遏制网络犯罪资金流动

以获利为目的的网络犯罪是一种全球性经济活动，造成了大多数网络安全和欺诈事件。所有反洗钱和金融业专业人士都应予以重视。这种网络犯罪适应性强、方式巧妙且有利可图，使我们损失巨大。它欺诈金融机构及其客户，并把我们的金融体系作为传输非法利润和支付款项的渠道。它的存在也为许多其他类型的网络犯罪提供了基础，包括黑客攻击和敌对国家攻击。

网络犯罪遍布全球，利用世界各地的公司和个人，伤害各个金融机构。因此，全球社会携手打击网络犯罪十分重要。美国金融业发达稳健，是网络犯罪有利可图的目标和渠道。

犯罪自文明诞生之时便存在，但网络犯罪是一个重大转变。以前，罪犯需要与受害人近距离接触；而现在，罪犯可以远距离甚至跨国危害机构和个人。这一转变意味着攻击者遍布全球，他们的被捕几率减小，盈利能力增加，并依靠金融业进行远距离犯罪。一直以来，执法行动有效打击犯罪行为，使犯罪活动控制一个可管理的水平，但对于网络犯罪它还没有达到同样的效果。这些都表明金融业可以在减少网络犯罪方面发挥重要作用。

网络犯罪的巨大盈利能力说明为之付出的代价之高和盗窃数量之大，但与此同时也带来了机会。执法部门和反洗钱界可以通过金融服务提供商“跟踪资金”，最终找到罪犯。此外，网络罪犯之所以采用这种方式欺诈，是因为其中有利可图。因此，找到一种减少利润流动的方法可以降低欺诈的盈利能力，从而减小犯罪经济的规模。

当异国网络罪犯进行网络犯罪和欺诈，使美国受害，代表非法利润的资金就通过美国金融体系到达系统外部，落入网络罪犯手中。要想侦查并遏制这一流动，必须了解网络犯罪和身份窃取经济（即参与者如何赚取金钱以及他们如何互相支付）。

网络犯罪和身份窃取经济

西部快捷国际洗钱案是首批探讨全球网络犯罪经济本质的刑事调查之一，数字货币兑换机构被指控贪污，其部分客户被指控是网络罪犯和身份窃贼。[1] 这个案例的经验依旧适用于今天，它告诉我们：

- 国际网络罪犯与国内身份窃贼的关系
- 被盗数据的交易市场以及用于何种犯罪
- 有助于贩卖被盗数据的价值转移方法
- 网络犯罪洗钱方法
- 网络罪犯和身份窃贼的匿名方法
- 揭露匿名的方法

成功的身份窃贼和网络罪犯擅长获得可观利润、实现匿名、逃避执法。但在获得利润的同时也暴露了有关犯罪和身份的证据。

减少网络犯罪和身份窃取经济的关键是理解它。该经济活动围绕数据盗窃、转售和使用，以达到身份窃取的目的。市场内有很多扮演不同角色的参与者，但所有人的目的都是赚钱。许多成功的参与者都利用国际平台，也就是说他们的网络犯罪需要依靠美国金融体系和美国参与者才能获利。

如何利用网络犯罪跨国获利

入侵电子邮件账户

入侵电子邮件账户是一种有利可图的网络欺诈，我们应该保护自己防止被骗。罪犯可能通过一个简单的方案，利用被入侵电子邮件账户获利。他们可能向受害者的所有邮箱联系人群发电子邮件：

“求助，我被困在［外国城市］，希望你能尽快给我汇点钱。

我手机丢了，电话联系不到我。”

[1] 调查和起诉持续了近 10 年，大多数被告认罪，三名选择庭审，控罪全部成立。见“Ukrainian Carder in $5 Million Ring Sentenced to 14-Plus Years in Prison, *WIRED*,”，2013 年 8 月 8 日，https://www.wired.com/2013/08/carder-eskalibur-sentenced/。

更大的威胁在于罪犯使用被入侵电子邮件帐户巧妙误导他人进行银行电汇并窃取资金。他们窃取了数以亿计的美元，代表了社会工程技术的进步。这种诈骗称为“商务电邮攻击”欺诈、“CEO 欺诈”或“CFO 欺诈”，每个金融业从业人员都必须了解。假设 A 公司定期收到 B 公司的发票，然后通过银行电汇付款。罪犯入侵 B 公司某员工的电子邮件帐户，冒充该员工向 A 公司发送电子邮件，提供“新的”银行电汇指示。A 公司的员工上当，于是 A 公司将资金汇至“新的”银行帐户，其实这是罪犯所控制的账户，资金立即被汇至国外。这种欺诈可能相当复杂且可信，形式多变，可以无须入侵电子邮件，还可以欺骗受害者长达几天或几周，从而延迟侦查。这种欺诈行为使用传统银行账户和银行电汇，窃取资金、洗钱并将资金转至国外，直接影响了传统的金融体系。

信用卡欺诈

信用卡欺诈需要许多参与者，各自在诈骗活动中扮演特定的角色，事成后分取报酬。如图 1，这种诈骗有三个基本步骤：

1. 窃取信用卡数据，如入侵零售商数据库
2. 将盗取的数据出售给身份窃贼
3. 使用被盗数据实施诈骗

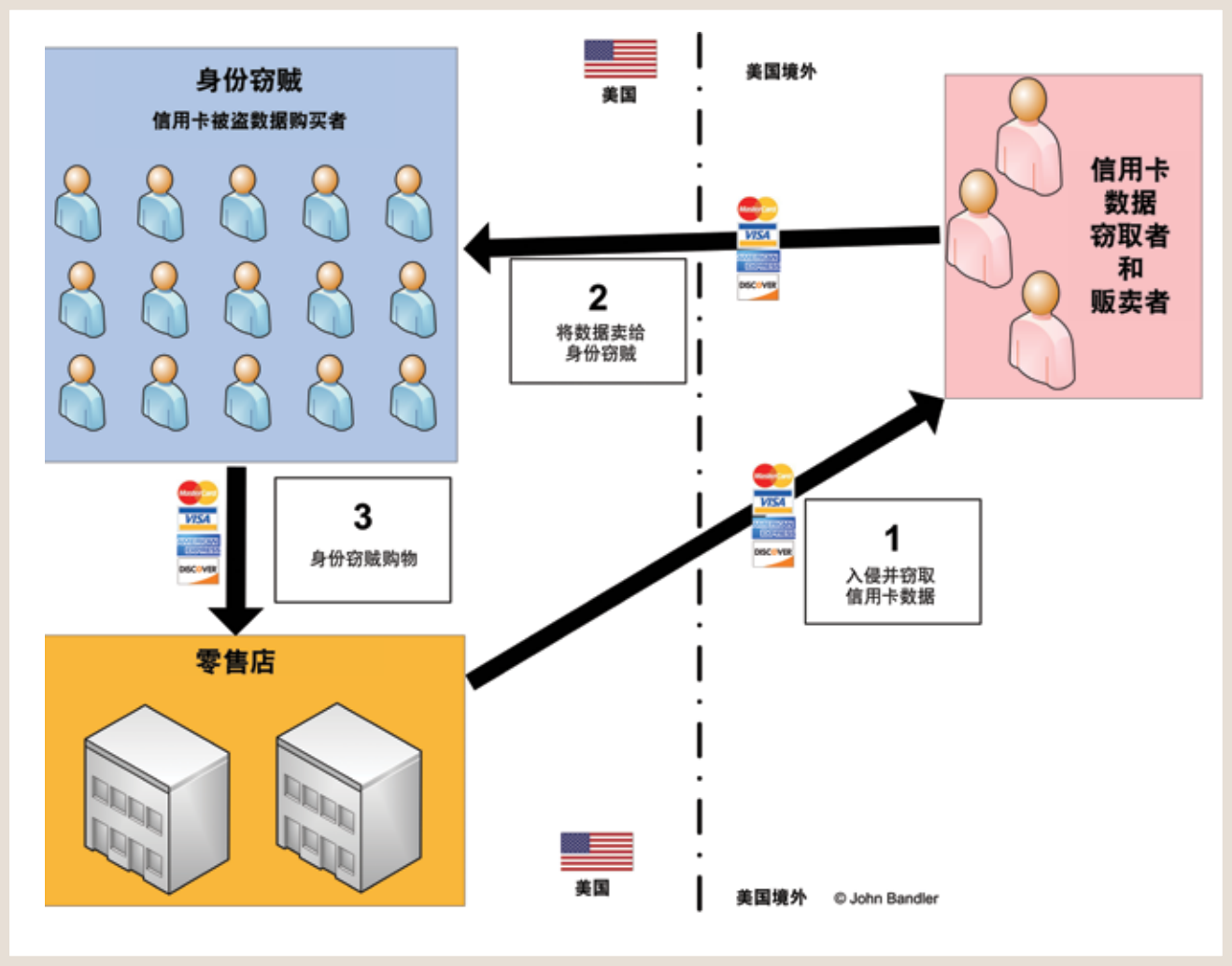

图 1：信用卡欺诈

此处所说的黑客位于美国境外，从美国零售商处窃取了数百万信用卡帐户的数据。窃取到的数据本身并不能给罪犯带来利益，所以他必须卖掉数据来赚钱。由于这些数据是从美国窃取的，因此最好跟美国的身份窃贼进行交易，因为在国外使用这些银行卡可能会触发欺诈警报。

身份窃贼以匿名方式购买被盗数据，每笔款项可能很小，几百或几千美元。付款可以采用转账服务，虚构付款人和收款人姓名，或使用比特币、WebMoney、Perfect Money 等数字货币。通过这样的方式，每个贩卖信用卡数据的供应商每年可以赚取数百万美元。

许多其他类型的网络犯罪诈骗也是一样，最终都需要美国国内人士向境外国际网络罪犯支付或转账。

转移资金

罪犯在付款和收款时也像合法商人一样试图平衡财务成本、便捷性、速度和可靠性，他们还需要匿名和保密。反洗钱专业人员应考虑网络罪犯用于转移资金的四种基本渠道：

- 传统金融体系的银行电汇
- 转账服务
- 数字货币
- 钱骡和空壳公司

自金融体系和支付方式产生以来，犯罪分子就一直在不当使用。网络罪犯会延续这种趋势，滥用任何可用的方式，这点不足为奇。

银行电汇

传统金融体系的银行电汇仍是全球资金转移的重要组成部分，对网络犯罪经济也至关重要。金融机构面临三重威胁：1) 他们一再受到攻击，成为欺诈或数据泄露受害者的风险大；2) 他们需要防止客户成为欺诈受害者；3) 他们需要防止自己在不知情的情况下被用作转移犯罪资金或进行犯罪活动的渠道。

有些银行电汇可能是欺诈引起的，包括上述入侵电子邮件帐户的情况。银行有检测客户账户是否遭受黑客攻击的程序，但有时还缺乏检测其他欺诈形式的程序。如果帐户持有人依赖于被入侵的第三方，或者帐户持有人以其他方式被欺骗或被用作网络犯罪欺诈的工具，银行可能无法发现。此外，银行的部分客户可能使用各种技术来掩盖资金的真正所有权、来源和目的地，包括通过钱骡账户和空壳公司。跟数字货币一样，银行电汇也扮演着重要角色。

转账服务

西联国际汇款公司等机构提供的转账服务是身份窃贼和网络罪犯的重要工具，因为他们可以通过转账购买被盗数据、进行网络犯罪服务，以及购买数字货币。为了保持匿名，付款和收款时他们会使用假名。每年赚取百万美元的网络罪犯可能会使用其他罪犯的服务来收款和转帐。收款人姓名偶尔会因为涉及犯罪行为而被冻结，在这种情况下，罪犯可以换一个收款人名字。

数字货币

数字货币二十年前就已经出现，网络罪犯和身份窃贼早已欣然应用。而数字货币受管制的历史仅有数年。尽管一些数字货币的倡导者敏感地认识到了其与网络犯罪的联系，但也应该承认和了解两者的协同作用。忽略了这一点，就是将行业置于危险之中，因为只有理解了这一点，才有可能使数字货币体系保持干净，从而确保数字货币成为可持续的受管制产业。

与犯罪的联系，并不是数字货币这种支付方式所独有的。想一想现金是如何与传统的街头犯罪交织在一起的，就像与毒品交易交织在一起那样。交易非法毒品时，犯罪交易是面对面的，毒品换取现金。成功的毒贩需要将大量现金纳入金融体系，为此他们制定复杂的洗钱机制。相比之下，网络犯罪和数据贩运犯罪交易在线完成，不适合用现金。付款要求在线、即时且匿名，以便将被盗数据交付给买方。数字货币可以做到这一点；因此，就像非法毒品交易用现金一样，网络犯罪经济用数字货币。对于反洗钱和执法专业人员来说，跟现金相比，数字货币有利有弊。

数字货币与传统银行和银行电汇有关。每个数字货币兑换商都需要一个传统银行帐户，而国际电汇十分必要，它用来传递资金，避免网络犯罪经济使用数字货币导致固有的贸易失衡。

数字货币会发生贸易失衡是因为美国内部的身份窃贼不断购买数字货币，用于向国际网络罪犯购买被盗数据。

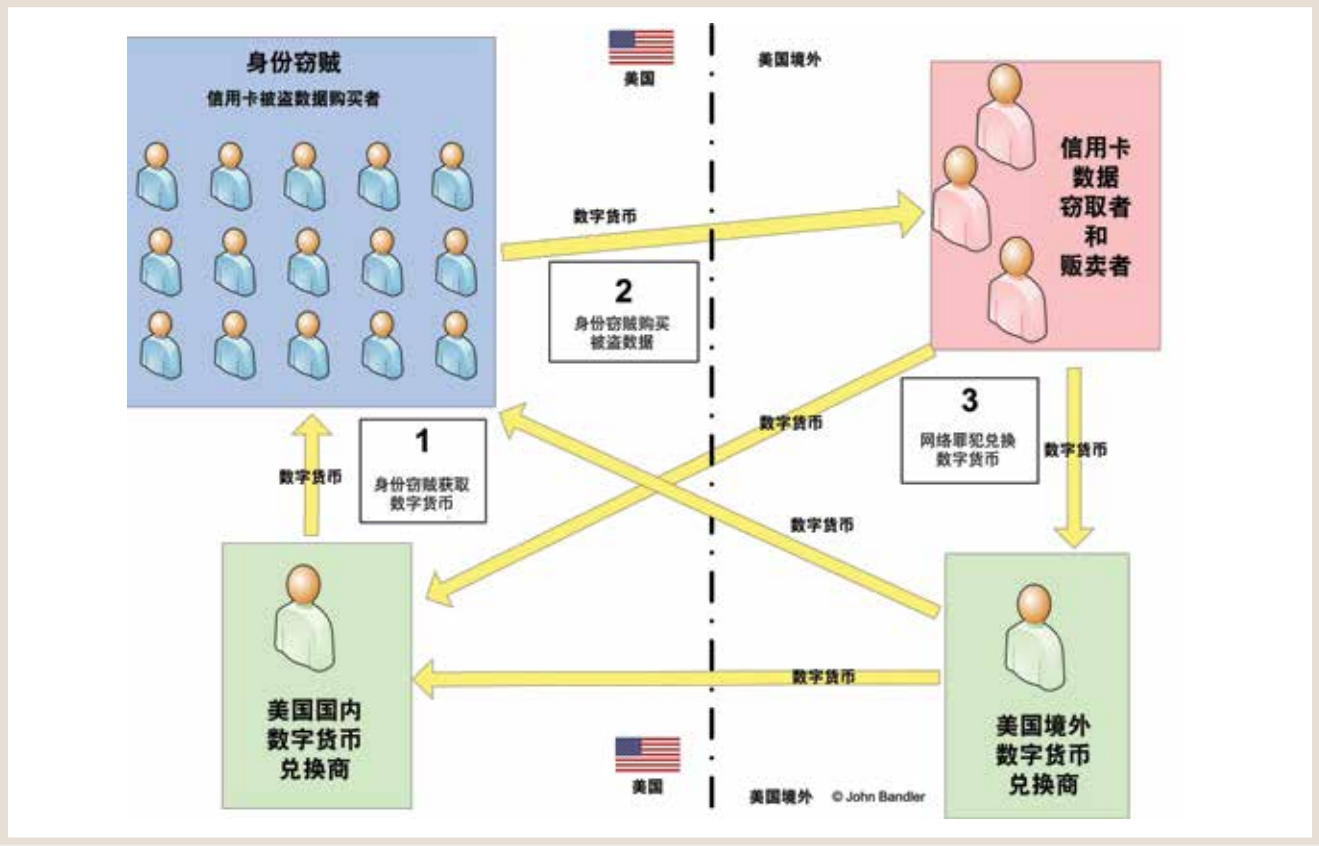

图 2：数字货币回流

这就造成了数字货币从美国到目的地国的持续流动，而这种数字货币最终需要被“送”回美国，这样就可以重新使用。

请看图 2 描述的基本步骤：

1. 身份窃贼获取数字货币

2. 身份窃贼向网络罪犯购买被盗数据

3. 网络罪犯用数字货币兑换法定货币

4. 重复——身份窃贼需要更多的数字货币来购买更多被盗数据

一个人可能支付了价值成百上千美元的数字货币。这就表示年度总流量达数百万美元。

此外，勒索软件欺诈有利可图、未受到制止，而且也依赖于数字货币，国际网络罪犯每年从中赚取数百万美元。勒索软件是一种恶意软件，感染用户的计算机，对其数据进行加密，再向用户索要赎金，直到受害人向其支付数字货币。成千上万的勒索软件受害者购买数字货币，支付给国际网络罪犯。

这些数字货币支付给国际网络罪犯造成贸易失衡，通过将数字货币送回美国才能重新平衡。数字货币回流可以通过数字货币的总交易实现，美国账户向国际账户进行银行电汇来换取数字货币。

钱骡和空壳公司

国际网络罪犯依靠美国国内机构进行收款和付款。盗取自美国受害者的资金最终要流向境外网络罪犯，钱骡提供一个便捷的中继站以传递资金。钱骡本质上是知情或不知情的接收并传输非法资金的人。

以前文提及的电子邮件帐户盗用诈骗为例，A 公司认为它将资金汇给了 B

公司的“新”帐户，但其实是在诈骗者的控制下汇给了钱骡的帐户。钱骡帐户在美国境内，于是A公司上当。如果A公司被告知进行国际汇款，他们就会知道这是一个骗局，因为B公司不会使用海外银行帐户。因此，国内钱骡帐户获得资金，再进行国际汇款。在骗局被发现之前，资金已经流出美国，无法挽回。有许多方法可以雇用钱骡，他们以看似合法的企业身份、网站和文档掩盖自己，有些粗糙，有些隐蔽。

虽然钱骡往往是“一次性”的（诈骗事件过后网络犯罪者不会再次使用），但是也有更长期的资金中继站。空壳公司（或空头公司）及其银行账户的设立和管理程序更多，因此不太会是一次性的。但两者的根本目的一致：隐藏帐户和真实拥有者的真正目的。一旦发现欺诈或洗钱，监管者和执法者很难确定欺诈行为的最终受益人。

每一个毫无防备的人都是供犯罪分子损害计算机或金融体系的途径

遏制网络犯罪资金流动

遏制网络犯罪资金流动需要重点关注以下几个方面：

- 个人网络安全和防范意识
- 加强金融体系的审查和监督
- 加强付款审查

个人网络安全和防范意识

网络安全和反欺诈不仅是专家的责任，也是个人的责任，就像系上安全带或晚上睡觉锁门。每一个毫无防备的人就是一条供犯罪分子损害计算机或金融体系的大道。网络安全和反欺诈需要从每一个人开始做起，保护个人和家庭，随后扩大到组织。每个人都可以从一个潜在的受害者变成检测传感器。

你应该采用基本的网络安全步骤保护自己：

- 金融、电子邮件和其他重要的在线帐户应使用双重认证（两步登录）
- 确保你的计算设备没有恶意软件并保持更新
- 定期备份数据并储存到离线设备上
- 不要打开可疑附件或点击可疑链接
- 收到任何付款指示后通过口头交流加以确认
- 运用常识

加强金融体系的审查和监督

金融体系面临之前讨论过的三重威胁，但由于拥有专门的知识和系统，而且能够访问重要数据库，所以有能力打击网络犯罪资金转移。金融体系是网络犯罪利润流出美国的最终管道，所以更深入的分析有助于识别犯罪。

网络罪犯将继续在美国民众中寻找受害者和钱骡，金融机构应运用自身在欺诈及洗钱检测方面的专业知识来识别这些情况，阻止非法资金流出美国。某些国家和银行更有可能接收到网络犯罪诈骗衍生的资金，但对于跟踪或收回被盗资金不予合作。汇到这些目的地国的款项应在汇款完成前仔细审查，因为一旦汇款便无法挽回。

加强付款审查

用于购买被盗数据的国际汇款遵循一定的模式，即使付款人和收款人使用假名。如果有足够的数据和经验，就可能区分违法支付和合法支付。同样，尽管很多数字货币账户可能是匿名的，通过分析付款仍可辨别犯罪目的。此外，数字货币回流至美国的模式也要加强研究。

根据美国对数字货币的监管，国内数字货币兑换机构必须“了解您的客户”(KYC)，这意味着身份窃贼可能倾向于使用国外的数字货币兑换机构。因此，国际汇款可能用于购买数字货币，这些模式也应当加以分析。

“了解您的客户”这种方法依赖于电话或在线身份验证，当碰到身份窃贼和罪犯的时候就暴露出内在弱点。这些罪犯几乎可以无限访问被盗个人的可识别信息，因此仅仅提供姓名、地址、出生日期和身份证件号码不足以确认身份。此外，如果支付公司识别出可疑活动，但只是阻止向一个非法账户汇款，罪犯另建一个便可。因此，可能还需要更深入的分析和更有效的补救办法。最后，必须考虑到这些罪犯能够伪造出以假乱真的身份证明，不管是网上还是当面出示。

结语

作为世界公民，我们为共同打击网络犯罪所付出的努力还不够，许多方面还需改进。金融界和反洗钱界应该认识到他们可以在这场战斗中发挥关键作用，并且应努力减少罪犯可以靠这些罪行获取的非法所得。

John Bandler 律师，CAMS，Bandler Law Firm PLLC 和 Bandler Group LLC 创始人，纽约州纽约市，johnbandler@bandlergroup.com