个人金融信息风险民事责任的实现

许娟 黎浩田[1]

【摘 要】:《中华人民共和国个人信息保护法》构建起来的个人信息处理者义务性规范为侵权责任的实现提供了更为全面的法律保障。但就金融企业这类个人信息处理者而言，现有个人信息保护的民事责任体系仍然难以实现个人金融信息损害赔偿的救济，需要引入风险民事责任，进一步完善现有民事责任体系。一方面，可以在《个人信息保护法》适用中做出解释：将金融企业市场特许经营许可设定为消费者格式合同的效力要件，将金融企业监管义务延伸至个人金融信息的民事责任认定之中。另一方面，可以对《个人信息保护法》进行创新性的研究：在丰富具体人格权权利内容的基础上，增加金融消费者人格要素的赋权规范；明确金融企业行业管理的禁止性规则，课以金融企业个人金融信息安全管理义务和信息风险评估义务；在通知公义务中构建默认付费或默认罚款等财产权保护模式。

【关键词】: 个人金融信息 风险民事责任 金融企业

随着数据利用行为所隐含的技术风险增长，包含个人信息的金融信息在技术迭代中被侵犯的事件也屡屡出现。2021 年 9 月 2 日，时任中国建设银行余姚城建支行行长的沈某在工作中侵犯金融消费者个人信息受到行政处罚一案[1]，引起社会各界对金融消费者个人信息安全的热切关注。早在 2020 年 5 月 8 日，中信银行发布了因泄露个人金融信息致王越池的道歉信[2]，随后该行又被曝在 2018 年就因“未经同意查询个人或企业信贷信息”遭受行政处罚；2018 年支付宝“年度账单”[3]事件曝光。此类事件中的金融消费者在维护金融信息权益时，面临信息不对称致使同意有效性降低等诸多问题，金融消费者在默示状态下的同意逐渐成为金融信息控制者的免责条款。长期以来，金融企业作为信息持有者，事先制定收集信息的协议，形成默示同意的客观事实，并凭借数据持有优势运用算法技术发掘潜在消费者。而默示同意范围不明、金融信息二次利用缺乏消费者同意以及金融企业共享信息不当等问题都潜藏着损害个人金融信息的风险。《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）第 28 条将“金融账户”等重要信息归类为敏感个人信息加以保护，推动个人信息保护迈入新阶段，也给个人金融信息保护的司法实践提供了新的视角。本文在个人信息权益保护的基础上，嵌入风险民事责任，尝试在金融消费者与金融企业利益平衡的基础上探寻个人金融信息保护的有效路径。

一、个人金融信息民事责任体系：基于现行法的检视

个人金融信息是为信息主体提供金融产品或者服务所必需的个人信息[4]。现行法对个人金融信息损害的风险规制一般采取原则性的规定，仅设置笼统的保密义务，未明确界定金融信息的保护边界。在法律、法规和规章对金融消费者信息保护缺位的同时，下位的金融领域规范性文件对各类损害个人金融信息情形的民事责任追究也并不完备，这在规范层面形成了个人金融信息保护的结构性困境。

1.法律法规和规章对民事责任的规定并不完备

在金融企业信息侵权事件中缺乏对个人金融信息的有效保护，是因为该领域的基础性法律——《个人信息保护法》及其他相

[1]**作者简介**：许娟，南京信息工程大学法政学院教授、大数据法治研究院院长
黎浩田，南京信息工程大学大数据法治研究院研究员
基金项目：国家社会科学基金项目“个人信息权利行使的平衡机制研究”（19BFX127）阶段性成果

关法律法规并未提供足够的确定性，其中的授权性或原则性条款使适用缺乏可操作性，导致法律的实践价值大打折扣。

（1）相关条文涵射中的敏感信息重叠难题

《中华人民共和国民法典》（以下简称《民法典》）第 111 条规定“自然人的个人信息受法律保护”，确立了金融企业“依法取得”和“确保信息安全”的宏观义务，并以“不得非法买卖、提供和公开个人信息”等规定限制金融企业对金融信息的处理行为。《民法典》第 111 条对信息保护的规定较为模糊，未进一步明确界分“个人信息”与“金融信息”这类敏感信息。《民法典》第 1033 条本质上是对信息的分类，列举了信息权侵权行为，却未对金融等特定领域作出规定。《民法典》第 1034 条再次强调个人信息受法律保护，并列举了个人信息的类型，其中许多属于金融活动过程中必定涉及的信息。根据该条，个人的私密信息适用有关信息权的规定，没有规定的可以适用有关个人信息保护的规定。2021 年 8 月 20 日全国人大常委会公布《个人信息保护法》，其中第 28 条将敏感个人信息定义为“容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息”，该定义涵盖了“金融账户”，确立了“特定目的”、“充分必要性”和“采取严格保护措施”为基准的敏感个人信息处理三要件，但仍需通过司法解释进一步明确什么是金融信息以及信息保护的法律路径。就《民法典》第 1034 条和《个人信息保护法》第 28 条而言，“私密”信息与“敏感”信息的范围有所重叠，在金融信息案件的法条适用中难免陷入二选一的困境。

（2）相关条文空缺情形下的信息自决短板

《民法典》第 127 条设置了参照其他相关法律规定的接口，第 1030 条也同样设置了适用其他法律、行政法规规定的接口，但是目前的相关法律、行政法规体系尚未健全到能够与其对接的地步。《商业银行法》《储蓄银行管理法》《反洗钱法》《银行业监督管理法》《消费者权益保护法》等有关金融信息的法律虽然都有对银行客户金融信息权保护的相关规定，但是这些规定却也存在着对金融信息保护的具体化不足及目标性不明确等问题，难以对金融消费者信息提供严密的保护。譬如现行《商业银行法》第 29 条规定了商业银行为存款人保密的原则，《证券法》第 38 条也规定了证券交易所、证券公司和证券登记结算机构对于客户账户的保密义务。但在金融交易中双方的交易信息一直存在不对等的状态，即在交易过程中一方拥有某种资料信息，而另外一方不拥有对等的相关资料信息[5]。因此，这些法规的有效性因为消费者和金融企业之间知识和权力的巨大的不对称而被消解。金融消费者做出知情的理性决策的实际能力远未达到《民法典》和《个人信息保护法》所预设的程度。《民法典》第 135 条[6]对民事行为形式相关规定承认默示形式，第 140 条[7]蕴含默示同意要素并构建了“法律规定”、“当事人约定”或“交易习惯”三种类型。现行部门法大都也只提到了同意制度并以明示同意作为重点，如《消费者权益保护法》关于“明示”“同意”的规定[8]；《网络安全法》则要求“明示并取得同意”[9]。《消费者权益保护法》第 29 条[10]规定经营者应采取措施保护消费者个人信息安全。从《消费者权益保护法》和《网络安全法》都规定的基于同意规则的信息保护模型来看，以“同意”作为核心的信息保护模式不注重强调“默示”与“明示”的明确区分，未能意识到默示条款的价值与重要性，在个人金融信息保护这一特殊领域容易造成风险扩散的严重后果。如《网络安全法》要求网络经营者在用户同意的基础上承担起维护用户个人信息不受侵犯的义务，但互联网金融消费者在签订电子合同时，“授权同意”的格式条款会成为网络经营者免责的依据。2019 年 12 月，国家计算机病毒应急处理中心通报多家银行手机 APP 存在“未向用户明示申请的全部隐私权限，涉嫌隐私信息不合规”的问题，这些问题往往被技术中立的外衣掩盖，甚至被算法等操作系统黑箱化。个人金融信息处理行为本质上具有智能科技活动的性质，必须约束金融企业凭借技术外力形成的任性，精确保护个人金融信息。而界分两类同意的条款空缺正使金融消费者日益丧失对个人信息的自主控制权，因此，对个人金融信息的保护还需对如何定义有效同意、获取同意的方式等予以明确。

3.相关条文无法应对司法实践的保护需求

基于《个人信息保护法》第 14 条，金融消费者同意处理个人金融信息的，该同意应当由个人在充分知情的前提下自愿、明确做出，并且法律、行政法规对取得单独同意或者书面同意另有规定的应遵从其规定。同时，《民法典》第 1038 条设置了信息处理者两个“不得”的禁止性条款，但现实生活以其复杂性消解了该条的理想化设定，一系列具有隐蔽性强、成功率高、作案时间长、涉案金额大等特点的金融大案背后都或多或少涉及对个人金融信息的侵害。当消费者因个人信息被侵犯提起诉讼请求时，还

往往面临财产损失计算无法可依的困境。例如游某诉徽商银行成都金牛支行案中，金融消费者基于对银行的信任而概括函授同意，提供了 U 盾和个人信息，支行行长伙同其他银行工作人员将其金融账户与其他客户的账号信息进行混淆造成理财回款的假象，蒙蔽游某继续在徽商银行储蓄、理财，最终使其遭到巨额资金损失，但其财产损失难以得到有效赔偿[11]。

2.规范性文件对民事责任的保护对象规定不一致

当新兴技术面世而法律缺位时，具有更强灵活性的规范性文件在调整失衡的法律关系中就会起到重要作用。作为个人信息的子概念[12]，个人金融信息范围的界定并不清晰，仅中国人民银行制定过的《人民币银行结算账户管理办法》《关于银行业金融机构做好个人金融信息保护工作的通知》《非银行支付机构网络支付业务管理办法》《金融控股公司监督管理试行办法》《金融消费者权益保护实施办法》《个人金融信息保护技术规范》等数部规范性文件，就使用过“银行结算账户信息”“客户信息”“敏感信息”“个人金融信息”“消费者金融信息”等名称，涵盖个人身份、财产、账户、信用、金融交易、借贷以及衍生信息等多个概念。同时，上述规范性文件与银保监会制定的《银行业金融机构数据治理指引》，国家市场监督管理总局、国家标准化管理委员会发布的《信息安全技术个人信息安全规范》中对金融信息保护对象的规定也不一致。即使这些规范性文件规定了金融企业的保密义务，但就如最新的《金融消费者权益保护实施办法》（2020 年版）新增了“金融消费者权利”，虽然一定程度上填补了个人金融信息保护的制度空缺，但对金融企业的民事责任规定仍不完善。

同样的情况还存在于国务院发布的规范性文件中，如《个人存款账户实名制规定》第 9 条所规定的保密义务的对象为存款人，却不包括金融交易中其他金融主体如贷款人、保证人等。在个人金融信息保护方面，立法的滞后直接致使金融企业获取客户个人金融信息被肆意侵犯，损害金融消费者的合法权益。即使国务院发布的《关于加强金融消费者权益保护工作的指导意见》将消费者个人信息的法律保护设定为金融消费者的信息安全权，但并未超越现行金融立法有关金融企业保密义务的规则要求，这些位阶较低的办法、通知等规范性文件虽明确了保密义务的范围和个人金融信息的范围，却因其自身效力在实践中不具有强制力，仍无法起到有效的保护作用。

二、从传统民事责任到风险民事责任：化解风险的新方案

《个人信息保护法》构建了以“告知—同意”为核心的个人信息处理规则，保障了金融消费者等个体在个人信息处理活动中的各项权利，强化了金融企业等个人信息处理者的义务。从近年来官方通报的典型事例来看，金融行业在金融消费者个人信息保护上存在的风险漏洞不仅具有系统性，也愈发显现复杂性，即在法律规制的系统性漏洞中蕴含着个人金融信息泄露、扩散的可能性。在国外，涌现出个人金融信息及其财产性利益被默示让渡给银行的案例，如“图尔尼尔案”[13]和“彼特森案”[14]，这些案例推动司法裁判在责任认定方面向前迈进了很大一步。在国内，刘某某诉工商银行上海分行侵犯隐私权案[15]和郭某诉民生银行南京分行案[16]等个人金融信息权益被默示让渡的案件亟待引起立法部门的重视和回应。随着金融消费者信息完成从公共物到风险物的客体性变迁，构建风险民事责任就成为保护金融消费者信息的必然选择。

1.金融行业的复杂性风险必然导致引入风险民事责任

大数据时代数据量巨大且商业价值高，损害个人金融信息的破坏性将产生杠杆效应，对个人金融信息安全构成严峻考验。防范系统性金融风险不仅是对金融行业的要求，对于整个经济社会发展也有重要意义。金融风险伴随着互联网全覆盖，不确定性弥散后使得原来有形世界逐渐挣脱传统良善机制的捆绑，传统法律机制对此却难以控制。在前述游某诉徽商银行成都金牛支行一案中，银行行长等人在利用金融消费者个人信息时，不仅侵犯了客户的个人信息权益[17]，而且还篡改金融消费者信用信息进行欺诈，骗取客户的巨额财产。个人金融信息一旦泄露或者被非法使用，极易导致自然人的人格尊严受到侵害，人身、财产安全受到危害，因此，对处理敏感个人信息的活动应当作出更加严格的限制。面对违法形态复杂性的挑战，金融企业必须按照“风险最小化，收益最大化”[18]的风险民事责任给自身设定义务，为金融消费者设定权利。个人金融信息的风险责任是金融企业违反风险义务所应承担的不利法律后果。个人金融信息风险责任的复杂性表明：责任形态既包括个人责任，也包括组织责任；既包括危险责

任，也包括后果责任；既存在客观责任，也存在主观责任；既存在间接责任，也存在直接责任。总的来说，金融复杂性风险是线性规律和非线性规律、单向度规律和互补性规律、被组织规律和自组织规律共存的风险形态，其中各种规律分别运转于各自有效的范围之内。复杂性方法把系统性方法作为一种特殊的极限情况包括在自身之中，这构成真正的复杂性方法和观点[19]，传统的单一主体行使方式不能有效解决个人金融信息本身的复杂性和共识达成过程的复杂性问题，加上个人金融信息本身的高度复杂性和利益敏感性，对风险扩散的因果认定只能从对确定性的追求转向对不确定性的分析[20]。

2.风险民事责任的引入顺应风险物客体性变迁所产生的合理性需求

无论从实践还是从法律目的上看，个人金融信息在公共领域是非共享不能带来巨大便利，因此，充分考虑个人信息保护的公共性背景或社群背景，承认个人金融信息具有公共性对于当代金融生活有重要意义。个人金融信息符合经济学上的“公共品”核心特征，即非竞争性和非排他性。信息公共物品带给金融消费者与金融企业的不只是便利，也有无处不在的风险。金融企业会利用该行业的特质和个人金融信息进行经营活动。在互联网发达时期，金融企业的盈利方式已不仅局限于传统的金融方式，更多的是互联网信息数据流量方式，因而这种情况下就意味着本来就处于弱势地位的消费者因为技术等原因变得更加容易被利用与侵犯。例如银保监会公布的处罚决定事由中，有中信银行对客户敏感信息管理不善致其流出至互联网[21]，支付宝（中国）网络技术有限公司对个人金融信息收集不符合最少与必需原则、对个人金融信息使用不当等[22]。金融消费者的个人金融信息是需要一定程度的社会控制来构建和保护的公共物品，在风险社会中消费者经过告知—同意框架让渡个人信息，而《个人金融信息保护技术规范》中的技术规范覆盖了风险规范，出现了风险规范缺失的制度困境。在这种情况下，单纯用民事法律关系保护公共物品存在极大的私法困境。因此，企业法人组织不仅要加大公共物品的管理性规范，更要及时构建契合风险防范的法律要素。在公法上，个人金融信息具有信息流通的价值，在流通增值收益的同时，难以控制的信息风险从流通环节外溢极大地危害着金融消费者的利益，严重地破坏了金融行业固有的法律秩序，更直观地破坏和抹杀了金融消费者的个体意志自由。尽管个人金融信息在定义上几乎被视为公共领域的组成部分，是可以广泛获得和使用的，但信息风险一旦挣脱了正义的捆绑，脱去了法律的绳索，就呈现风险物的特性。从个人信息权益保护的角度来看，期望通过个体自我决定、自我主宰以保护自己信息权利的意思主义民法学说，对个人信息权益保护的思考不免陷入过于简单的桎梏，我们有必要通过对现行法律规定的检视与反思来探寻有效的个人金融信息法律保护路径。

3.风险民事责任契合个人金融信息的规则填补空间

随着互联网金融产品的迭代，金融领域默示同意个人身份信息的法律保护已经难以应对个人金融信息风险的复杂性。为了预防潜在风险，其一，在个人金融信息保护场景，企业应当设置风险行为规则，即类似于合同的附随义务，例如消费者报告义务，即借鉴美国 FCRA 这类响应计算机化和数字记录的信息法，提供“消费者报告”机制，由消费者报告代理机构进行对任何针对消费者信用价值或个人特征的通信，用于建立消费者的信用资格。同时，详细规定在什么情况下可以向另一方提供消费者报告，以及将这些报告用于执法或聘用等目的的法律限制。其二，将一部分特定风险信息从信息目录中独立出来进行保护，将金融消费者记录定义为“金融企业在系统或合同中‘维护’的‘与金融消费者直接相关的信息’”。其三，设置公平信息惯例的法定义务，作为默示同意信息利用的前置条件。将金融消费者个人信息的存在与遵循公平信息惯例的义务联系起来，对处理金融消费者信息的组织规定义务，禁止金融信息运营商未事先征得订户的书面或电子同意情况下收集任何与订户有关的默示同意个人身份信息。

三、风险民事责任与民事责任体系的衔接：塑造结构性赋权机制

在金融信息保护领域，对与《个人信息保护法》相关的现行法律、法规和规范性文件进行及时更新，才能确保该法顺利实施，更好地推动个人金融信息保护与信息流通利用制度健康发展。为了稳定公共秩序与私权保护，在现行安全保障义务的基础上，对作为私权主体的金融企业利用个人金融信息应当提出进一步的风险预防要求[23]。面对现行法存在的系统性规范缺失，明确金融企业的风险民事责任，赋予金融消费者人格权，在金融信息保密义务的基础上，增加金融企业信息安全管理义务和信息风险评估义

务并灵活增减义务规则，以保障个人金融信息的安全性，更好地保护金融消费者个人信息权益。

1.概括赋予金融消费者人格权

个人金融信息利用行为规则并不能取代信息权利的保护路径，信息权利保护应当顺应信息风险的复杂性。个人金融信息归属于人格权法，可以通过《民法典·人格权篇》为信息技术的未来发展留下解释空间[24]。针对金融消费者信息保护的私法缺位，可以借助《民法典》第799条[25]让消费者的人格权在个人金融信息保护中得以具体化。针对个人金融信息的内涵、搜集范围和手段、处理方式、侵权形式等正在发生巨大变化，金融企业存在产品宣传引人误解[26]、系统权限管理漏洞、外包机构管理缺陷等诸多风险[27]的情况，在金融消费者人格权益私法保障不足的背景下，需要增加金融消费者民法人格权的公法要素。在国外，《加州消费者信息法案》（2018）通过增加消费者反歧视权，赋予消费者诉讼权利以获取赔偿，并设立“消费者信息基金”，通过金融市场普遍非歧视的服务保障金融消费者的个人信息，确立了消费者信息的宪法基本权利保护和社会法保护模式。在国内，《民法典》颁布之后，互联网信息领域中的司法解释将面临极大挑战，民法人格权条文或许能够提供金融消费者基本权利保障的赋权入口[28]。同时，从广州互联网法院审理的王女士在某银行“被刷脸”一案[29]来看，增加对金融消费者生物特征的有效识别，是避免个人生物特征信息利用超过必要限度的关键措施。针对消费者金融信息人格所蕴含的财产性利益保护，未来可以根据《个人信息保护法》第70条和最高人民法院有关个人信息保护的司法解释[30]，对于用AI变脸等深度伪造技术对金融消费者群体的信息权益造成的伤害，制定由消费者组织或由国家网信部门确定的组织提起民事公益诉讼的具体规范指引，以此补位人格权侵权保护之不足。

2.具体课以附随义务：个人金融信息安全管理义务和风险评估义务

《个人信息保护法》第9条和第59条分别确定了个人信息处理者和个人信息处理的受托人对个人信息处理活动采取必要安全措施的义务，在第51条[31]和55条[32]也具体阐述了个人信息处理者采取措施防范安全风险和影响评估等义务。由于技术的发展，风险民事责任具体化中内嵌的义务性规范也应当不断细化明确，尤其在金融领域，需要通过具体的司法解释课以金融企业信息安全管理义务和信息风险评估义务两项义务。金融产品是信息的组合，由于构成原理复杂，即使在信息适量的情况下，普通消费者也很难完全理解信息的内容从而对产品有全面认知。专业化复杂化的金融合同使消费者处于不利地位，他们难以依常识判断金融产品是否存在瑕疵。正是由于金融消费合同的特殊性，因此法律对金融企业予以一定程度的规制，金融企业除应提供合法合规的金融产品和服务，还应对风险警示等重要事项予以充分适当的说明[33]。在伊某与中国工商银行盘锦分行储蓄存款合同纠纷再审案件中[34]，最高人民法院明确银行在为自然人办理业务时应尽到最大的注意和风险提示义务。需要强调的是，面向消费者的金融产品通常具有复杂性和不可理解的特点，有必要在司法解释中细化金融企业的信息安全管理义务和信息风险评估义务等附随义务，要求金融企业引入内部程序和机制，以确保消费者对产品的正确理解，从而降低个人和社会成本，增加消费者对金融企业的信任。

关于个人金融信息安全管理义务，依据《个人信息保护法》第38条和第40条，只有关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的信息处理者，在向境外提供数据时才需要通过国家网信部门组织的安全评估。《个人信息保护法》已给出信息分级保护问题的法定方案，即区分一般个人信息的处理和敏感个人信息的处理，第51条还对个人信息进行了横向的切分。设置金融企业信息安全管理义务，旨在促使金融企业采取符合法律法规、国家标准的安全措施，妥善保管所收集的个人金融信息，防止信息遗失、毁损、泄露或者篡改。在监管条例中应当明确金融企业在没有尽到信息保护义务时应当承担的法律责任，不仅是行政责任，还包括相应的民事责任和刑事责任；要制定更加详细的处罚措施，加大处罚力度，增加违法成本，充分保障金融消费者的个人信息权益[35]。2019年上海金融法院在丁某诉甲银行储蓄存款合同纠纷案[36]的判决书中就指出，银行负有妥善保管金融消费者银行卡卡号、密码的义务，对网上银行业务客户资料负有安全保障义务。另外，为保障个人金融信息安全，金融企业需建立良好的数据存储空间，保障其安全，并构建个人金融信息更新机制，保证信息的及时性、准确性和有效性。需要说明的是，金融企业保护消费者个人金融信息安全的义务不因其与外包服务供应商合作而转移、减免。

《个人信息保护法》第 56 条罗列了个人信息保护影响评估的内容，包括单方处理敏感个人信息、利用个人信息进行自动化决策、个人信息流转（包括委托、提供和公开）、向境外提供以及其他对个人有重大影响的五类场景。风险评估可分为自身风险评估和外包机构风险评估。金融企业自身的风险评估应当由金融监管机构进行，内容包括对金融企业保护措施的评估，如内部机制的完善、自身履行职责的状况与能力等。金融企业应当充分审查、评估外包服务供应商保护个人金融信息的能力，在相关协议中明确外包服务供应商保护个人金融信息的职责和保密义务，并采取必要措施保证外包服务供应商履行上述职责和义务[37]。

3.增设默认付费和默认罚款的财产权保护机制

《个人信息保护法》第 44 条明确个人对其个人信息的处理享有知情权、决定权。由于在金融交易中存在交易双方信息披露不对称的情况，因此对金融消费者知情权的保护尤为必要。为了保持金融消费者与金融企业的利益平衡，应在通知义务等普遍的公法义务保护模式中增加市场平等服务协议中的私法保护模式，即“默认付费”和“默认罚款”。

（1）以默认付费模式赋予金融企业信息开发权

对于金融企业与金融消费者之间的信息利用关系，学理上存在两种解释：一种是认为信息从金融消费者提交给金融企业开始就已完成所有权的转移，从此信息归属于金融企业，金融消费者对其再无权利[38]；另一种则认为金融企业和金融消费者之间是“保管”关系，金融消费者为了享有金融产品及服务而提供自身的信息，金融企业只是将这些信息作为加密手段或是金融产品的附属品予以保存[39]。需要说明的是，个人金融信息同时具有流转价值与安全价值，实现上述价值的平衡需赋予金融企业部分信息权以开发信息价值[40]，同时应规定相应的义务，保障金融消费者权利。纯粹的保管关系无法满足这一要求，因为保管合同关系属于静止法律关系，即金融企业作为信息的保管人对于信息履行保管义务，但过严的信息保护会抑制金融创新的动力。金融企业与消费者之间建立的交易关系实质为金融消费合同关系，金融企业对个人金融信息合理利用及保密是金融消费合同中的附随义务。现存普遍免费模式[41]存在虚化“同意原则”[42]、降低网络服务提供者责任等问题，在此情形下，现实中网络信息消费者在特定领域下会更加重视个人信息的利用与信息保护，且宁愿支付对价以获得网络信息产品和服务，对于该人群的合理需求，法律应当提供相应的制度供给满足其需求，由此构建金融消费者在金融领域中个人信息的财产权保护制度——默认付费。

（2）以默认罚款模式实现金融消费者权益保障

前述默认付费作为义务性规范是基于消费者对个人金融信息的敏感程度，通过金融企业提供付费服务的方式实现消费者个人金融信息的保护，即金融企业应当遵守具体的规则，否则应当承担“罚款”责任。金融企业无论是根据其法定义务还是合同义务，都应该对个人金融信息负有保密义务，这是对金融消费者信息权和财产权的保护。金融消费者与金融企业签订客户服务协议（金融消费合同），金融企业基于该合同收集相应服务所需的客户个人数据，并且作为数据控制者同时需要承担数据安全保障的义务（如采取加密、匿名处理等技术手段），在法律允许和客户授权范围内合理使用数据并履行信息披露义务[43]。在大数据背景下，金融企业掌握大量数据信息，与金融消费者在议价能力方面存在较大优势，前面论证的金融企业与金融消费者之间建立的合同关系中，因其违反约定义务的成本较低，金融企业往往不会对个人金融信息尽到合理利用与保密义务[44]，金融消费者权益的有效保障难以实现。

“默认罚款”旨在督促合同强势一方履行安全保障义务，并通过在软件系统中设置信息强制默认罚款来实现。提高企业不履行义务的费用负担，可以提高消费者作为合同弱势一方的议价能力。根据“默认罚款”监管部门可以直接惩罚不履行合同义务的缔约一方，以使合同相对方具有相等的议价能力。信息的默认强制设置（包括默认罚款设置）将不利于提供更多信息的一方，也有可能虚化了告知移除规则，但是这些默认规则在定义上是非多数主义的，会由于罚款议价能力的改变而改变，如果不能有效地保证履行安全保障义务，合同相对方将频繁地改变默认。软件执法的灵活性在于将安全保障义务与经济上的可负担性进行合理计费，这种随时改变算法的个人金融信息保护也是一种金融市场交易的产权化机制。

四、个人金融信息风险民事责任的承担路径

在个人金融信息损害救济方面，《个人信息保护法》等相关法律必须有对应的条文对接风险民事责任，使个人金融信息风险民事责任落到实处。从构成要件层面来看，将风险民事责任架设至民事责任体系的主要问题在于，因果关系等核心概念与传统体系中的含义并不完全一致。为实现个人金融信息的损害救济，可以将金融企业市场特许经营许可架设入格式合同的效力要件，在一定范围内放宽因果关系推定标准并施行严格的归责原则。

1.金融企业市场特许经营架设至金融领域格式合同的效力要件

在金融领域，个人金融信息处理者与消费者之间往往签订格式合同，前者利用在市场的优势地位，通过预设的格式条款使消费者处于不利地位。鉴于此，有必要将金融企业市场特许经营架设至金融领域格式合同的效力要件之中。《民法典》第153条第一款明确规定“违反法律、行政法规的强制性规定的”为民事法律行为无效情形之一。根据通说，法律、行政法规中的强制性规范属于“效力性强制规范”的包括两类：一类是“明定无效型”，即法律、行政法规明文规定违反强制规定的法律行为无效的情形；另一类是“危害公序型”，即违反该强制规定即损害公共秩序的情形。金融企业市场特许经营是由政府有关部门许可授予的，具有很强的行政管理特征。在金融企业的经营方式和经营范围上，行政机关对金融从业机构进行行政许可审批，并颁发市场主体资格和经营资格证照。即使是仅限制一方当事人市场进入（准入）资格或资质条件的“资质限制类”强制性规范，若损害社会公共秩序（主要情形为损害公众安全）的，则也属于效力性强制规范。

2.金融企业监管义务架设至个人金融信息的风险民事责任认定

由于金融消费者合同的设立及其履行一定程度上依赖金融企业的诚信，为寻求合同相对方履约的法律基础，必须建立履行协议的空间和范围。公义务架设至私义务可以通过私法诉讼中私法规范的公法要素来实现，当消费者以金融企业作为被告不履行合同义务而提起诉讼的时候，举证规则应当纳入行政监管认定的结论（如金融企业内部管理失职的行政处罚决定书）。

（1）金融企业违约责任中架设公义务条款

金融企业与消费者以协议方式拟定相关的义务，该协议通常是行政机关以行政手段规制的格式合同[45]或金融企业经过行政机关事前审查制定的合同，在该类合同中将安全保障义务作为金融企业违约责任架设入公义务中。此种安全保障义务不论是通过行政规定的方式，还是通过行政合同的方式制定，对于行政机关、金融企业和金融消费者而言都更加契合现行公共高效治理与私权保护的目的，也更体现公私法领域多维度立法融合的趋势[46]。而以上公法私法融合实现的一种有效形式就是契约方式，行政机关除了通过制定监管规则之外，更为方便的方式是通过行政合同与金融企业约定安全保障义务，通过这种由公法上诚实信用原则的附随义务架设而形成的安全保障义务作为履行合同的基础，只要金融企业有违反义务的行为，除了行政合同所具有的作为民事契约的归责，还会受到行政合同因约定了安全保障义务而带来的公法上的惩罚，即行政机关依据行政合同既可以追究违约责任也可以主张违反安全保障义务而进行行政处罚[47]。具体来看，此类行政合同要求金融企业和互联网金融平台通过与消费者用户签订协议的方式来敦促双方遵守法律法规以及互联网相关公约[48]。实践中，公权力的影响力已经慢慢渗入对金融企业与消费者签订的格式合同之中，这种行政监督的力量对于市场的整饬效果是立竿见影的。

（2）增加判断金融企业侵权责任的公法要素

依据《个人信息保护法》第69条规定，金融企业侵害个人金融信息权益的侵权赔偿责任适用过错推定责任，即若金融企业不能证明自己没有过错的，就应当承担损害赔偿等侵权责任。但在司法实践中，金融消费者一方在调查取证和举证质证时面临银行等金融机构的压倒性优势，对于金融企业内部管理漏洞导致的个人金融信息损害难以查清事实[49]，行政机关在进行行政监管时依据原来的单一公法监管规制也已失去效用。行政机关为了保护消费者个人金融信息，需要将风险民事责任纳入金融企业与消

费者民事协议的范围，与金融企业的安全保障义务一起作为规制企业的方式，由此完成金融企业的严格过错责任推定。金融企业在利用消费者信息提供产品和服务的过程中对于消费者信息造成的损害，不论是自身造成的还是基于第三人造成的，基于协议中金融企业应遵守的风险民事责任，对可能发生的损害消费者个人信息的行为直接推定企业承担责任，此乃主观要件客观化处理的合理方式。

在网络侵权领域，出现平台侵犯个人信息利益时，因果关系的认定问题往往更为棘手。这不仅仅是因为大数据时代信息的海量性、传播的即时性和复刻的便利性使得人们的交易模式发生了巨大的变化，企业普遍启用的算法机制也使得责任溯源的路径荆棘丛生[50]。在金融网络领域，追求明晰和单一化的因果关系链条，在某种程度上已经背离互联网时空的复合性以及科技发展的规律。在金融企业侵犯消费者信息的案件中，法院往往基于高度盖然性的标准，即当全案证据显示待证事实存在的可能性大于其不存在的可能性，使得法院有理由相信事实很可能存在时，尽管还不能完全排除存在相反的可能性，也允许法院依据高度盖然性标准认定待证事实，因而现实中往往是基于此来认定企业高度存在泄漏消费者个人金融信息的可能性[51]。但这种高度盖然性的因果关系判断更多的是基于法官的内心确信，是基于法官的知识体系及生活经验做出的判断，具有极大的不确定性与不严谨性。因此，在个人金融信息侵权诉讼中，举证困难的一方，将行政监管机关做出的金融企业内部监管失职等相关文书作为证据，司法机关以此作为推定因果关系成立的综合判断指标的重要考量因素，不失为一种更为公平高效的方式[52]。

注释：

1[1]甬银保监罚决字[2021]64 号。

2[2]《脱口秀演员池子交易流水遭泄露，中信银行深夜致歉》，https://www.163.com/dy/article/GIV0SVJ50549B1FP.html。

3[3]深圳市法学会：《聚焦“支付宝年度账单事件”》，https://www.sohu.com/a/219129029_100011665。

4[1]朱芸阳：《个人金融信息保护的逻辑与规则展开》，《环球法律评论》2021 年第 6 期。

5[1]易涛：《金融隐私权法律保护问题探析》，《科技与法律》2016 年第 1 期。

6[2]《民法典》第 135 条：“民事法律行为可以采取书面形式、口头形式或者其他形式”。

7[3]《民法典》第 140 条：“行为人可以明示或者默示作出意思表示。沉默只有在有法律规定、当事人约定或者符合当事人之间的交易习惯时，才可以视为意思表示”。

8[4]《消费者权益保护法》第 29 条：“经营者收集、使用消费者个人信息，应当……明示收集、使用信息的目的、方式和范围，并经消费者同意。”

9[5]《网络安全法》第 22 条第 3 款：“网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意。”

10[6]《消费者权益保护法》第 29 条：“经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。”

11[7]成都市中级人民法院[2021]川 01 民初 9707 号判决书。

12[1]朱芸阳：《个人金融信息保护的逻辑与规则展开》，《环球法律评论》2021 年第 6 期。

13[2]英国“图尔尼尔”案中法院援用“默示条款”理论作为认定银行承担金融隐私信息权保护义务的理论基础，认为该银行违反了对客户的金融隐私信息保护义务，应承担赔偿责任；银行对金融隐私信息权保护的范围包括银行因其与客户关系的存在而获得的任何信息，且金融隐私信息权保护义务不因客户结清账户或停止使用账户而终止。

14[3]美国“彼特森”案中，法院将银行对金融隐私信息权的保护范围限于有关账户的信息和客户的交易情况两个方面。该案开启法院认可银行未经客户许可而透露其信息时，客户得以银行违反了与客户的契约间的默示条款为由起诉银行的先河。

15[4]参见上海市高级人民法院[2016]沪民申 2161 号判决书。

16[5]赵兴武、徐高纯、邵小波：《未经许可查询客户信用信息南京一银行被判书面赔礼道歉》，《人民法院报》2012 年 3 月 23 日。

17[1]金融隐私信息权是由隐私信息权引申出来的下位概念，实质是传统隐私信息权在金融领域的一种延伸，也是隐私信息权由消极被动的权利向积极主动的权利的一种转变。金融隐私信息权，是指权利主体积极主动地支配控制与自身的财产、交易相关或其他能够反映个人信用状况的信息的权利。具体参见谈李荣：《金融隐私信息权与信用开放的博弈》，法律出版社 2008 年版，第 1 页。

18[2][美]赫伯特·西蒙：《管理决策新科学》，李柱流等译，中国社会科学出版社 1982 年版，第 33 页。

19[3]陈一壮：《包纳简单性方法的复杂性方法》，《哲学研究》2010 年第 8 期。

20[4][比]伊利亚·普利高津：《确定性的终结：时间、混沌与新自然法》，湛敏译，上海科技教育出版社 1998 年版，第 146 页。

21[5]银保监罚决字[2021]5 号。

22[6]杭银处罚字[2018]23 号。

23[1]Edward J.Janger,Paul M.Schwartz,"The Gramm-Leach-Bliley Act,Information Privacy,and the Limits of Default Rules",Minnesota Law Review,2002(86),pp.1249-1261.

24[2]张新宝：《民法典为 AI 立法留下空间》，https://www.sohu.com/a/396790633_114988。

25[3]《民法典》第 799 条：“任何组织或者个人不得以丑化、污损，或者利用信息技术手段伪造等方式侵害他人的肖像权。未经肖像权人同意，不得制作、使用、公开肖像权人的肖像，但是法律另有规定的除外。”

26[1]杭银处罚字[2018]23 号。

27[2]银保监罚决字[2021]5 号。

28[3]人格权与基本权利及其他公法上权利之间的暧昧关系也引发了我国学者对人格权的规范品质的反思。具体参见姚辉：

《从立法论迈向解释论的人格权编》,《清华法学》2020 年第 3 期。

29[4]广州互联网法院:《银行不能证明办卡及贷款者为其本人，驳回全部诉请》,《人民法院报》，2021 年 8 月 19 日。

30[5]贺荣:《国务院新闻办公室举行司法审判服务保障全面建成小康社会新闻发布会答记者问》,国新网,http://www.scio.gov.cn/xwfbh/xwbfbh/wqfbh/44687/46962/index.htm。

31[6]《个人信息保护法》第 51 条：“个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：（一）制定内部管理制度和操作规程；（二）对个人信息实行分类管理；（三）采取相应的加密、去标识化等安全技术措施；（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；（五）制定并组织实施个人信息安全事件应急预案；（六）法律、行政法规规定的其他措施。”

32[7]《个人信息保护法》第 55 条：“有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：（一）处理敏感个人信息；（二）利用个人信息进行自动化决策；（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；（四）向境外提供个人信息；（五）其他对个人权益有重大影响的个人信息处理活动。”

33[8]黄莉萍、潘晟:《金融消费合同中的品质担保责任问题探究》,《行政与法》2017 年第 6 期。

34[9]最高人民法院[2017]最高法民再 174 号判决书。

35[1]黎四奇、苗羽亭:《大数据背景下金融隐私权的保护》,《财经理论与实践》2019 年第 4 期。

36[2]参见上海金融法院[2019]沪 74 民终 200 号判决书。

37[3]例如建立外包服务供应商的竞争机制，严格审核其资格，提高准入门槛；通过签订合同等方式对相关事项予以明确规定并严格履行个人金融信息等资料交接登记手续，保证职责范围内的责任清楚划分，明确资料交接相关查验程序；完善资料交接及销毁制度；外包服务期结束之后严格要求该公司及相关人员将金融信息及资料等退回或者销毁，并派专人予以监督。参见杨为程、张金金:《互联网金融信息中的隐私权保护》,《新疆教育学院学报》2017 年第 4 期。

38[4]United States.Miller,425U.S.at442-43&443(1976);Smithv.Maryland,442U.S.735,736-37(1979).

39[5]Joseph Jerome,"Big Data:Catalyst for a Privacy Conversation",Indiana Law Review,2014,pp.1-30.

40[1]何颖:《数据共享背景下的金融隐私保护》,《东南大学学报（哲学社会科学版）》2017 年第 1 期。

41[2]网络服务提供者通过普遍免费模式实现初期扩张，往往会因过分索取用户的个人信息作为经营的战略资源或用于进行交易的数据财产而损坏用户的个人信息权益，并且免费的实质是以数据支付为对价，网络服务提供者免费获得了最有价值的资源--用户的注意力，并将消费者和更多的注意力转化为市场份额，以实现营利的目的。

42[3]方禹:《个人信息保护中的“用户同意”规则：问题与解决》,《网络信息法学研究》2018 年第 1 期。

43[4]赵吟:《开放银行模式下个人数据共享的法律规制》,《现代法学》2020 年第 3 期。

44[5]金融机构与金融监管机关之间成立的是垂直的行政监管关系，法国隐私监管机构根据通用数据保护条例（GDPR），对谷歌处以 5700 万美元罚款，原因是谷歌在设立账户时，以广告为目的迫使人们“同意”对其数据进行处理。具体参见 Ceresearch：《由谷歌高额罚单案再谈金融消费者信息安全权》，https://mp.weixin.qq.com/s/a TJyde Rq2a177Qf Dsl_tnw。

45[1]王瀚、张超汉：《格式合同的行政规制》，《科学经济社会》2009 年第 4 期。

46[2]通常而言，在经营者入驻平台阶段，平台需要对其进行实名登记并审查相关主体的资质是否完备，同时在日常的运营阶段还负有报告义务。对于网络平台内运营的经营者，网络平台不仅需要进行资格审查，还需督促应用程序提供者发布合法应用程序，尊重和保护应用程序提供者的知识产权。另外，网络平台在运营过程中也需要对用户的个人信息安全承担保障责任。参见 Federal Trade Commission,"Privacy&Date Security Update:2018",Federal Trade Commission and Staff Reports,https://www.ftc.gov/reports/privacy-data-security-update-2018。

47[3]王学辉、赵昕：《隐私权之公私法整合保护探索——以“大数据时代”个人信息隐私为分析视点》，《河北法学》2015 年第 5 期。

48[1]如《区块链信息服务管理规定》第 7 条、《互联网新闻信息服务管理规定》第 14 条、《互联网论坛社区服务管理规定》第 6 条等。

49[2]何沛芸、吕新文：《千余毕业生莫名被开多张农行卡，当事人要了解真相》，https://m.thepaper.cn/baijiahao_15808648。

50[3]See Thomas Hemnes,"The Ownership and Exploitation of Personal Identity in the New Media Age",Marshall Rev.Intell.Prop.L.,2012(1),pp.1-39.

51[4]参见北京市朝阳区人民法院[2018]京 0105 民初 36658 号判决书。

52[5]王晓锦：《人工智能对个人信息侵权法保护的挑战与应对》，《海南大学学报（人文社会科学版）》2019 年第 5 期。