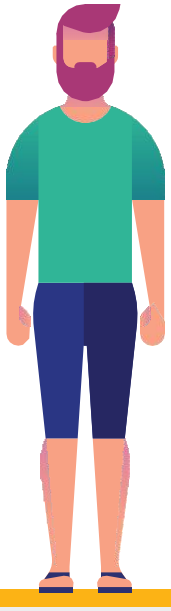
人工智能推进支付安全变革

VISA

目录



概要

在日新月异的支付行业，人工智能 (AI) 的发展影响深远，潜力巨大。它支撑起底层的安全架构，提供顺畅无阻、安全无忧的支付体验，满足消费者一直以来的期望。本报告将简要介绍人工智能如何推进支付安全格局的变革，以及Visa如何利用人工智能开发技术能力，助力合作伙伴优化决策制定，改善风控并确保支付安全，无需牺牲流畅无阻的顾客体验。

认识艾弗利

跟随艾弗利一起，看看人工智能是如何影响和改变他的日常生活的

人工智能简介

过去几十年间，技术创新主要集中于提升自动化程度和连接性，带来巨大的社会和经济利益。下一波技术变革将由人工智能 (AI) 推动，助力消费者更加轻松有效地开展各类日常活动，有望取得前所未有的成果。

人工智能对金融服务整体和支付服务这一细分类的潜在影响也同样显著。借助人工智能，支付能够超越单纯的交易范畴，变得更加自动化、互动化和个性化，并融入人们的日常体验，覆盖不同支付渠道和设备。然而，要实现这样的进步，我们必须具备与时俱进的安全架构，应对日新月异的支付安全威胁。

艾弗利在家登录线上商城选购书籍。在商品页面的“购买此商品的顾客也同时购买”标题下，他看到其他人的购买选择，于是将建议购买的书籍添加到购物车中。然后，艾弗利又登录视频平台，他的主页上有一个“为你推荐”版块，里面推荐的节目与艾弗利的喜好恰好相符。

人工智能的定义和应用场景

人工智能是一项有关计算机系统的理论和技术开发，目的是使用计算机系统完成通常只有人类才能胜任的任务。人工智能让机器从经验中学习，适应新的输入信息并模仿人类执行任务。人工智能的三大商业应用领域包括：**机器学习、自然语言处理和图像识别。**

机器学习

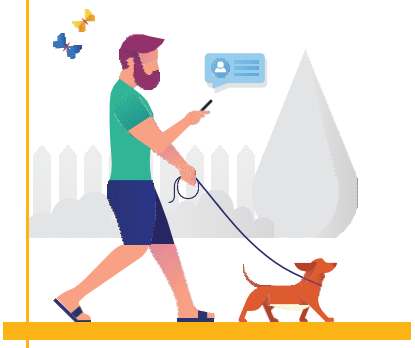
机器学习让机器从数据中反复学习如何执行一项特定任务，无需通过编程对机器提出指令。深度学习是机器学习的一个具体分类， 它的基础是人工神经网络，这种计算方法模仿了人脑形成突触连接解决问题的方式。

机器学习为银行提供了评估、批准和管理信贷申请的新方式。通过机器学习，银行可以利用电信账单和水电煤账单支付记录等非传统的数据点，为没有传统信用记录但信用良好的个人批准申请。这种应用场景有望覆盖17亿金融服务不足的人群，帮助他们接入正规的信贷网络。[1]

自然语言处理

自然语言处理 (NLP) 是指机器识别人类所说的话，将其转换为文字来理解内容，然后将文字输入到某一搜索机制中，最后向初始命令返回结果的整个过程。虚拟数字助理是自然语言处理应用中最为常见的一种。事实上，到2025年，虚拟数字助理的用户数量预计将增长至10亿以上。除了Amazon 的Alexa这样受到欢迎的数字助理，全球的银行也在为消费者提供聊天机器人服务，将客服体验数字化，在青睐"数字优先"的顾客面前脱颖而出。瑞典银行SEB Group推出了一个名为Aida的聊天机器人，它可以帮助银行顾客解决各种支付卡问题和帐户问题。除了为消费者提供易于使用的服务外， 到2022年，聊天机器人还有望每年为企业节省超过80亿美元。[2]

自然语言处理的应用远远不止聊天机器人。例如，应用注册流程往往过于繁琐，有25%的客户因为身份验证 (KYC) 不便而放弃使用应用程序。自然语言处理可以从应用程序中提取信息，帮助简化这种繁琐的注册流程，缩短注册用时。此外，自然语言处理还可用于自动归类文档，便于金融专业人士轻松确认是否已经获得KYC相关规定要求的所有具体信息。



艾弗利注意到自己的借记卡对帐单上有一笔不认识的交易。他轻松打开移动银行APP，与聊天机器人对话。不到30分钟，他的问题解决了。艾弗利很乐意使用银行提供的客服渠道，因为它易于访问又安全省时。

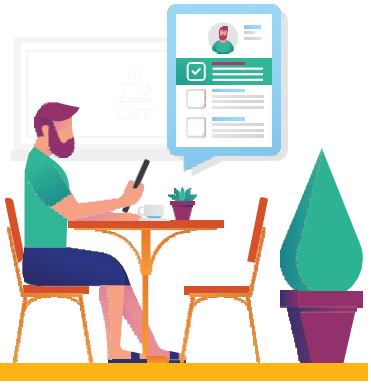
图像识别

图像识别利用人工智能识别地点、人物、标识、物体和建筑物。Amazon Go自动化零售体验就是这一技术应用的范例。 在Amazon Go商店内，顾客可以直接取走商品离开商店，不用等待结账。商店内部署了图像识别技术，可以检测商品何时被拿走或放回货架，并在顾客的虚拟购物车中追踪商品去向。就金融服务而言，发卡机构越来越多地使用人脸识别完成移动登录，大大缩短了用户访问帐户和完成银行业务所需的时间。

艾弗利登录自己的社交媒体帐号并将照片上传至相册。当他在照片中标记朋友时，社交媒体服务为他推荐照片中可以标记的人。如今，计算机视觉功能识别人脸的准确度已高达98%，与人类的能力不相上下，让艾弗利和有同样需求的用户在照片中准确快速地标记人像。[3]

Visa部署人工智能为支付安全保驾护航

Visa的AI解决方案旨在打造更加安全有保障的支付生态体系。正如Visa副总裁和人工智能专家Scott Boding所说："目前很多客户都是依靠人力完成欺诈检测，十分耗时；而我们尝试使用人工智能识别这些繁琐任务并实现自动化。我们希望利用人工智能帮助客户提高效率。"[4]



打造顺畅无阻、安全无忧的支付体验

账户注册

随着网络攻击范围的扩大，犯罪分子不断利用消费者数据伪造身份，实施欺诈。他们将真假信息混淆，创造新的身份，用于开设新账户并进行欺诈性消费和贷款。一项由Visa委托Forrester Consulting公司进行的研究发现，过去两年间，39%的全球受访企业经历过新帐户欺诈（例如使用窃取的身份信息开设欺诈帐户），同期有32%的全球受访企业经历过伪造身份欺诈。

为了帮助客户解决账户注册流程中的痛点，Visa开发了Visa高级身份识别解决方案(Visa Advanced Identity Solution, VAIS)。这项解决方案利用机器学习，分析欺诈活动在不同发卡机构间转移的模式和账户申请过程中是否有异常的身份信息使用。VAIS会生成风险评分，供发卡机构审核申请者时参考。它利用了发卡机构的Clearinghouse Service（清算所服务）数据，其中收集了某一特定消费者在所有发卡机构被批准或拒绝的申请、消费者提交申请的速度和其它相关数据。然后VAIS将这些数据整合，使用模式识别和机器智能创建动态的消费者画像，让大规模的实时申请审核成为可能。

艾弗利希望在新的发卡机构First Digital申请信用卡。这是他与这家发卡机构的首次互动，First Digital有机会提供流畅的账户申请和创建流程，赢得艾弗利这个顾客。通过机器学习模型分析传统数据和新型数据，First Digital能够了解艾弗利的个人信用度，并高效批准信用卡申请。

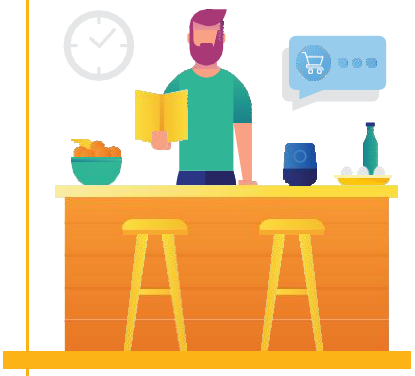
艾弗利申请信用卡时感觉流程快捷，且相对轻松。这是因为First Digital部署了人工智能技术，简化了被称为"顾客身份验证" (KYC) 的重要安全流程， 便于验证艾弗利的身份并评估与他的申请相关的所有潜在风险。

身份验证

随着企业与消费者的互动逐渐转向数字渠道，加上消费者越发期望获得顺畅无阻的体验，在数字环境下使用传统方式验证消费者身份变得困难重重。Visa委托Forrester Consulting公司进行的一项研究显示，34%的全球受访者表示，最终用户身份验证过于复杂是支付安全管理的关键挑战。企业必须简化消费者的身份验证流程，并投资使用正确的工具，从而准确判断用户是否使用了真实身份。这在欺诈手段日益纷繁的当今尤为重要：Forrester的这项研究还显示，32%的全球企业在过去两年间经历过帐户接管欺诈。

为了提供顺畅且安全的身份验证，企业采取了生物特征识别等各种身份验证方式。Visa Biometrics解决方案提供多因子 (multi-factor) 和带外 (out-of- band) 身份验证，消费者能够安全无缝地通过人脸、指纹和语音识别验证身份，免去输入PIN码和传统密码的麻烦。此外，这项生物特征识别方案采用先进的机器学习技术确认生物特征匹配结果，识别诱骗攻击，为顾客增加一层安全保障。

利用生物特征等其它数据元素可以更加准确地评估用户身份，而不会为流程增加不必要的障碍。Visa Consumer Authentication Service (VCAS) 利用帐户资料和地理位置等数据点支持发卡机构的身份验证策略，为每次身份验证请求评分。VCAS使用基于风险级别的身份验证，让发卡机构快速动态地评估交易风险，根据数据建模应用规则标准，并判断是否有足够信心在后台被动验证持卡人，还是需要持卡人更加主动地参与验证。在交易的另一端，商户可以使用Cardinal Consumer Authentication服务完成先进复杂、基于AI的异常监控和检测。加强商户和发卡机构之间的数据交换有助于逐步优化风险决策，减少消费者体验中的不畅感。 Visa利用人工智能开发安全的身份验证解决方案，助力合作伙伴成功应对日新月异的支付形势。



艾弗利去厨房准备晚餐，但发现忘买主要食材，于是他通过语音助手订购了食材。久而久之，语音助手记住了艾弗利的声音，能够根据声音特征识别他的身份。

交易授权

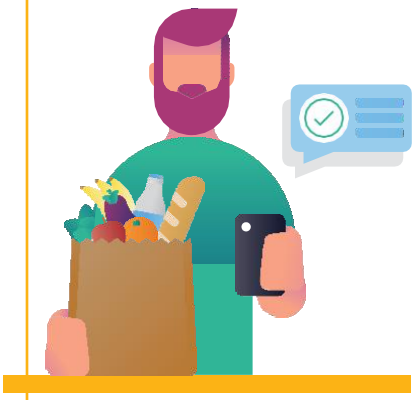
识别欺诈性交易时的误报是企业面临的一大障碍，这意味着他们经常无法区分合法交易和非法交易。在数字渠道下，风控既关乎实现规模销售，也关乎防范欺诈，误报问题也就显得尤为重要。2018年，全球有价值相当于2780亿美元的无卡交易被拒绝，年同比增长达27%[5]。人工智能可以分析海量交易数据，有助于更加精准地识别纷繁复杂的犯罪活动，最终帮助企业将误报率降至最低，批准更多的合法交易。

Visa利用人工智能的力量开发先进工具，保护持卡人免受欺诈侵害，让商户可以放心提交订单，让发卡机构在拒绝非法交易的同时批准合法交易。发卡机构可以利用Visa高级授权服务(Visa Advanced Authorization, VAA)。这项服务实时评估进入VisaNet的授权，帮助发卡机构及时识别和应对新兴欺诈模式和趋势。VAA使用先进的风险检测技术，评估所有进入Visa网络的Visa卡授权。在处理交易的过程中，VAA会给出风险评分，而发卡机构可以根据VAA评分在交易通过之前阻止潜在的欺诈损失。VAA已被全球129个国家和地区的8000多家发卡机构采用，仅2018年一年就阻止了约250亿美元的欺诈损失。[6]

与VAA功能相辅相成的是Visa策略管理（Visa Strategy Manager）解决方案。这项服务是利用算法，分析顾客的历史数据，识别在其他情况下可能漏网的欺诈账户和它们之间的关联性。然后这些算法会用于Visa Risk Manager——这是一项基于VisaNet的智能决策解决方案，帮助银行提高销售点的交易批准率，同时拒绝风险最高的交易。

为了支持和赋能广大商户的交易授权，Visa提供了CyberSource Decision Manager (CyberSource DM)解决方案。CyberSource DM中包含了260多个异常检测器和15个针对具体地区、渠道和行业的风险模型，每个模型都经过优化，能够识别不同场景下的欺诈行为。CyberSource DM还采用基于机器学习的实时融合建模 (real-time fusion modeling) 专利技术，实现欺诈防范功能。实时融合建模结合有效的传统静态模型和当下最为先进、数据分析能力更为敏捷的自主学习模型，帮助企业更加高效有力地管理和检测欺诈行为。

这些产品和服务为持卡人和消费者的交易增添一层安全保障，让发卡机构和商户更加放心。



艾弗利消费下单的体验十分轻松，如果这时发卡机构拒绝交易，他会十分失望。另一方面，如果发卡机构批准了欺诈性交易授权，艾弗利就不得不与发卡机构联系，对扣款提出争议——这样的体验也很令人沮丧。好在艾弗利的发卡机构使用先进算法对交易评分并判断风险，确认风险水平相对较低，于是批准支付。

利用网络安全服务保护支付生态体系

在高度互联的当今世界，滥用消费者信息和数据的方式也在不断翻新。2018年，网络犯罪的规模预估达到6000亿美元[7]，一次数据泄露的平均成本接近120万美元[8]。仅2018一年，全球就有27亿条记录被泄露[9]。鉴于这一问题影响广泛，消费者和企业都将网络安全放在首要位置。

人工智能能够帮助我们解决这一普遍问题。随着攻击手段不断翻新，企业必须适应变化，以灵活而动态的方式检测和阻止这些攻击。Visa深知战略制定需要与时俱进。我们已开发多种解决方案，让保护消费者和企业不再局限于交易层面。例如，基于AI的Visa Account Attack Intelligence解决方案将深度学习应用于经过VisaNet处理的海量Visa交易，识别网络犯罪分子在账户测试中利用了哪些发卡机构、商户和银行识别码 (BIN)，企图猜测卡片主账号 (PAN)、过期日期和CVV2码。机器学习技术可以检测复杂的账户枚举模式，消除误报，并在欺诈性交易发生之前提醒受影响的金融机构和商户。Visa致力于保护支付生态体系的完整性，保障持卡人信息安全——这一解决方案能够帮助我们成功实现目标。

“与时俱进”的欺诈分子如何利用人工智能

欺诈分子也在不断更新欺诈手段和攻击媒介，因此有可能利用人工智能，而不是仅仅使用简单的黑客技术。欺诈分子可以利用人工智能简化社交诈骗 (social engineering) 策略并优化逃脱网络安全检测的能力。此外，随着人工智能技术的进步，欺诈分子可以轻松（且廉价）地完成并行式和分布式攻击——只要具备随时可用的服务器和基本的编程技能。

就社交诈骗而言，欺诈分子会制作看似合法的视频、音频文件和电子邮件，目的是欺骗他人泄露信息。结果是，消费者可能点击非法链接，使得欺诈分子捕获他们的个人信息，或者以比现在更大的规模侵入原本仅限内部访问的企业IT系统。这一现象十分猖獗，全球有三分之一的公司曾受到社交诈骗的影响。[10]

欺诈分子还会将人工智能并与现有的恶意软件技术相结合，开发一系列难以对付的新兴恶意软件。一旦通过人脸识别、地理定位或语音识别确定目标，就会执行恶意操作；但在开展攻击之前，恶意软件只会潜伏在暗处。

应对这些潜在挑战的关键在于继续在整个生态体系内共享情报，合作制定战略，提供行业层面的解决方案。

应对这些潜在挑战的关键在于继续在整个生态体系内共享情报，合作制定战略，提供行业层面的解决方案。

趋势前瞻

人工智能对消费者生活的影响是变革性的。今天的AI和50年前诞生之初的AI看上去完全不同，而50年后的AI也会与今天的AI大相径庭。无论AI如何变化，不变的是消费者、商户和金融机构对安全和信赖的需求。目前大多数人工智能研究和应用程序专注于模式识别和声音识别，但在深度学习领域对交易数据（即时间序列数据）的研究较少。Visa将海量支付数据与尖端技术知识相结合，推进业界领先的深度学习研究，探索交易数据的应用。我们也因此取得多项解决方案专利，可以做到在几毫秒内完成大规模的深度学习应用。Visa将继续开发和部署强大的AI应用程序，加固安全保障基础，引领支付领域的深度学习应用。

Visa将继续开发和部署强大的AI应用程序，坚固安全保障基础，引领支付领域的深度学习应用。

作者简介

Michael Jabbara是Visa全球风控团队的高级总监，负责领导Visa的全球风控战略计划、执行和运营职能下开展的多项战略计划。他的电子邮箱是yjabbara@visa.com。

Sofia Katsaggelos是Visa商户销售与收单团队的业务拓展分析师。她的电子邮箱是sokatsag@visa.com。

鸣谢

本报告作者希望感谢众多Visa同僚提供的意见和见解，其中特别感谢Carolina Barcenas、Melyssa Barrett、David Capezza、Ann Ewing、David Henstock、Aruna Joshi、Andrew Naumann、Penny Lane、Tara Lavelle、Shane Malloy、John Zhan和Anna Wintle。

信息参考须知

1. 福布斯，《全球17亿成年人无银行账户》(1.7 Billion Adults Worldwide Do Not Have Access To A Bank Account)，2018年6月
2. Financial Brand，《认识银行业最有趣的11种聊天机器人》(Meet 11 of the Most Interesting Chatbots in Banking)，2018年3月
3. 财富，《Facebook的新算法：看不见脸也能认出你》(Facebook's new algorithm can recognize you even if your face is hidden)，2015年6月
4. PYMNTS.com，《VisaCyberSource：AI的作用是预测，不是晓知》(Visa CyberSource: AI's Role Is To Predict — Not to Know)，2019年5月
5. 排除因资金不足和发卡机构/交换机无法响应导致的交易拒绝。电商消费数据截至2018财年末，比较2017和2018财年的数据得出年同比增长比例。销售金额基于VisaNet授权数据得出。欺诈金额基于发卡机构报告的TC40数据（包括VisaNet以外渠道处理的交易）得出。
6. PYMNTS.com，《Visa Advanced Authorization 防范250亿美元的欺诈损失》(Visa Advanced Authorization Blocks $25 Billion in Fraud)，2019年6月
7. BusinessWire，《最新全球网络安全报告显示：网络犯罪造成全球经济近6000亿美元损失》(New Global Cybersecurity Report Reveals Cybercrime Takes Almost $600 Billion Toll on Global Economy)，2018年2月
8. 卡巴斯基实验室，《数据泄露的代价》(What is the Cost of a Data Breach)，2018年5月
9. BloomBlog，《2018：数据泄露之年》(2018: The Year of the Data Breach)，2018年12月
10. T-Systems，《社交诈骗》(Social Engineering)，2019年