻击和数据泄漏。其次，个人信息的获取和交换变得更加便捷，为不法分子提供了更多的机会来获取和滥用个人信息。此外，一些金融机构在数据管理和保护方面存在缺陷，导致个人信息易于被窃取。为了有效应对这一风险，需要对泄漏风险进行评估，并制定相应的防范策略。通过深入研究和分析，可以为金融信贷行业提供科学、可行的防范措施。

一、金融信贷个人信息泄漏的后果

（一）财务损失

金融信贷个人信息包含了个人身份证号码、姓名、银行账户等敏感信息，如果这些信息泄漏给恶意的第三方，他们可能会利用这些信息进行各种欺诈行为，比如盗取个人银行账户资金，申请贷款或信用卡等，进而导致个人遭受财务损失。

（二）信用危机

泄漏个人信贷信息后，信息被不法分子用于违法犯罪活动，导致相关金融机构在与个人贷款、信用卡等相关业务中进行风险评估时，可能会将个人列为高风险客户，这将对个人的信用记录造成负面影响，进而影响个人获取信贷的能力，甚至可能导致信用被严重破坏，难以再次获得金融服务。

（三）个人隐私泄漏

个人信贷信息的泄漏将涉及个人的隐私权问题。当个人的敏感信息被泄漏后，不仅会导致金融欺诈等问题，还可能导致个人的名誉受损，甚至受到进一步的骚扰、邮件诈骗、电话骚扰等。个人的隐私泄漏将严重侵害个人权益，增加了身份盗窃、网络攻击等风险。

尽管金融机构在保护个人信息方面采取了一定的措施，但由于技术手段的进步和恶意攻击的不断演进，保护个人信贷信息已成为金融机构亟待解决的重要问题。不仅金融机构应加强信息安全管理，个人也应增强自身的信息安全意识，避免随意泄漏个人敏感信息，确保自身的财产安全和个人隐私权的保护。

二、个人信息泄漏风险评估的方法

（一）数据收集与预处理

首先需要收集和获取与个人信息相关的数据，包括个人身份信息、交易记录、网络行为等。然后对数据进行预处理，包括数据清洗、去除噪声、数据统一化等，以保证数据的质量和一致性。

（二）特征选择与提取

在数据分析过程中，需要根据个人信息泄漏的特点和发生的背景，选择合适的特征进行分析。这些特征可以是个人信息的属性、与个人信息相关的其他数据，以及与个人信息泄漏事件相关的因素等。然后通过一定的特征提取方法，将原始数据转化为可以用于建模的特征。

（三）模型选择与建立

根据个人信息泄漏风险评估的要求，选择合适的模型进行建立。常用的模型包括逻辑回归、决策树、支持

向量机等。根据实际情况，可以单独使用一个模型，也可以结合多个模型进行综合评估。

（四）模型训练与验证

在建立好模型后，需要使用已有的数据进行模型训练，以使模型能够具备一定的泛化能力。然后使用独立的测试数据集对模型进行验证和评估。通过比较模型的预测结果和实际结果，可以评估模型的准确性和可靠性。

（五）模型调优与验证

在模型训练和验证过程中，可能会出现模型欠拟合或过拟合的问题。需要通过调整模型的参数、增加或减少特征等方式来改进模型的性能。同时还需要使用更多的测试数据对模型进行验证，以保证模型的稳定性和可靠性。

（六）风险评估与结果解释

模型训练和调优完成后，可以使用该模型对新的个人信息数据进行风险评估。通过模型输出的结果，可以评估个人信息泄漏的风险程度，并对风险结果进行解释和解读。可以根据不同的风险等级，采取相应的风险管理措施，保护个人信息的安全。

在实际应用中，还可以借助一些数据分析和建模的工具来辅助进行个人信息泄漏风险评估。例如，使用Python编程语言中的数据分析库可以快速进行数据处理和建模；使用可视化工具可以直观地展示数据特征和模型结果；同时也可以使用数据挖掘和机器学习平台来快速构建和验证模型。这些工具可以提高个人信息泄漏风险评估的效率和准确度。

三、金融信贷个人信息泄漏风险防范策略

（一）建立全周期的个人信息风险评估模式

我国《个人信息保护法》仅对其适用条件和评估进行了简单的规定，但在具体操作中还需要细化。建立个人信息风险评估机制，既要在法律上将其确立为一种基本的民法义务，也要对其进行完善，并将其应用于信息处理行为的整个过程，从而形成一种较为系统、科学的个人信息风险评估模型，这也正是防范个人信息泄漏风险的重要手段。

借鉴《民法典》1035条对个人信息处理过程的有关规定，构建了一套完整的个人信息风险评估模型：第一，个人信息的收集、存储环节：金融机构应当明确个人信息收集的目的，并且仅限于完成特定金融信贷业务所需要的信息。在收集个人信息时，应当明确告知被收集者个人信息的使用目的、使用范围以及可能涉及的风险，获得其明示同意。第二，个人信息的处理、加工环节：金融机构在处理个人信息时应遵守信息收集的合法目的和范围，保证个人信息的合法性、正当性和必要性。不得超出合理范围处理个人信息，不得未经授权使用个人信息。对于敏感个人信息，金融机构应加强保护措施，严格限制和监管敏感个人信息的处理。例如采取数据脱敏、加密等技术手段，确保敏感信息的安全性。第三，个人信息处理结果公开环节：金融机构在进行个人信息公开时，应明确公开的范围和目的，并与被公开信息的个人进行充分告知和取得明示同意。公开的个人信息应保证准确性和完整性，避免对个人权益造成不必要的损害。金融机构应建立健全的个人信息申诉和回应机制，对公众提出的个人信息保护问题和建议及时回应和解决。及时处理申诉和建议，维护公众的合法权益。

通过全周期的个人信息风险评估模式，金融机构可以针对个人信息的收集、存储、处理、加工和公开等环节进行综合评估和管理，确保个人信息的安全和合规处理，最大限度地减少个人信息泄漏的风险。

（二）建立对行业个人信息保护的统一标准

首先，金融机构应与相关部门、行业协会等共同制定和推广针对个人信息保护的统一标准，明确个人信息的分类、处理、存储和共享等规范。这些标准应包括对个人信息的采集、使用和保护的规定，同时涵盖技术、管理、人员和法律等方面的要求。其次，金融机构可以向行业内其他机构推广和分享个人信息保护的最佳实践，通过行业内的交流和合作，共同增强个人信息保护意识和水平。金融机构可以举办研讨会、培训班等活动，邀请相关专家和行业领导者分享成功的个人信息保护案例，借鉴和推广先进的个人信息保护经验。第三，金融机构可以主动引入第三方机构进行信息安全评估和认证，以验证其个人信息保护措施的有效性和合规性。第三方机构的认证可以增加金融机构在个人信息保护方面的可信度，提高客户对其信息安全措施的信任。最后，金融机构应积极与监管部门和执法机构合作，在个人信息保护方面共同开展监督和执法工作。金融机构可以配合监管部门对其个人信息保护情况进行审查和监测，及时纠正存在的问题，并配合执法机构对个人信息泄漏等违法行为进行调查和处理。

通过建立与推广行业标准，金融机构能够在个人信息保护方面达到更高的统一标准并遵循合规要求。推广行业最佳实践和引入第三方认证机制可以促进行业内的信息安全水平提升。与监管部门和执法机构的合作能够及时发现和应对个人信息泄漏风险，并增强监管的有效性。

（三）加强金融机构的内部控制与权限管理

金融机构处理大量客户的敏感个人信息，如身份证号码、银行账号等。加强内部控制和权限管理可以确保员工只能访问和操作其工作职责所需的信息，减少误操作或滥用权限的风险，保护客户个人信息的安全性。

首先，实施严格的权限管理制度：金融机构应设定不同层级的权限，确保员工只能访问其工作职责所必需的信息，并限制其对敏感个人信息的访问与操作。例如，高级员工可能拥有更高级别和更多范围的权限，而低级员工只能访问有限的信息。其次，加强内部控制措施：金融机构应建立健全的内部控制机制，包括内部审计和风险控制等环节。例如，定期对员工进行信息安全培训，强调个人信息的保密性和责任，定期检查员工操作记录，及时发现异常操作和风险。第三，强化数据访问和使用的监控：金融机构应建立数据访问和使用的监控系统，记录员工对个人信息的访问和使用情况。例如，通过日志记录系统，实时监控员工对个人信息的操作，检测和报告任何异常访问行为，及时采取措施防止信息泄漏。最后，限制外部接入权限：金融机构应设立防火墙和其他安全措施，限制外部人员对内部系统的接入权限，防止未经授权的人员获取敏感信息。例如，只允许授权的人员通过VPN等安全通道远程接入系统，同时使用加密和多重认证等方式确保接入安全。

这些措施可以确保员工只能访问到其需要的信息，减少个人信息受到非法获取的可能性。同时，对员工进行培训和监控，可以增强员工的信息安全意识，及时发现和阻止异常操作。对外部人员的接入进行限制，可以保障个人信息的安全。

（四）加强金融机构的信息技术与风险监测

金融机构应加强其信息技术和风险监测能力，以更好地防范个人信息泄漏风险。首先，金融机构应投入足够资源来建立先进的信息技术基础设施，包括网络、服务器、数据库等，以确保其能够安全地存储和处理客户的个人信息。此外，应保持这些系统的更新和维护，确保其安全性和稳定性。其次，金融机构应采取一系列的数据安全措施，如加密数据传输、数据备份、访问控制等，以防止个人信息在传输和存储过程中被泄漏或篡改。此外，金融机构还应定期进行漏洞扫描和安全审计，及时发现并修复系统的漏洞。第三，金融机构需要建立健全的网络安全体系，包括入侵检测和防火墙等技术手段，以防止黑客攻击和未经授权的访问。此外，金融机构还应严格控制对公司网络和系统的访问权限，并采取多重认证机制，确保只有授权的人员才能访问敏感信息。最后，金融机构应建立有效的风险监测和预警机制，对系统和数据进行实时监控，及时发现异常活动和潜在的安全风险。还可以借助数据分析和人工智能等技术手段，对大量的交易和数据进行监测和分析，以发现可能存在的信息泄漏风险。此外，金融机构应定期对员工进行信息安全培训，增强他们的信息安全意识和技能，教育他们如何正确处理和保护客户的个人信息。此外，金融机构还应建立严格的员工行为准则，明确规定员工在处理个人信息时的责任和义务。

总之，建立强大的信息技术基础设施和数据安全措施，加强网络安全防范，建立风险监测和预警机制，加强员工培训和信息安全意识教育都能有效地保护客户的个人信息安全。

四、结论

本文主要研究了金融信贷个人信息泄漏的风险评估与防范策略，先是详细介绍了金融信贷个人信息泄漏的后果和个人信息泄漏风险评估的方法。为了能够防范金融信贷个人信息泄漏，提出了几项防范策略，包括建立全周期的个人信息风险评估模式、建立统一的行业个人信息保护标准、加强金融机构的内部控制与权限管理以及加强信息技术与风险监测。通过本文的研究，可以有效评估个人信息泄漏的风险并采取相应的防范措施，以保护个人隐私和减少潜在的损失。

参考文献

[1]颜瑜.因个人信息泄漏导致的信用卡欺诈风险的防控实践[J].中国信用卡，2023，（04）：47-49.

[2]李逸飞.论法律视角下公民个人信息泄漏的危害与防控[J].法制与社会，2020，（06）：11-12.

[3]陈丽慧，高妍，刘演强，崔宇华，邰凤珍.个人信息泄漏的事前防范研究——以监管和行业自律为切入点[J].法制与社会，2018，（16）：165-168.