

VISA

反诈骗攻略： 市场对策和 行业洞察



2025 年 8 月

目录

综述	4
简介	5
诈骗的定义	6
有哪些利益相关者参与实施反诈骗对策？	8
反诈骗框架如何明确责任与问责制？	9
利益相关者如何应对诈骗？	12
Visa 内部举措	16
结论	19
附录	20





保密声明

本文件中包含的信息（以下简称“信息”）是作为 Visa 客户和/或 Visa 支付系统参与者提供给您的。该信息属于机密内容，受 Visa 核心规则和 Visa 产品与服务规则以及/或保密协议中的保密限制约束，这些限制规定了您对信息的使用方式。您同意对该信息保密，并仅在作为 Visa 客户和/或 Visa 支付系统参与者的身份下使用该信息。该信息仅可在您所在组织内按需知情的原则进行传播。请注意，根据美国联邦证券法，该信息可能构成重大非公开信息，在知悉重大非公开信息的情况下买卖 Visa Inc. 的证券将构成违反适用的美国联邦证券法的行为。

免责声明

在本文件中，案例研究、统计数据、研究结果、总结和建议“按原样（AS IS）”提供，仅供参考，不应作为运营、营销、法务、技术、税务、财务或其他建议的依据。您应当咨询您的法律顾问，以确定您的具体情形须遵守哪些法律法规。具体观察结果、建议或项目的实际成本、节支和收益可能因您的特定业务需求和项目要求而异。就性质而言，建议并不能保证未来的业绩或结果，并且受到难以预测或量化的风险、不确定性和假设的影响。对于您使用本文所含信息（“信息”）（包括任何类型的错误、遗漏、不准确或不及时）之行为，以及您通过使用这些信息而得出的任何假设或结论，Visa 概不承担任何责任。Visa 不作任何明示或默示的保证，并明确否认有关适销性或适用于特定用途之保证，同时不保证不侵犯任何第三方的知识产权。在适用法律允许的范围内，对于您或任何第三方根据任何法律理论须承担的任何损害赔偿——包括但不限于任何特殊性、间接性、附带性及惩罚性损害赔偿，以及业务利润损失、业务中断、业务信息丢失及其他金钱损失的损害赔偿，Visa 概不承担任何责任（即使已被告知此类损害赔偿的可能性）。

前瞻性陈述

本文件中的信息包含美国 1995 年《私人证券诉讼改革法案》界定的前瞻性陈述。前瞻性陈述通常包含“相信”、“估计”、“预期”、“打算”、“可能”、“项目”、“展望”、“可以”、“应该”、“将要”、“继续”及其他类似表述。前瞻性陈述的示例包括但不限于，我们就金融行业的诈骗和防诈骗发展形势而做出的陈述。就性质而言，前瞻性陈述：(i) 仅陈述自其发表之日起的预期；(ii) 并非对历史事实的陈述或对未来业绩的保证；以及 (iii) 会受到各种风险、不确定性、假设或者难以预测或量化的环境变化的影响。因此，鉴于各种因素（例如，Visa 向美国证券交易委员会提交的文件详列的因素），实际结果可能与我们的前瞻性陈述存在重大不利差异。您不应过分倚赖于这些陈述。除非法律另有规定，否则，我们不计划针对新信息、未来发展或其他原因而对任何前瞻性陈述做出更新或修改。

综述

诈骗问题在全球普遍存在、不分国界，对全球各地的个人和企业都造成影响。近年来，诈骗问题的发生频率、涉案损失出现激增趋势，使该问题变得日益复杂、难以辨识——尤其是在人工智能（AI）得到广泛应用的背景下。

根据全球反诈骗联盟（Global Anti-Scam Alliance, GASA）的数据，2022 年 8 月至 2023 年 8 月期间，诈骗造成的损失共计超过 1 万亿美元¹。据报道，亚洲市场因诈骗而损失的国内生产总值（GDP）高于其他地区。

金融生态圈中的各种利益相关者——包括金融机构、基础设施提供商、社交媒体平台、支付网络、监管机构和消费者——在打击诈骗方面发挥着至关重要的作用。每个利益相关者分别承担特定的重要职责，以建立韧性防御来抵御相关威胁。为保护消费者，监管机构建立了明确责任与问责制的反诈骗框架。亚太地区围绕身份验证、情报共享和提高消费者意识，采取了各种反诈骗举措。帮助消费者了解诈骗风险及征兆是极其重要的，保持警惕的群众仍然是我们防范诈骗的第一道防线。随着 AI 的进步，代理型商务正在成为现实。代理型 AI 即将通过自适应异常检测和前瞻性威胁预测，为扩大反诈骗规模设定新的标准。

Visa 致力于与金融生态圈内的各个利益相关者合作，共同保护消费者和企业，防止其遭受诈骗。过去五年，为减少诈骗并增强网络安全，Visa 在相关技术方面投资了 120 多亿美元。归根结底，建立生态圈全局化方案对于有效打击诈骗和保护所有相关方的至关重要。



诈骗是一种不分国界的威胁。Visa 致力于与全球生态圈利益相关者合作，有效且高效地打击诈骗。根据我们的见解，为保护生态圈，并确保商业在安全环境下持续蓬勃发展，结合各方力量共同应对诈骗是至关重要的。



Stefaan D'Hoore

Visa 亚太区风险官

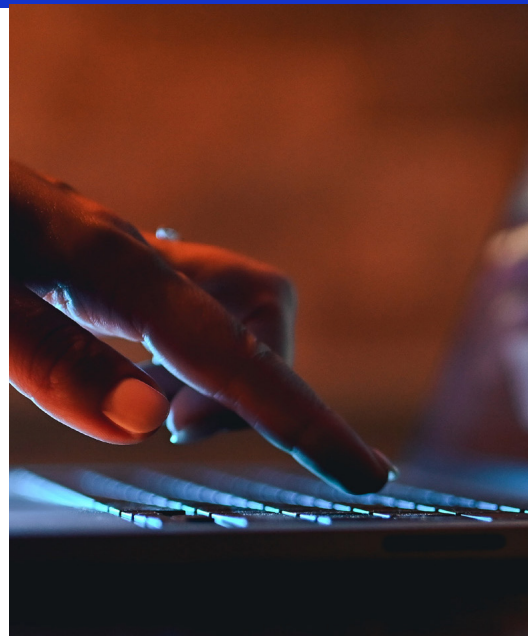
¹ 全球反诈骗联盟（GASA, 2024）。《全球诈骗状况报告：12 个月内被骗 1 万亿美元》。

简介

随着数字应用程序及工具的日益普及和演变，消费者可快速、无缝地完成转账。到 2026 年，全球使用电子钱包的人口预计将超过 52 亿²，而到 2028 年，全球零售电子商务销售额预计将达到 6.8 万亿美元³。然而，这也给诈骗分子带来更多骗取消费者和企业钱财的可乘之机。在全球范围内，诈骗一直是一个反复出现的、对各行各业的人们造成影响的问题，据估算，诈骗活动每年造成的相关损失达 1 万亿美元⁴（超过全球 GDP 的 1%）。随着 AI 的应用，该形势进一步延续，即使对有辨别力的人而言，诈骗也变得更具有欺骗性。

对于诈骗问题，亚太区的国家和地区也未能幸免。事实上，据估计，2024 年，该地区的个人消费者因诈骗而遭受的损失共计 6880 亿美元⁵。具体而言，在新加坡，诈骗造成的损失从 2020 年的 2.66 亿新元⁶，增长至 2024 年的 11 亿新元，增长了 145%⁷。在澳大利亚，2024 年报告的诈骗损失超过 20 亿澳元⁸，比 2020 年报告的 8.5 亿澳元增长了 135%。值得注意的是，台湾消费者在一年中遭受了 74 亿美元的诈骗损失⁹，占台湾 GDP 的 1%¹⁰。作为商业和金融生态圈中的领先支付服务提供商，Visa 致力于让诈骗问题获得更多关注，共同应对诈骗损失额的惊人增长。

本白皮书将从三个方面，考察政府和行业参与者的反诈骗对策，这三个方面包括：涉及的主要参与者、责任与问责制的概念，以及亚太地区利益相关者为打击诈骗行为而采取的行动。我们将通过这些视角来阐述合作应对措施将如何有效且高效地打击诈骗，并最终帮助各方更好地保护金融生态圈，以确保商业在安全可靠的环境下持续蓬勃发展。



您知道吗？

750 亿美元

2021 年至 2023 年，加密货币平台有 750 亿美元遭诈骗分子骗取¹¹。

全球几乎有一半的人口每周至少经历一次诈骗。

来源：全球反诈骗联盟（GASA）和 Feedzai《2024 全球诈骗状况报告》

² Juniper Research (2023)。《到 2026 年，全球电子钱包用户超过 52 亿人》。

³ eMarketer (2023)。《2025 年全球零售电子商务预测》。

⁴ 联合国开发计划署 (UNDP) (2023)。《UNDP 与全球联盟伙伴共同发布反诈骗攻略》。

⁵ 全球反诈骗联盟 (2024)。《2024 年亚洲诈骗报告：损失 6880 亿美元》。

⁶ 新加坡警察部队 (2024 年)。《2023 年诈骗与网络犯罪年度简报》。

⁷ 新加坡警察部队 (2024 年 2 月)。《关于 2024 年诈骗与网络犯罪年度简报，您应当了解的五件事》。

⁸ 澳大利亚竞争与消费者委员会 (2024)。《反诈骗报告》。

⁹ 全球反诈骗联盟 (2023)。《马来西亚、泰国和台湾的数十亿美元去哪儿了？》

¹⁰ BERNAMA (2023)。《新闻报道》。

¹¹ Griffin, J. M., & Mei, K. (2024)。《Crypto Flows 平台如何助长“奴役”现象？杀猪盘经济学》。SSRN。



诈骗的定义

通常，人们认为欺诈 (fraud) 与诈骗 (scam) 是同一回事。然而，这两个词语之间存在微妙的差异。诈骗通常涉及欺骗行为，即误导消费者进行交易，而欺诈则可能在消费者不知情或者未参与的情况下进行。Visa 将诈骗活动定义为诱骗持卡人进行支付或授权支付的行为。这与欺诈略有不同，欺诈涵盖范围广，包括未经授权获取个人信息或资金的行为。诈骗不分国界，它往往利用多种渠道，在账户到账户 (A2A) 交易和卡支付之间切换。

常见诈骗类型¹²



杀猪盘

“杀猪盘”一词源于猪农（诈骗分子）在屠宰猪之前，先将猪（受害者）育肥的做法。在这种诈骗中，诈骗分子首先通过社交媒体或约会应用，与受害者交朋友。然后，他们与受害者建立信任，之后引诱他们通过诈骗平台转移现金、投资于加密货币或其他形式的资产。



冒充执法部门 / 银行职员

在此类诈骗中，诈骗分子冒充公职人员，谎称受害者因犯罪活动而面临调查，并告诫受害者勿联系同伴，因为后者正在接受审查。同时，诈骗分子还可能将电话转接到“其他机构”，以增加可信度。然后，要求受害者从账户中转账，以用于调查。



就业诈骗

在此类诈骗中，诈骗分子向受害者提供就业机会，即通过远程执行任务而获得“回报”。受害者可能需要支付一定的费用才能获得更高级别的工作。最初，诈骗分子需要发放一小笔金额来换取受害者的信任。一旦建立了信任，诈骗分子就会诱使受害者赚取更多金额。当受害者发现这些金额无法提取时，便无法再联系诈骗分子。



电子商务诈骗

在此类诈骗中，受害者点击社交媒体平台上的线上广告或线上市场中的帖子来购买物品，在付款后便无法再联系“卖家”。通常，这些物品的价格较低，以吸引受害者。



包裹投递诈骗

在此类诈骗中，诈骗分子通过短信或电子邮件，向受害者告知，由于邮资不足等原因，其包裹无法送达。然后，诈骗分子将受害者重定向至某个链接，要求其完成必要的付款，并借此获得受害者的个人信息。

¹² 联合国毒品与犯罪问题办公室（2024 年 10 月）。《东南亚跨国有组织犯罪与网络诈骗、地下银行和技术创新之汇集：不断变化的威胁格局》。



诈骗的定义

目前，尚未建立普遍接受的诈骗分类标准。

这一点造成了多方面的挑战，包括：

- 难以界定和衡量诈骗活动的完整范围，影响识别和报告。
- 难以促进执法部门、金融机构与其他利益相关方之间的有效沟通、数据共享和协调应对。
- 导致消费者因不确定自己是否遭遇诈骗或害怕自己须承担相关责任，而放弃予以报告。

美国联邦储备委员会开发了 ScamClassifier 模型¹³，用于支持对诈骗活动进行统一的、详细的分类、报告、分析和识别。该模型根据一系列问题，按类别和类型对诈骗进行分类。它能够辨别授权和未授权付款以及诈骗未遂等情形，捕捉诈骗造成的全方位影响。



如果在 Visa 的支付网络中发生了诈骗，Visa 会采取措施，以识别码 C（商户虚假陈述）和 D（操纵账户持有人）予以识别。C 类诈骗是指商户故意误导账户持有人，例如，销售与表面宣传不符的商品。D 类诈骗是指商户操纵账户持有人，让他们完成看似合法的交易。具体包括账户持有人向诈骗受益人汇款、误信自己将获得虚假财富或帮助陷入困境的个人。此外，报告可进一步分为七个方面，以便更详细地反映诈骗的类型（购物、投资、杀猪盘、预付费、发票、CEO 诈骗、冒充）。

诈骗之界定的标准化将为改进诈骗检测和预防工作奠定基础。尽管如此，金融生态圈仍需要在精确分类与灵活应对不断演变的诈骗伎俩之间保持平衡。¹⁴

¹³ 美联储金融服务（2024）。《ScamClassifier 模型》。

¹⁴ 全球反诈骗联盟（2024）。《诈骗的分类与衡量：2024 年美洲全球反诈骗峰会》。

有哪些利益相关者参与实施反诈骗对策？

根据分析，以下一个或多个利益相关者（排序不分先后）在实施反诈骗框架和方案中，发挥了积极作用。

金融机构

金融机构（FI）作为消费者资金的保管者，在各种支付渠道（包括银行转账、实时支付和卡）防范诈骗方面发挥着至关重要的作用。它们身处一线，负责检测可疑活动、教育客户，并通过先进的技术和分析，迅速对报告的诈骗予以应对。此外，商户收单机构必须在入网流程中实施严格的尽职调查措施，并采用先进的诈骗检测和监控工具，以防止假冒或串通的商户从诈骗中获利。

加密货币行业

随着数字资产的日益普及，加密货币行业的角色正在扩展。加密货币通常用于延续诈骗行为，2021 年至 2023 年间，诈骗分子将约 750 亿美元的诈骗收益转移到了加密货币交易所¹⁵。为打击诈骗分子利用加密货币（具有快速性和匿名性）的行为，交易所和钱包提供商应加强“了解你的客户”（KYC）和反洗钱（AML）举措，并对加密货币转账实施强有力的控制。

基础设施提供商

电信企业提供的基础设施为许多诈骗行为提供了渠道（例如，利用电话和短信），因此，这些企业的联手合作对于识别和阻止诈骗通信至关重要。

技术平台

随着技术和社交媒体的加速发展，诈骗案件的数量激增，诈骗分子可通过网络钓鱼、虚假个人资料和误导性广告来欺骗用户。实施主动监控、通过诈骗内容检测和删除流程进行早期干预，以及为用户提供相关教育等举措是至关重要的。

商户

线上和线下商户每天都需要直接与消费者进行交互并开展交易。当有人报告诈骗交易时，它们可通过确保客户旅程安全、使用强大的身份验证工具，以及与金融机构合作，发挥至关重要的作用。

支付网络

支付网络在处理交易和维护金融生态圈安全方面发挥着关键作用。它们与金融机构、行业合作伙伴和执法部门密切合作，采取相应措施检测诈骗行为并减轻其影响（包括阻止可疑交易活动）。

监管机构和执法部门

政府和监管机构负责制定防诈骗政策和框架，确保通过强有力的法律和监管规定来保护金融生态圈。执法部门负责调查诈骗活动并提起诉讼，确保不法分子被追究责任。他们通常与国内外其他利益相关者开展合作。

消费者

归根结底，消费者是金融生态圈的核心，他们既是诈骗的主要对象，也是防范诈骗的关键参与者。作为防范诈骗的第一道防线，消费者需要保持警惕并做出清醒决策，通过了解常见的诈骗伎俩和报告可疑活动来保护自己。

¹⁵ Griffin, J. M., & Mei, K. (2024). 《Crypto Flows 平台如何助长“奴役”现象？杀猪盘经济学》。SSRN.

反诈骗框架如何明确责任与问责制？

在关于如何有效解决诈骗问题的持续讨论中，责任与问责制是核心主题。就诈骗行为而言，责任是指针对损害进行赔偿的法律义务，通常要求责任实体对受害者遭受的损失予以赔偿。问责是指这些实体有义务采取有效措施来防止诈骗，并确保遵守监管要求。监管机构以保护消费者为目标而设计责任框架，并试图在多个相关方之间划分诈骗责任。

根据分析，有多个司法管辖区建立了明确责任与问责制的监管框架，以帮助有效应对诈骗问题。本章将对英国、新加坡、澳大利亚和台湾（因各自的积极监管措施而被选定）制定的监管框架进行非全面比较分析。如附录1中的概述所示，每个司法管辖区都规定了责任实体必须履行的具体反诈骗义务。尽管这些框架的范围和适用性各不相同，但它们的主要目标都是明确责任、确保落实问责，并保护消费者，防止其遭受诈骗损害。

关键要素包括：

- **责任：** PSP 须向受害者做出赔偿，赔偿金额不超过 85000 英镑（上限）。赔偿金可在发送 PSP（受害者的开户行）和接收（诈骗分子使用的收款银行）PSP 之间，按 50:50 的比例分摊。
- **问责：** 规定了 PSP 的赔付窗口期（五个工作日内）。发送 PSP 可延展五天的期限，以便收集信息，但赔付须于首次索赔起 35 个工作日内完成。
- **消费者保护：** 这一赔偿上限意味着，在 99.8%（按数量）或 90%（按金额）¹⁷ 的快速支付 APP 类诈骗案件中，受害者都将获得完全赔偿。强制性赔偿旨在激励 PSP 积极部署防范和检测措施，以保护消费者，防止其遭受 APP 诈骗。此外，《2024 年支付服务（修订）条例》¹⁸ 允许 PSP 在遭遇 APP 诈骗情况下，延迟将交易贷记至收款人的 PSP 账户。

英国的支付系统监管机构（PSR）颁布了新规则¹⁶，该规则自 2024 年 10 月起生效。根据该规则，对于授权推送支付（APP）类诈骗的受害者，支付服务提供商（PSP）须赔偿 100% 的损失（不超过 85000 英镑），除非受害者在相应案件中存在“重大过失”。

¹⁶ 支付系统监管机构（2024）。《面向 APP 诈骗受害者的开创性保护措施即日起实施》。

¹⁷ 支付系统监管机构（2024）。《APP 诈骗：赔偿上限——政策声明》。

¹⁸ 英国国家档案馆（2024）。《2024 年消费者保护（修订）条例》。

新加坡金融管理局（MAS）和资讯通信媒体发展管理局（IMDA）颁布了《共同责任框架指南》（SRF）¹⁹（自 2024 年 12 月生效）。该框架明确了诈骗（尤其是网络钓鱼诈骗）损失责任的划分。

关键要素包括：

- **责任：**成本分摊通过“瀑布式”方法而确定。负责的金融机构（为消费者开立付款账户）为第一顺位，若违反了义务，须赔偿受害者的全部损失。如果负责的金融机构已履行其义务，但电信企业尚未履行，则由电信企业承担全部损失。如果负责的金融机构和电信企业都履行了各自的义务，则由消费者承担全部损失。MAS 的《电子支付用户保护指南》（EUPG）²⁰ 于 2024 年 12 月生效。EUPG 规定了消费者在何种情况下必须或者无须为未经授权的交易造成的损失承担责任。SRF 和 EUPG 中的责任规定不适用于新加坡发行的信用卡、签账卡和借记卡的交易，相关规定见新加坡银行协会（ABS）《银行业务守则——信用卡》。
- **问责：**金融机构和电信企业必须实施 SRF 和 EUPG 中规定的反诈骗措施。EUPG 概述了金融机构和消费者对未经授权交易和错误交易的责任，以及金融机构针对这些交易造成的损失而应向消费者提供的基本保护。SRF 规定的金融机构职责源自 EUPG。电信企业必须实施身份验证措施和反诈骗短信过滤措施。
- **消费者保护：**SRF 和 EUPG 为明确消费者赔偿及责任提供了明确的框架，并提供了一套旨在简化消费者索赔的结构化流程。

澳大利亚财政部颁布了《反诈骗框架》（SPF）²¹（自 2025 年 1 月起生效）。该框架概述了各部门的义务。

关键要素包括：

- **责任：**银行、电信企业和数字平台提供商若未能履行各自的反诈骗义务，则须各自承担相应责任。该框架允许消费者在这些部门未履行各自义务的情况下寻求赔偿。澳大利亚金融投诉管理局将决定每个部门须承担的赔偿份额。
- **问责：**各实体必须遵守所属部门特定的反诈骗行为准则。财政部颁布的《反诈骗——强制性行业规范》²²（审核中，截至 2023 年 11 月）概述了具体义务。
- **消费者保护：**SPF 规定了受监管实体须履行的基本义务，以通过“预防、检测和打击”，保护消费者，防止其遭受诈骗。

¹⁹ 新加坡金融管理局（2024）。《共同责任框架指导方针》。

²⁰ 新加坡金融管理局（2024）。《电子支付用户保护指南》。

²¹ 澳大利亚财政部（2025）。发布内容。

²² 澳大利亚财政部（2023）。咨询结果。

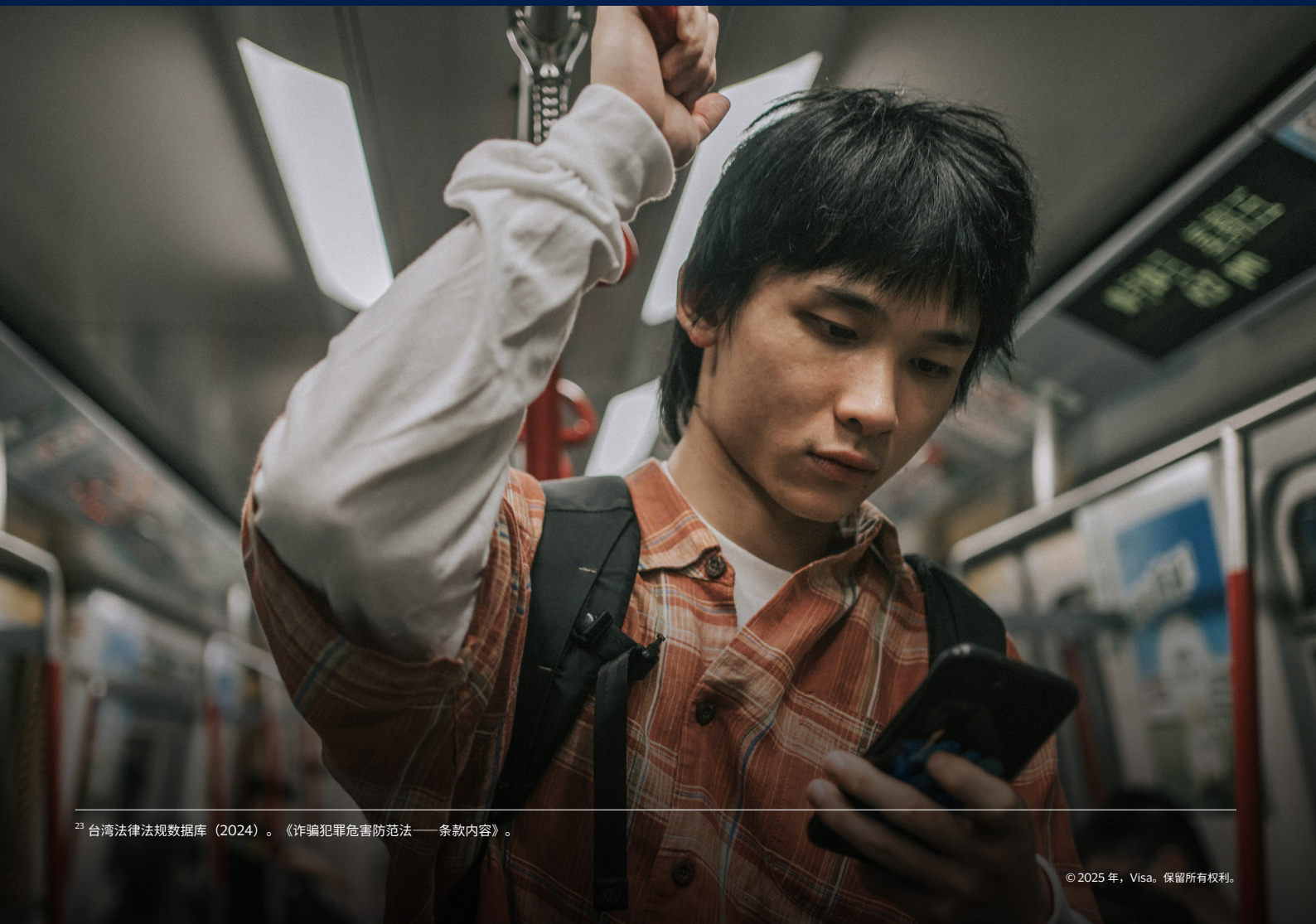
在台湾，为应对日益严重的数字金融犯罪，“内政部”于2024年7月颁布了《诈骗犯罪危害防范法》（FCHPA）²³。该法案适用于一系列行业，主要是在台湾大量投放线上广告的数字平台。

关键要素包括：

- **责任：**数字平台和诈骗广告商若未能履行各自的义务，则须承担连带责任。
- **问责：**金融机构、虚拟资产服务提供商（VASP）、电信企业、数字平台、电子商务商户和第三方支付服务提供商必须采取具体的反诈骗措施，若出现违规行为，则须接受处罚。
- **消费者保护：**该法案要求迅速采取行动删除诈骗广告、为广告商和赞助商制定信息披露和身份验证要求，并规定了诈骗防范计划和透明度报告义务。这些措施旨在防止诈骗广告的传播，强化台湾广告平台的问责制。

英国、新加坡、澳大利亚和台湾的监管框架代表了各自为应对日益严重的诈骗威胁而采取的多方面战略。这些框架为生态圈利益相关者设定了明确的期望，以强化其各自的反诈骗措施。尽管这四个框架的范围和适用性各不相同，但它们都旨在明确责任与问责制、加强消费者保护，并为受害者建立明确的追索途径。其他司法管辖区可借鉴这些方案，制定适合自身的反诈骗框架，以增强抵御诈骗的能力、保护消费者，并维护全球金融体系的完整性。

²³ 台湾法律法规数据库（2024）。《诈骗犯罪危害防范法——条款内容》。



利益相关者 如何应对诈骗？

通过研究英国、澳大利亚、新加坡和台湾建立的监管框架可见，问责制对于有效防范诈骗和减轻诈骗影响至关重要。这些框架的基石是利益相关者必须履行的反诈骗义务。

在亚太地区，许多国家尽管未建立正式的诈骗防范框架，但其监管机构和行业团体仍然积极实施打击诈骗的措施。在本章中，我们将深入探讨利益相关者承担的正式义务及其采取的行业主导的举措，这些举措可分为三个方面——身份验证、情报共享和提高消费者意识。我们将探讨这些举措如何增强诈骗防范，并确保协调应对（附录 2 载列了非详尽概述）。



身份验证

身份验证方法在打击诈骗方面发挥着至关重要的作用，它能够确保仅获得授权的个人才能访问和执行交易。在此过程中，务必要实行“智能摩擦”（smart friction）这一概念，因为它可引入足够的安全措施来验证合法性，而不至于给用户带来过重的负担。

安全的通信渠道

诈骗分子部署的一种常见诈骗方法是，使用与真正企业机构使用的字母数字发送者标识（发送者 ID）相同的标识，来伪装其向手机用户发送的短信。为应对这一问题，2022 年，新加坡资讯通信媒体发展管理局（IMDA）成立了新加坡短信发送者 ID 登记处（SSIR）²⁴，作为负责对在新加坡使用的发送者 ID 进行登记的中央机构。试图仿冒已登记发送者 ID 的短信将被预先拦截。2023 年 12 月，澳大利亚建立了类似的登记处²⁵。2025 年 1 月，印度储备银行（RBI）发布了关于防止使用语音通话和短信实施金融诈骗的规定²⁶。根据这些规定，受监管实体须使用中央数字情报平台（DIP）上的手机号码撤销列表（MNRL），对商业通话使用特定的系列编号，并采取其他反诈骗措施。随着短信钓鱼诈骗案件的数量激增，新加坡²⁷、马来西亚²⁸以及最近的泰国²⁹等亚太市场已禁止金融机构通过短信发送超链接。

适用范围：金融机构 / 电信企业 / 支付网络 / 商户

金融机构与电信企业的合作

令人关注的是，金融机构和电信企业等各个部门之间加强了合作，通过技术创新来打击诈骗。其部分原因在于，在诈骗案件中，这些部门往往交织在一起，促使它们采取更协调的应对措施予以解决。一则新闻报道，澳大利亚最大的电信企业之一 Telstra 与澳大利亚联邦银行（CBA）宣布了 Scam Indicator³⁰ 反诈骗合作计划，旨在检测和拦截手机上的可疑来电。之后，该计划的范围扩展至座机，以保护其最弱势的客户群。Westpac 和 Optus 公布了澳大利亚另一项反欺诈合作，双方共同为 Westpac 客户引入了应用内呼叫功能，以减少银行冒充类诈骗³¹。该解决方案标以 Westpac 品牌并经由 Optus 验证，可显示来电原因，从而更有效地确保合法性并降低冒充风险。

适用范围：金融机构 / 电信企业

²⁴ 新加坡资讯通信媒体发展管理局（2022）。《2023 年 1 月之前，须完成所有短信发送者 ID 的登记》。

²⁵ 澳大利亚通信与媒体管理局（2025）。《短信发送者 ID 登记处》。

²⁶ 印度储备银行（2025）。《防止使用语音通话和短信实施金融诈骗——监管规定和制度保障》。

²⁷ 新加坡金融管理局（2022）。《MAS 与 ABS 宣布了加强数字银行安全的措施》。

²⁸ 马来西亚国家银行（2023）。《2023 年年度报告》。

²⁹ 泰国国家报（2023）。《银行业与金融》。

³⁰ Telstra（2023）。《Telstra 与 CommBank 扩大合作，以提高诈骗检测率》。

³¹ 澳大利亚西太平洋银行（Westpac）（2024）。《Westpac SafeCall 将帮助客户轻松举报诈骗》。



数字身份

越来越多国家正在转而采用生物识别方法，因为它是一种更安全的身份验证形式。自 2018 年以来，新加坡采用了 Singpass 这套国家数字和生物识别系统，它允许用户访问政府数据源、公共服务和私人平台（包括设置银行账户和手机注册等金融服务）。除了共同责任框架之外，MAS 和 IMDA 正在探索更强大的带外身份验证解决方案——包括符合“线上快速身份验证”（FIDO）标准的令牌，以增强针对未经授权网络钓鱼交易的防御。澳大利亚政府还通过了《2024 年数字 ID 法案》³²，以建立一套国家数字 ID 系统，旨在为个人提供安全便捷的线上身份验证方式。

适用范围：金融机构 / 技术平台 / 商户

支付标记化

支付令牌是唯一的加密数字标识符，它取代了为完成电子商务交易而必须提供的卡详细信息，为消费者创造了安全性和便利性。在印度，支付标记化相关服务须凭借印度储备银行（RBI）颁发的授权³³而运营。在中国，香港金融管理局（HKMA）和证券及期货事务监察委员会（SFC）正在积极推动开发支付标记化和数字资产，推出了 Project Ensemble³⁴ 和数字债券资助计划³⁵ 等举措，同时还发布了关于支付标记化产品和虚拟资产的指导意见。台湾银行家协会于 2024 年发布了一系列关于设备钱包配置的自我监管指南。

适用范围：金融机构 / 商户 / 监管机构 / 行业团体

安全带外身份验证

短信已成为个人和企业普遍使用的交互工具，同时也无意中成为诈骗分子利用受害者的媒介。香港³⁶、新加坡³⁷ 和马来西亚³⁸ 等市场的主管机关一直在鼓励采用带外身份验证用户通过单独的安全渠道（例如，采用生物识别技术的手机应用，作为短信一次性密码的更安全替代方案）来进行交易验证。如果短信身份验证不可避免（例如，当消费者无法安装应用时），建议发卡机构加强对此类交易的监控。

适用范围：金融机构



³² 澳大利亚议会（2024）。《2024 年数字 ID 法案》。

³³ 印度储备银行（2021 年 2 月 5 日）。《主指令——非银行金融机构——住房金融公司（储备银行）指令》，2021 年。

³⁴ 香港金融管理局（2024）。《香港金管局推出 Project Ensemble，以支持香港支付标记化市场的发展》。

³⁵ 香港金融管理局（2024）。《香港金管局推出数字债券资助计划》。

³⁶ 香港金融管理局（2024）。《线上支付卡交易强化措施》。

³⁷ 新加坡金融管理局（2024）。《新加坡银行将加强对网络钓鱼诈骗的抵御能力》。

³⁸ 马来西亚通信与多媒体委员会（2024）。《马来西亚国家银行指示金融机构加强防范金融诈骗》。



情报共享

信息共享可显著提高实体检测和预防诈骗的能力。群体智慧有助于更快地识别新的诈骗伎俩，并让所有参与者都能采取预防措施。一项重要的全球举措是建立全球反诈骗联盟。该联盟的主要任务是召集各国政府、执法部门和行业合作伙伴交换信息，共同防止诈骗。该联盟创建了全球信号交换平台，用于分享有关诈骗的实时洞见和诈骗滥用数据³⁹。



数据交换

澳大利亚金融犯罪数据交换平台（AFCX）等独立的数据共享交换平台让行业实体能够以安全高效的方式，共享有关潜在诈骗的信息。新加坡的 ScamShield 平台⁴¹提供了一套产品和工具（包括一款应用和一个网站），以帮助公民识别和报告诈骗。

适用范围：金融机构 / 监管机构和执法部门

反诈骗中心

在地区层面，已有多个市场设立了反诈骗中心，包括香港（反诈骗协调中心）、新加坡（反诈骗指挥部）、马来西亚（国家诈骗应对中心）、澳大利亚（国家反诈骗中心）和台湾（警察局反诈骗小组），以促进私营部门、监管机构和执法部门之间的协作，共同应对威胁。2024 年 5 月，新加坡和马来西亚携手合作，追回了新加坡受害者汇入马来西亚银行账户的被骗资金⁴⁰。

行业论坛

除了正式的数据共享交换平台以外，行业论坛和协会在信息共享方面也发挥了至关重要的作用。这些论坛为各行各业的实体提供了分享见解、讨论新兴趋势和合作开发解决方案的机会。此外，它们在打击诈骗方面培养了群体意识和集体责任感。例如，澳大利亚银行协会（ABA）制定了《澳大利亚反诈安全协议》⁴²，该协议概述了打击、检测和应对诈骗活动的措施。

³⁹ 全球反诈骗联盟（2025）。《全球信号交换》。

⁴⁰ 海峡时报（2023）。《澳大利亚反诈骗框架》（SPF）“越来越多的国家建立了反诈骗中心；加强团队合作和应对速度对追回损失的资金至关重要”。

⁴¹ ScamShield（未注明）。<https://www.scamshield.gov.sg/>

⁴² 澳大利亚银行协会（2023）。《反诈安全协议》。

消费者意识

保持敏锐和警惕的公众仍然是防范诈骗的第一道防线。在披露个人凭证时，个人有直接责任检查网络卫生并加以辨别，以减轻诈骗风险。

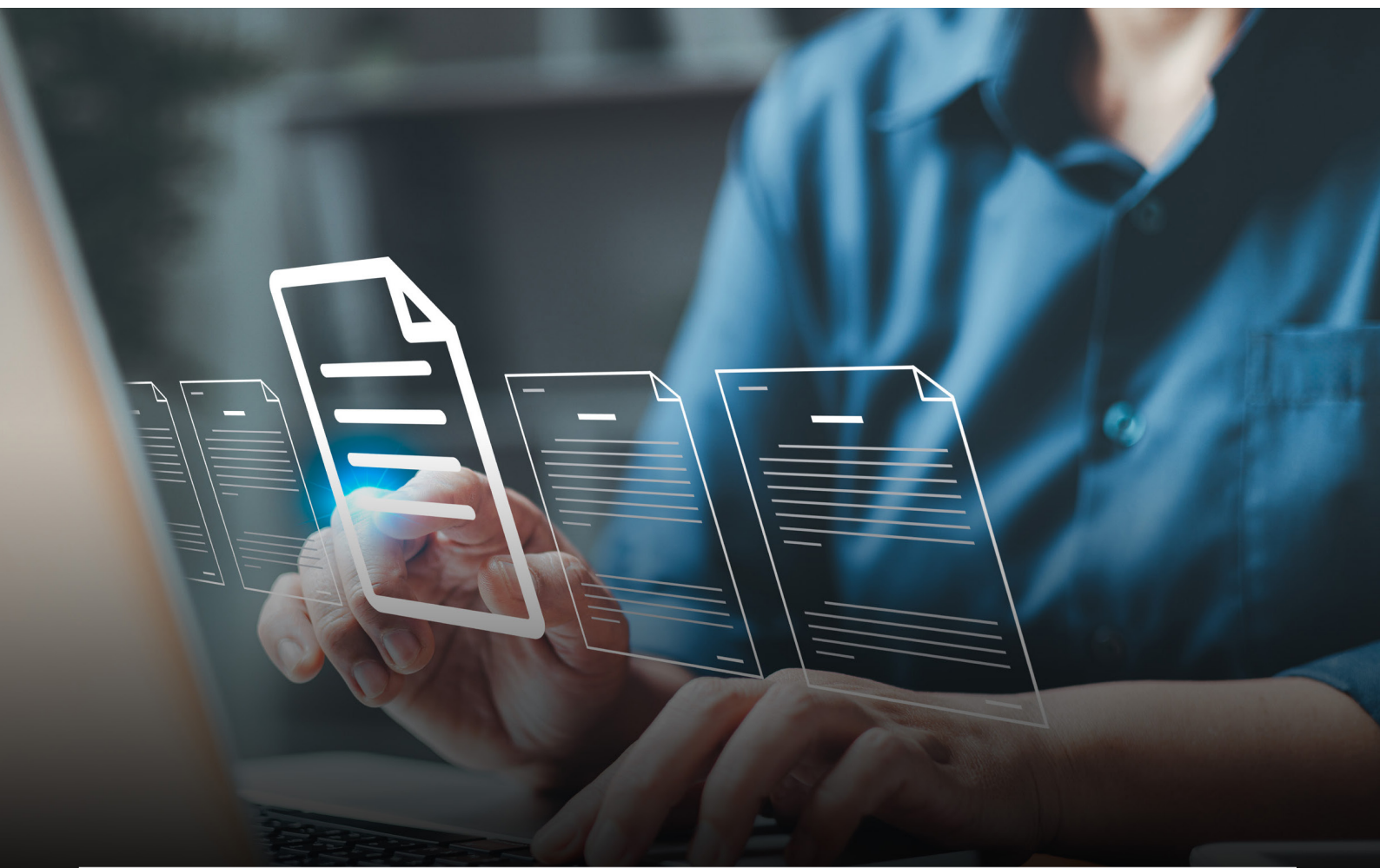
支付控制

用于管理卡安全功能的支付控制措施是重要的诈骗检测措施。MAS 要求银行实施交易警报和高风险交易警告——包括设置通知和在线转账的阈值、延迟新令牌激活，以及对重大账户变更实行冷静期。同样，澳大利亚《防诈安全协议》也建议部署卡控制措施——包括加强警告、采取延迟，以及对高风险渠道设定限制。卡控制措施越来越多地掌握在消费者手中，以便其更有力地控制自身安全。除了这些支付控制措施以外，该协议还要求客户通知须清晰地传递信息。

公共诈骗搜索引擎

银行和监管机构一直通过教育公众，帮助其了解诈骗的类型以及如何避免诈骗，强调消费者个人有责任对诈骗保持警惕。例如，香港 CyberDefender（“守网者”）开发“Scameter”搜索引擎，以帮助公众识别欺诈和诈骗。此外，另一款应用 Scameter+ 可用于检测消费者设备上可能与诈骗或欺诈有关的通话和网站⁴³。

适用范围：金融机构 / 监管机构和执法部门



⁴³ CyberDefender（未注明）。Scameter。https://cyberdefender.hk/en-us/scameter/



欺诈通常不分对象，但诈骗是针对个人的。这些诈骗直接影响受害者的生活，有时会造成毁灭性的影响。

Michael Jabbara

Visa 高级副总裁、全球金融生态圈风险与控制主管



Visa 内部举措

Visa 认为，行业共同提供防诈教育并帮助提高防诈意识，是防止消费者和企业成为诈骗受害者的关键。Visa 与客户密切合作，部署了一流的诈骗防控技术，并提供了消费者教育和生态圈意识方面的最佳实践，以帮助打击欺诈和诈骗。Visa 网络拥有 110 亿个端点，每年平均处理 2000 多亿笔交易，积累了独特而广泛的、反映诈骗趋势和来源的数据，并积极与全球各地的执法部门和行业团体开展合作，以实现情报共享。过去五年，Visa 在全球范围内投资了约 120 亿美元用于技术开发和创新，以阻止诈骗、保护商户和消费者，防止其遭受损失。具体而言，Visa 实施了多项策略和解决方案来管控诈骗：

Visa 打击诈骗实践

Visa 打击诈骗 (VSD) 实践⁴⁴ 于 2025 年 3 月公布，旨在解决 Visa 生态圈中针对消费者的诈骗。VSD 通过利用 Visa 的深厚专业知识、技术和合作伙伴关系，保护消费者、客户和企业：

- **诈骗情报：**VSD 汇集了一支跨学科团队，负责在各种诈骗中部署防控策略。除了聘请一流的工程师和 AI 开发人员之外，Visa 还重点招聘非传统反诈职业路径的人员，例如，前执法人员、前军职人员和数据可视化专家。
- **主动诈骗调查：**VSD 通过主动调查流程来防控诈骗，该流程利用多种渠道和方法，及时识别并解决诈骗，防止其对消费者造成毁灭性损失。
- **检测和打击诈骗：**VSD 利用尖端技术和广泛的专有网络级数据来分析和阻止诈骗。调查人员采用生成式 AI 工具，该工具能够进行相关性和图形分析，以识别复杂的关系，并解析大量数据，以识别真阳性、造成影响的诈骗活动。之后，Visa 与金融机构、执法部门和第三方合作伙伴合作，共同破坏诈骗网络基础设施。VSD 旨在通过与主要利益相关者合作，瓦解诈骗行为，防范未来的诈骗活动。

通过检测诈骗分子使用的伎俩、工具和基础设施，VSD 可从源头上瓦解诈骗活动。

适用范围：整个金融生态圈

⁴⁴ Visa (2025 年 3 月)。《Visa 公布打击诈骗实践，以帮助保护全球消费者和金融生态圈》。

Visa 账户对账户保护 (VPA2A)

Visa Protect 是一组风险评估和身份验证产品，旨在通过针对 Visa 网络内外交易的新型 AI 解决方案，保护消费者和企业。诈骗交易很可能是账户对账户交易。通过 Visa Protect，Visa 创建了一套名为“Visa 账户对账户保护”（VPA2A）的解决方案，可为金融机构提供实时风险评估功能，以便其分析欺诈和诈骗的可能性，从而在发送资金之前，做出明智的决策。评分利用了 Visa 专有模型、卡数据、本地实时支付网络数据，以及从全球诈骗趋势中吸取的经验。例如，Visa 在英国发布了 VPA2A⁴⁵，在之前的试用过程中，该解决方案成功检测到通过银行诈骗检测系统的 54% 的诈骗交易。此外，Visa 还针对阿根廷实时支付 (RTP) 生态圈，对 VPA2A 做出调整，并与处于阿根廷金融生态圈核心地位的 COELSA 技术公司共同推出新款 VPA2A⁴⁶。

适用范围：发卡机构

诈骗报告

根据要求，发卡机构须在 Visa Rail 上报告并标记诈骗，从长远来看，此做法将有助于改进解决方案和情报，从而使客户受益。Visa 提高了欺诈报告机制的精细化程度，以便更详细地报告诈骗行为，与一般的欺诈行为相区分。这有助于客户更清晰地了解不同的诈骗伎俩。Visa 观察到，最近几个季度，诈骗报告数量激增（同比增长三个百分位）。然而，我们认识到，这些报告并未全面捕捉到所有诈骗，要全面分析诈骗形势，还需发现更多的诈骗案例。

适用范围：发卡机构 / 收单机构 / 商户

Visa 支付威胁情报

Visa 支付威胁情报 (VPTI) 旨在提供一流的主动情报，将威胁情报与 Visa 的网络级数据相结合，生成关于特定行业或机构面临的关键威胁和威胁行为者的定制报告及洞见。VPTI 可提供有关商户或客户账户以及基础设施潜在违规的警报。此外，VPTI 还包括一个托管服务组件，由专门的风险分析师针对客户所在机构，提供特定的暗网情报和策略，以增强诈骗防范。

适用范围：发卡机构 / 收单机构 / 商户

⁴⁵ Visa (2024)。《Visa 针对账户对账户支付交易的保护》。英国案例研究。

⁴⁶ Visa (2024)。《Visa 利用人工智能，实时防范欺诈行为》。



支付标记化

2023 年，由于采用了 Visa 令牌服务（VTS），亚太地区的数字经济规模增长了 20 多亿美元⁴⁷，整个亚太地区的令牌渗透率接近临界点。VTS 将 16 位借记卡或信用卡号码替换为唯一标识符——即只有 Visa 才能解锁的“令牌”。Visa 令牌旨在保护支付凭证、实现增强数据的传输，从而帮助提高支付成功率并降低诈骗率。令牌的这些优势及其跨设备的易用性可改善消费者体验。令牌还可增强对每笔交易的控制，使数据交换丰富化，从而改进对支付交易的处理。这些改进减少了合法交易被支付系统拒绝的情况，从而避免给消费者和商户带来沮丧的体验。通过采用 VTS 处理数字支付交易，商户的支付成功率得到提高，支付诈骗率降低了一半以上（58%）⁴⁸。

适用范围：整个金融生态圈

Visa 规则

基于 Visa 的规则体系⁴⁹（《Visa 核心规则》和《Visa 产品与服务规则》，统称为“Visa 规则”），我们得以始终如一地确保用户安全、可靠地访问我们覆盖全球的网络。Visa 规则支持用户使用 Visa 产品及服务并利用其实施创新，同时也代表了 Visa 与其客户之间达成的具有约束力的合约。这些规则以全球原则为依据，并根据具体国家和地区的特定法规而做出适当调整，旨在最大程度地降低风险。这使得持卡人、商户、发卡机构和收单机构能够高效可靠地进行交易，而无需分别进行相互审查。Visa 规则专门分发给客户，以便其管理各自的 Visa 计划，确保整个金融生态圈的信息平等。这些规则用于规约用户对系统的使用和访问，为参与权、交易要求、风险和安全控制以及争议解决流程设置参数，以保护网络中的参与者。Visa 规则为客户在系统中的义务和职责（包括与结算程序、责任、交易争议和违约事件相关的义务和职责）提供了高度的法律确定性。

⁴⁷ Visa (2023 年 10 月 5 日) Visa 支付标记化使亚太地区的数字经济规模增长 20 亿美元

⁴⁸ Visa 风险部，2022 财年第一季度至第四季度全球各国每月 CNP 令牌交易超过 1000 笔的商户的令牌诈骗率与 PAN 诈骗率（按 PV）。商户的个体结果可能有所不同。

⁴⁹ Visa (2024)。《Visa 核心规则》和《Visa 产品与服务规则》。

结论

诈骗是一种普遍存在且不断演变的威胁，对全球各地的个人、企业和经济都造成影响。随着诈骗的日益复杂化，尤其是随着 AI 的应用，我们亟需采取一套面向整个生态圈的全局性解决方案。

本白皮书所述的见解反映了金融实体、基础设施提供商、社交媒体平台、支付网络、监管机构和执法部门以及消费者等各个利益相关者所发挥的关键作用。其中每个利益相关者分别承担特定的义务和职责，这对于建立具有韧性的诈骗防御机制至关重要。

英国、新加坡、澳大利亚和台湾等不同司法管辖区的反诈骗监管框架为有效应对诈骗提供了宝贵的经验教训。这些框架强调了界定责任与问责制的重要性，以保护消费者。其他地区可借鉴这些不同的方案，制定适合自身的反诈骗策略，以增强抵御诈骗的能力，保护消费者。附录 3 和附录 4 概述了针对新加坡和澳大利亚诈骗环境以及这些市场采取的反诈骗策略的案例研究。

尽管如此，仅履行这些义务并不足以免除利益相关者的职责。建立一套全面的、分层的方案——包括金融生态圈中所有参与者之间开展合作、持续改进防诈骗技术、积极地向消费者提供相关教育，对于建立具有韧性的诈骗抵御机制至关重要。

从身份验证、情报共享到监管框架，并不存在适合所有诈骗的单一解决方案。从根本上而言，利益相关者需要通过国内和国际合作，最大程度地减轻诈骗对社会的影响，确保为所有人提供安全的环境。Visa 致力于协助金融生态圈实现这一愿景，确保在整个过程中提供强有力的保护。通过共同努力、持续保持警惕和采取积极措施，我们可以共同建立一个更强大、更安全的防御体系，以应对不断变化的诈骗威胁。随着我们进入代理型商务的新领域，代理型 AI 有望通过专业模型网络，实时自主检测、应对和缓解诈骗威胁，从而彻底改变反诈骗策略。当下，我们亟需为这个新的代理型商务时代做好准备，帮助金融生态圈进一步为所有人提供更高的可靠性和安全性。



附录 1：反诈骗监管框架

方面	英国	新加坡	澳大利亚	台湾
框架名称	快速支付授权推送支付（APP）类诈骗赔偿要求	共同责任框架指南（SRF）	防诈骗框架（SPF）	诈骗犯罪危害预防法（FCHPA）
监管机构	支付系统监管机构（PSR）	新加坡金融管理局（MAS）和资讯通信媒体发展管理局（IMDA）	财政部、澳大利亚竞争与消费者委员会（ACCC）	“内政部”、“金融监督委员会”、“数字事务部”、“国家通信委员会”
生效日	2024 年 10 月	2024 年 12 月	2025 年 1 月	2024 年 7 月
对诈骗的界定	APP 诈骗是指受害者授权向其认为合法但实际上由诈骗分子控制的收款人账户进行付款。	诈骗是指犯罪分子诱使消费者付款或提供个人信息的、看似授权的交易。	诈骗是指诈骗分子试图诱使消费者使用受监管的服务，向诈骗分子付款或提供个人信息——无论是否成功、是否造成损失。	参考《刑法》第 43 条、第 44 条和第 339-4 条。
范围（覆盖面）	涵盖在快速支付和清算所自动支付系统（CHAPS）上处理的 APP 诈骗。	涵盖一些存在数字关联（即诱使消费者点击网络钓鱼链接并在虚假数字平台上输入凭据，因而能够从账户进行未经授权的交易）和新加坡关联的网络钓鱼诈骗。	涵盖所有被划入 SPF 定义范围的诈骗。不包括在无消费者操作的情况下不当得利的诈骗、网络犯罪、涉及缺陷产品的交易，以及在逼近的暴力威胁下进行的交易。	涵盖有组织诈骗、冒充诈骗和数字诈骗。
范围（适用性）	适用于英国的所有支付服务提供商（PSP），包括使用快速支付系统（FPS）或 CHAPS 的支付服务提供商。	适用于新加坡的金融机构和电信企业，涵盖一些看似有消费者授权的交易。	初始发布版本适用于银行、电信企业和数字平台，适用于其他行业的版本预计于日后发布。	适用于金融机构、虚拟资产服务提供商（VASP）、电信企业、数字平台、电子商务商户和第三方支付服务提供商。
责任方	PSP 有责任做出赔偿，除非发现消费者存在“重大过失”。	金融机构和电信企业若未能履行 SRF 规定的义务，则须承担责任。	银行、电信企业和数字平台提供商若未能履行 SPF 规定的义务，则须承担责任。	数字平台和线上广告商若未能履行 FCHPA 规定的义务，则须承担连带责任。
成本分摊	赔偿金可在发送 PSP（受害者的开户行）和接收（诈骗分子使用的收款银行）PSP 之间，按 50:50 的比例分摊。	损失的分摊基于金融机构和电信企业是否履行了各自的职责（“瀑布式”方法）。框架中概述了报告授权交易和损失分摊的详细工作流程。	通过对违规行为的民事处罚来强制履行义务，协作方案便于在不同部门之间分配职责（截至 2023 年 11 月，针对特定部门的法规仍在审核中）。	数字平台和线上广告商若未能履行各自的义务，则须承担连带责任。不合规的平台运营商还可能面临额外的流量管控、访问限制或者域拦截措施，以防止持续造成损害。
情报共享	消费者在提出索赔后，应按照 PSP 的要求，同意 PSP 代表消费者向警方报告，或者，PSP 可要求消费者直接向国家主管机关报告 APP 诈骗的具体情况。	金融机构和电信企业应共享与诈骗相关的信息，以降低风险。	要求企业与 ACCC 共享实用的诈骗情报，ACCC 会将其分发给其他企业、执法部门和国际合作伙伴，以便后者采取行动，共同防范、检测和打击诈骗。	金融机构和 VASP 须回应其他金融机构和准金融机构的探询，以防止欺诈和诈骗。
利益相关者的义务	- 在 5 个工作日内，向受害者做出赔偿，金额不超过 85000 英镑（上限，符合 FSCS 的规定）。 - 索赔金额不设下限，但 PSP 可自行确定索赔金额超过 100 欧元。 - 向消费者明确传达 APP 诈骗的风险，以及消费者根据赔偿政策而享有的权利。	- 金融机构和电信企业必须实施特定的保障措施，例如，诈骗监控、实时警报和短信反诈骗过滤。《电子支付用户保护指南》中规定了负责的金融机构和消费者的具体义务。 - 共享诈骗相关信息。 - 遵循诈骗报告流程。	- 遵守行业特定的行为准则。财政部《反诈骗——强制性行业规范》（截至 2023 年 11 月，仍在审核中）中概述了具体义务。 - 未能履行 SPF 规定义务的企业可能面临至高 5000 万澳元的罚款。	- 在收到执法部门通知后 24 小时内，强制删除诈骗广告。 - 实施稳健的身份验证措施。 - 加强广告中的信息披露。 - 制定并实施防诈骗计划，并发布年度防诈骗报告。 - 违规的金融机构和 VASP 可能面临至高 200 万元新台币的处罚。

附录 2：亚太地区部分市场的反诈骗对策 *

方面	主题	澳大利亚	香港	印度	印度尼西亚	日本	新西兰	新加坡	台湾
身份验证	安全带外身份验证	✓	✓	✓			✓	✓	
	多重身份验证	✓	✓	✓	✓		✓	✓	✓
	安全通信	✓		✓		✓	✓	✓	✓
	金融机构 - 电信企业协作	✓	✓					✓	
	数字身份	✓	✓	✓			✓	✓	
	支付标记化	✓	✓	✓	✓		✓	✓	
情报	反诈骗中心	✓	✓		✓		✓	✓	✓
	数据交换	✓	✓				✓ 试行	✓	✓
	行业论坛	✓	✓	✓	✓	✓	✓	✓	✓
消费者意识	支付控制	✓	✓	✓	✓		✓	✓	✓
	公共诈骗搜索引擎		✓						✓ 试行
	公共宣传活动	✓	✓	✓	✓	✓	✓	✓	✓
监管框架	责任 / 问责	✓					✓	✓	✓

*此列表是亚太地区部分市场实施的反诈骗应对措施（包括监管义务和 / 或行业倡议）的非详尽列表。

附录 3：新加坡案例研究

新加坡诈骗现状

在新加坡，诈骗已成为一个重大问题，受害者年损失金额创纪录，2024 年达到 11 亿新元⁵⁰。最常见的诈骗类型包括就业诈骗、电子商务诈骗、熟人诈骗和网络钓鱼诈骗。新加坡警察部队（SPF）报告称，2023 年，就业诈骗案件数量达到历史最高水平；2024 年，电子商务诈骗最为常见。诈骗分子通常通过消息平台、社交媒体、电话和线上购物平台与受害者联系——这些是诈骗分子最常使用的联系方式。

政府和行业对策

在新加坡，打击诈骗的方法⁵¹具有多层次、覆盖面广的特点，强调了消费者和行业利益相关者各自职责的重要性。就近期发展状况而言，新加坡政府一直强调采取生态圈全局化反诈骗方案的重要性，以促进多个政府机构以及私营部门实体之间的合作。同样重要的是，公众须保持清醒和警惕，这是共同打击诈骗的基础前提。新加坡采取三管齐下的策略打击诈骗——包括上游和下游措施，以及公众教育。

图 1：新加坡总体反诈骗策略（来源：新加坡金融管理局）



上游措施包括 ScamShield 手机应用和 SRF 等举措，下游措施包括银行保护措施和欺诈检测技术。公众教育工作侧重于社区赋权和消费者抗诈骗能力培训。这种多管齐下的方案旨在破坏诈骗活动、保护消费者，创建一个更具抗诈骗能力的新加坡。

国际合作

SPF 与马来西亚皇家警察和国际刑警组织（INTERPOL）等国外同行和合作伙伴密切合作，开展信息交换和联合调查及行动，共同打击跨国诈骗。例如，2024 年，在一起商业电子邮件泄露诈骗案中，SPF 反诈骗中心（ASC）与东帝汶主管机关和国际刑警组织合作，共同追回了 4000 多万美元（约 5300 万新元）的巨额损失。

⁵⁰ 新加坡警察部队（2024）。《年度诈骗和网络犯罪简报》。ScamShield。

⁵¹ 新加坡金融管理局（未注明）。《打击诈骗》。<https://www.mas.gov.sg/regulation/combating-scams>

附录 4：澳大利亚案例研究

澳大利亚诈骗现状

诈骗是澳大利亚面临的一个严重问题。虽然在澳大利亚所有卡欺诈类型中占比约 90% 的无卡欺诈（CNP）案件的数量于 2021 年至 2023 年间出现了强劲增长⁵²，但与诈骗相比，其数量仅占诈骗案件数量的四分之一⁵³。诈骗分子倾向于授权欺诈（诈骗），因为利用人际信任而获得的回报更高。根据澳大利亚金融犯罪数据交换平台（AFCX）截至 2022-23 财年末的数据⁵⁴，近一半的诈骗损失是通过加密货币交易所处理的。诈骗分子使用社交媒体、短信、电话、电子邮件和手机应用等各种渠道联系受害者。根据 2024 年关于诈骗活动的最新《反诈骗报告》⁵⁵，社交媒体是最常见的诈骗联系方式（总损失 6950 万澳元），而电话是给受害者造成实际损失最多（1.072 亿澳元）的诈骗联系方式。

政府和行业对策

澳大利亚政府和行业正在通过多方面的举措，应对诈骗案件数量增长的问题。澳大利亚竞争与消费者委员会（ACCC）等机构通过其 Scamwatch 平台，积极提供相关公众教育，并提供了诈骗报告机制。ACCC 还于 2023 年 7 月，建立了国家反诈骗中心（NASC）。澳大利亚证券投资委员会（ASIC）侧重于监管金融市场，并向消费者提供关于如何防范欺诈的教育。与此同时，澳大利亚网络安全中心（ACSC）加强了国家网络安全，为个人和企业提供了支持，并推动了网络事件的报告。这些机构以专题组和工作组的形式，根据相关政策共同开展合作，以阻止诈骗。

与此同时，各行业实体在反诈骗工作中，也发挥了至关重要的作用。金融机构部署了先进的诈骗检测系统，并积极开展教育活动，向客户宣传如何防范诈骗。电信企业使用技术拦截诈骗电话和短信，并与政府机构共同合作。零售和电子商务部门实施了安全支付系统和增强型客户身份验证流程。行业协会制定了最佳实践指南，并推动信息共享，而澳大利亚银行协会（ABA）《防诈安全协议》则体现了公私伙伴关系和跨行业合作的重要性，以进一步加强澳大利亚对诈骗的抵御能力。

国际合作

NASC 在网络犯罪联合警务协调中心安排了一名借调人员，并积极参与国际执法合作——包括参加 2024 年 3 月在伦敦举行的全球反诈骗峰会。2024 年 12 月，澳大利亚资讯通信媒体发展管理局（ACMA）和通信办公室（Ofcom）公布了一套新的务实合作框架，以推动互助和信息共享，实现消费者权益保护成果。根据该框架，澳大利亚和英国的通信监管机构之间签署了一份新协议，以联手打击电话诈骗、垃圾邮件和骚扰电话。此外，澳大利亚支付行业自律机构 AusPayNet 加入 GASA 并成为支持会员⁵⁶，旨在加强其国际合作和网络，打击诈骗和欺诈。

⁵² 澳大利亚支付网络（2023）。《2023 年诈骗统计数据》。

⁵³ 国家反诈骗中心（2023）。《2023 年反诈骗报告》。

⁵⁴ 澳大利亚的财政年度为 7 月 1 日至 6 月 30 日。

⁵⁵ 澳大利亚竞争与消费者委员会（2024）。《2024 年反诈骗报告》。

⁵⁶ 全球反诈骗联盟（2023）。《澳大利亚支付网络（AusPayNet）加入 GASA，成为支持会员》。



Visa 如何提供帮助？

有关更多信息，请访问 Visa [网站](#)，或者联系 Visa 亚太区风险团队：
[Wanjing Ji \(wji@visa.com\)](mailto:Wanjing.Ji@visa.com) 或者 [Jie Ying Tan \(jietan@visa.com\)](mailto:Jie.Ying.Tan@visa.com)。

