UNODC
Escritório das Nações Unidas
sobre Drogas e Crime

FRAUDE ORGANIZADA

DOCUMENTO TEMÁTICO

ESCRITÓRIO DAS NAÇÕES UNIDAS SOBRE DROGAS E CRIME

DOCUMENTO TEMÁTICO

FRAUDE ORGANIZADA

NAÇÕES UNIDAS
Viena, 2024

Agradecimentos

O presente documento foi preparado pela Seção de Apoio à Conferência, Divisão de Crime Organizado e Tráfico Ilícito, Divisão de Assuntos de Tratados do Escritório das Nações Unidas sobre Drogas e Crime (UNODC).

Pesquisa e elaboração

O presente artigo foi elaborado por Michael Skidmore, consultor. O UNODC gostaria de reconhecer as contribuições de Ramy Abdelhady, Victoria Luján Ecarri, Roxana-Andreea Mastor e Riikka Puttonen, da Seção de Apoio à Conferência, que contribuíram para o desenvolvimento do documento. O documento temático se beneficiou das valiosas contribuições de muitos membros da equipe do UNODC que revisaram e forneceram informações para várias seções, incluindo Loide Aryee, Renata Delgado-Schenk, Giovanni Gallo, Magdalena Howland, Theodore Leggett, Glen Prichard, Jason Reichelt, Tim Steele e Woody Tan.

Contribuições

Outros indivíduos e organizações contribuíram para a preparação do presente documento. O UNODC reconhece com profunda gratidão aqueles que compartilharam sua expertise e experiência durante a reunião internacional de especialistas realizada presencialmente em Viena e online de 4 a 6 de março de 2024: Jorij Abraham (Aliança Global Antifraude), Bina Bhardwa (Instituto de Pesquisa em Políticas de Crime e Justiça), Muhammad Bin Mohamed Farid (Singapura), Sebastian Bley (Agência da União Europeia para Cooperação Policial), Mark Button (Universidade de Portsmouth, Reino Unido da Grã-Bretanha e Irlanda do Norte), Mina Chiang (Consultoria em Pesquisa em Humanidade), Nicholas Court (Organização Internacional de Polícia Criminal (INTERPOL)), Ian Dyson (Reino Unido), Richard Goldberg (Estados Unidos da América), Cosmin-Adrian Iordache (Ministério Público Europeu), Eric Kasper (Consultoria em Pesquisa em Humanidade), Jeanette Kroes (INTERPOL), Dexter Laggui (Filipinas), Michael Levi (Universidade de Cardiff, Reino Unido), Nicholas Lord (Universidade de Manchester, Reino Unido), Mary Rose Magsaysay (Filipinas), Rafael Henrique Martins Fernandes (Brasil), Jennifer Mendez (Sociedade Americana de Direito Internacional), Daniel Mostardeiro Cola (Brasil), Olegs Olins (Letônia), Christopher Omahi Ogbaji (Nigéria), Sophia Rowe (Jamaica), Kien Soloman (Reino Unido), Victoria Ugo-Ali (Nigéria), Dan Joshua Valenton (Filipinas), Thomas Von der Gathen (Serviços de Pagamento da Áustria), Xiumei Wang (Universidade Normal de Pequim), Kathy Waters (Advocacia Contra Golpistas de Romance) e Robin Tim Weis (Projeto Zero).

A publicação do presente artigo foi apoiada por uma contribuição financeira do Governo do Reino Unido. O conteúdo do artigo é de responsabilidade exclusiva do UNODC e não reflete necessariamente as opiniões do Governo do Reino Unido.

Produção editorial: Seção de Publicações, Escritório das Nações Unidas em Viena.

CONTEÚDO

Introdução

A fraude evoluiu significativamente ao longo dos anos, adaptando-se aos avanços tecnológicos e às mudanças na sociedade. Tornou-se cada vez mais sofisticada, muitas vezes usando manipulação psicológica, possibilitada pelas tecnologias de informação e comunicação (TICs). O alto volume e a gravidade da fraude representam um risco significativo para as pessoas, economias e prosperidade em todo o mundo, e têm um impacto negativo na confiança do público no estado de direito. No entanto, desenvolver uma compreensão precisa da fraude apresenta vários desafios. As vítimas geralmente subnotificam a fraude devido a sentimentos de vergonha, autoculpa ou constrangimento, bem como à falta de reconhecimento de que um crime ocorreu.[1] Além disso, uma parcela significativa da fraude tem como alvo empresas, muitas das quais optam por não denunciar esses crimes para evitar prejudicar sua reputação.[2] O anonimato e o distanciamento frequentemente associados à perpetração de fraude ocultam as identidades dos infratores tanto das vítimas quanto das autoridades, dificultando os esforços para avaliar padrões subjacentes, fatores de vulnerabilidade e riscos associados. Além disso, a natureza dinâmica da fraude — que está constantemente sendo adaptada às mudanças nos sistemas legais, sociais, comerciais e tecnológicos — significa que métodos novos e inovadores do crime podem passar despercebidos dentro de dados oficiais estáticos. Em muitos casos, as entidades policiais nacionais não têm capacidade para investigar e descobrir os infratores e os grupos criminosos organizados por trás do crime:[3] É necessária a cooperação internacional, o que sugere a necessidade de dar maior destaque à fraude no quadro político e legislativo contra o crime organizado.[4]

A comunidade internacional reconheceu a escala preocupante da fraude e a necessidade de esforços conjuntos para preveni-la e combatê-la.[5] A Assembleia Geral, na sua resolução 78/229, reafirmou a importância do trabalho do Escritório das Nações Unidas sobre Drogas e Crime (UNODC) no cumprimento do seu mandato na prevenção ao crime e à justiça criminal, incluindo o fornecimento aos Estados-Membros, mediante solicitação e como uma questão de alta prioridade, de cooperação técnica, serviços de consultoria e outras formas de assistência, e a coordenação e complementação do trabalho de todos os órgãos e gabinetes relevantes e competentes das Nações Unidas no que diz respeito a todas as formas de crime organizado, incluindo fraude. No entanto, a intersecção entre fraude e crime organizado não é bem compreendida e é ainda mais complicada por sobreposições com outras áreas-chave, incluindo crimes cibernéticos, crimes de

1 Mark Button, Christopher Lewis eJacki Tapley, "Não éum crime sem vítimas: o impacto da fraude nas vítimas individuais enas suas famílias", Security Journal, vol. 27, No. 1 (fevereiro de 2014).

2 Cynthia Courtois e Yves Gendron, "Pesquisa: por que os relatórios de fraude corporativa estão em baixa", *Harvard Business Review,* 1º de julho de 2020.

3 A análise de dados criminais no Reino Unido da Grã-Bretanha e Irlanda do Norte explorou as ligações entre os delitos de fraude relatados pelo público e o crime organizado e estimou que pelo menos 31 por cento poderiam ser atribuídos ao crime organizado. Isso foi baseado em várias características, incluindo o envolvimento de co-infratores, reincidência, roubo de grandes quantias de dinheiro eonível de sofisticação (por exemplo, planejamento ou habilidade técnica). No entanto, a interpretação é desafiada pelas informações contextuais limitadas sobre os infratores e processos criminais subjacentes e pela falta de clareza conceitual para traçar linhas firmes em torno da fraude que pode ser atribuída ao crime organizado (veja Ruth Crocker e outros, The Impact of Organized Crime in Local Communities (Londres, The Police Foundation, 2017).

4 Hans-Jörg Albrecht, "Polícia, policiamento e crime organizado: lições da pesquisa sobre crime organizado", em *European Law Enforcement Research Bulletin, Edição Especial de Conferência n° 2, Detlef Nogala e outros, eds. (Luxemburgo, Serviço de Publicações da União Europeia, 2017); e Michael Levi, Ognian Shentov eBoyko Todorov, eds., Financing of Organised Crime (Sofia, Centro de Estudos da Democracia, 2015).*

5 Ver resoluções do Conselho Econômico e Social 2004/26, 2007/20, 2009/22, 2011/35 e 2013/39, sobre a cooperação internacional no domínio da prevenção, investigação, repressão e punição de fraudes econômicas e crimes relacionados à identidade.

colarinho branco, lavagem de dinheiro e corrupção.[6] Uma compreensão da fraude organizada é necessária para informar as decisões dos formuladores de políticas e outras partes interessadas e impulsionar respostas eficazes. A Convenção das Nações Unidas contra o Crime Organizado Transnacional, o principal instrumento global juridicamente vinculativo para prevenir e combater todas as formas e manifestações do crime organizado transnacional e proteger as vítimas, fornece uma estrutura para entender a natureza da fraude organizada e como a resposta a ela pode ser integrada à resposta às diferentes ameaças apresentadas pelo crime organizado transnacional.

Escopo do Documento Temático

Fraude é uma categoria expansiva de crime. Um dos maiores desafios para entendê-la é seu escopo. Ela abrange uma gama de comportamentos criminosos que são unidos pelo princípio comum da desonestidade. As oportunidades de empregar a desonestidade para fins de fraude abrangem toda a gama de cenários sociais, comerciais, financeiros e tecnológicos, que podem variar em diferentes regiões do mundo.[7] Essas oportunidades são exploradas por criminosos de origens altamente diversas, desde profissionais que exploram uma posição corporativa legítima até criminosos cibernéticos de comunidades carentes.[8] Dessa forma, a fraude é distinta de muitas outras categorias criminais que abrangem comportamentos criminosos mais discretos que ocorrem em cenários específicos (por exemplo, roubo). Essa diversidade cria desafios em termos de desenvolvimento de uma imagem única, coesa e abrangente da fraude.

O presente documento aborda fraudes perpetradas por grupos criminosos organizados (ou seja, fraude organizada). O papel do crime organizado pode variar dependendo do tipo de fraude, embora, em maior ou menor grau, tenha uma abrangência (*footprint*) em quase todos os tipos de fraude. Para fins de limitar o escopo do documento temático, os seguintes elementos não estão incluídos:

- Outros crimes em que a fraude desempenha um papel facilitador, incluindo o uso fraudulento de identidade para impedir que um perpetrador seja rastreado, como a abertura de contas financeiras para lavar o produto do crime;[9] comunicações fraudulentas para entrar em um relacionamento com uma vítima com o propósito de chantageá-la ou extorquir dinheiro[10] dela; e anúncios de emprego fraudulentos para recrutar e traficar vítimas para trabalho forçado e servidão.[11]
- Fraudes cujo alvo são os interesses financeiros do Estado (por exemplo, regimes fiscais), como a fraude intracomunitária do operador fictício (também conhecida como fraude MTIC ou fraude do IVA); fraudes de impostos especiais de consumo, em que os direitos sobre produtos importados não são pagos (por exemplo, combustível); fraudes em contratos públicos; e pedidos fraudulentos de subsídios[12] governamentais. O cenário de políticas e respostas para lidar com esses tipos de fraude pode ser distinto, sendo composto por várias agências e poderes regulatórios além da aplicação da lei (por exemplo, a autoridade fiscal).[13] As ligações entre esses tipos de fraude e o crime organizado estão mais bem estabelecidas na literatura.[14]

O foco do documento é a fraude organizada que tem como alvo membros individuais de instituições públicas ou privadas com o objetivo de obter benefícios financeiros ou materiais.

6 Jay S. Albanese, "Crime organizado como crime financeiro: a natureza do crime organizado refletida em processos e pesquisas", Victims and Offenders, vol. 16, No. 3 (2021); e Andrea Di Nicola, "Rumo ao crime organizado digital e à sociologia digital do crime organizado", Trends in Organized Crime (2022).
7 Michael Levi, "Fraude organizada e fraudes organizacionais: descompactando a pesquisa sobre redes e organização", Criminology and Criminal Justice, vol. 8, No. 4 (novembro de 2008). Veja também International Criminal Police Organization (INTERPOL), "INTERPOL global financial fraud assessment" (Lyon, França, 2024).
8 Veja, por exemplo, Arjan Reurink, *Financial Fraud: ALiterature Review,* MPIfG Discussion Paper, No. 16/5 (Colônia, Alemanha, Instituto Max Planck para o Estudo das Sociedades, 2016); e Mikol A. Mortley, "A crime of opportunity: an analysis of the Jamaican lottery scam" (Kingston, 2017).
9 Simon Baechler, "Fraude documental: a sua identidade estará segura no século XXI?", European Journal on Criminal Policy and Research, vol. 26, No. 3 (setembro de 2020).
10 Anna Coluccia e outros, "Golpes de romance online: dinâmica relacional e características psicológicas das vítimas e dos golpistas – uma revisão de escopo", Prática Clínica e Epidemiologia em Saúde Mental, vol. 16 (2020).
11 Relatório Global sobre Tráfico de Pessoas 2022 (publicação das Nações Unidas, 2022), p. 102. Para mais informações, consulte a seção sobre fraude no emprego no capítulo II do presente documento; e INTERPOL, "INTERPOL global financial fraud assessment", p. 20.
12 Shann Hulme, Emma Disley e Emma Louise Blondes, eds., Mapeando o risco de crimes graves e organizados se infiltrarem em empresas legítimas: Relatório final (Bruxelas, Serviço de Publicações, 2021); Agência da União Europeia para a Cooperação Policial (Europol), Avaliação da ameaça de crimes graves e organizados: Crime na era da tecnologia (Haia, 2017); e Europol, Esquemas de fraude online: uma rede de enganos, Série de relatórios Europol Spotlight (Luxemburgo, Serviço de Publicações da União Europeia, 2023).
13 Mark Button, David Shepherd e Dean Blackbourn, The Fraud "Justice Systems": Um estudo de escopo sobre os sistemas civis, regulatórios e caminhos privados para a "Justiça" para Fraudadores –Relatório Principal (Portsmouth, Reino Unido, Universidade de Portsmouth, 2016).
14 Hulme, Disley e Blondes, eds., Mapeando orisco de crimes graves e organizados.

Metodologia

Desenvolvendo uma tipologia

Há uma infinidade de princípios que podem ser adotados para representar as diferentes dimensões da fraude. Eles podem incluir os principais facilitadores técnicos ou criminais subjacentes que fornecem as ferramentas para perpetrar a fraude, por exemplo, os principais métodos para explorar canais de comunicação como telecomunicações ou publicidade online,[15] e processos de invasão, roubo de identidade ou engenharia social.[16] Organizar o conhecimento da fraude de acordo com esses princípios pode fornecer insights sobre os processos subjacentes que impulsionam o comportamento de fraude; no entanto, a visibilidade desses diferentes elementos pode ser limitada. Isso ocorre porque as vítimas que relatam os crimes geralmente não sabem como a fraude foi perpetrada.[17] Além disso, alguns facilitadores subjacentes impulsionam várias formas de crime; por exemplo, hacking e invasão de sistema podem ser precursores de fraude, mas também outras categorias de crimes (por exemplo, chantagem em ataques de ransomware).

As categorias de fraude desenvolvidas para o presente documento assumem uma perspectiva centrada na vítima e, portanto, têm um foco principal na narrativa ou estratagema que é apresentado às vítimas (por exemplo, o investimento ou romance). Neste contexto, o documento baseia-se em trabalhos anteriores que adotam princípios semelhantes para desenvolver uma tipologia de fraude com base nas vítimas e suas experiências, como uma tipologia para refletir a recompensa, benefício ou resultado esperado ou prometido da vítima a partir da comunicação fraudulenta.[18] Há convergências nos métodos subjacentes às categorias baseadas em vítimas, com semelhanças nas tecnologias e técnicas de engano usadas pelos infratores envolvidos nos diferentes tipos de fraude. Alguns criminosos podem se envolver em vários tipos de fraude como parte de um único esquema fraudulento ou empregar técnicas semelhantes para se envolver em diferentes tipos de esquemas fraudulentos.

Uma categoria incluída na tipologia é a fraude que tem como alvo empresas e organizações. Isso reflete uma categoria de vítima em vez de uma narrativa ou ardil específico e, portanto, incorpora diversos esquemas e métodos fraudulentos. Esses tipos de fraude foram consolidados para garantir que empresas e organizações sejam reconhecidas como um grupo-chave de vítimas.

Essas categorias são apresentadas como um passo inicial para desenvolver uma linguagem e entendimento comuns das diferentes categorias de fraude organizada. As categorias não são necessariamente reservadas a grupos criminosos organizados, mas cada categoria será discutida no contexto da fraude organizada. Algumas categorias são mais abrangentes do que outras, com uma infinidade de subcategorias, algumas das quais são discutidas de forma não exaustiva no documento temático.

---

15 Por exemplo, David Ng'ang'a Njuguna, John Kamau eDennis Kaburu, "Uma revisão das estratégias de mitigação de ataques de smishing", *International ournal of Computer and Information Technology, vol. 11, No. 1 (fevereiro de 2022); Jean-Loup Richet, "Como as comunidades cibercriminosas crescem e mudam: uma investigação de comunidades de fraude de anúncios", Technological Forecasting and Social Change, vol. 174, art. No. 121282 (janeiro de 2022); e Shadi Sadeghpour e Natalija Vlajic, "Anúncios e fraude: uma pesquisa abrangente sobre fraude em publicidade online", Journal of Cybersecurity and Privacy, vol. 1, No. 4 (dezembro de 2021).*

16 Jason RC Nurse, "Cybercrime and you: how criminals attack and the human factors that they seek to exploit", em The Oxford Handbook of Cyberpsychology, Alison Attrill-Smith eoutros, eds. (Oxford, Oxford University Press, 2019).

17 Mark Button eoutros, "Fraudes online: aprendendo com as vítimas por que elas caem nesses golpes", The Australian and New Zealand Journal of Criminology, vol. 47, No. 3 (dezembro de 2014).

18 O documento temático baseia-se em pesquisas anteriores que buscaram delinear as diferentes categorias de fraudes direcionadas a indivíduos e/ou empresas, como Michaela Beals, Marguerite DeLiema e Martha Deevy, "Framework for a taxonomy of fraud" (Stanford, Califórnia, Stanford Center on Longevity, 2015); e Michael Levi e John Burrows, "Measuring the impact of fraud in the UK: a conceptual and empirical journey", The British Journal of Criminology, vol. 48, No. 3 (maio de 2008).

Revisão da literatura

O presente documento apresenta uma pesquisa exploratória para examinar a natureza da fraude organizada conforme vivenciada em diferentes regiões do mundo. Ele contém uma compilação e revisão de informações de artigos de periódicos acadêmicos, documentos de políticas e publicações.

Uma busca de fontes on-line foi concluída para identificar publicações que abrangem infrações ou infratores de fraude organizada. O assunto de fraude organizada, ou crime organizado no contexto de fraude, recebeu cobertura limitada na literatura existente. O presente documento contém uma síntese de evidências coletadas em vários campos criminológicos relacionados, incluindo fraude, crime organizado e crime cibernético. O documento não contém uma revisão sistemática da literatura, mas é, em vez disso, uma análise direcionada da literatura principal com o objetivo de representar e ilustrar alguns dos temas essenciais.

Estudos de caso

Estudos de caso foram coletados para fornecer exemplos ilustrativos de fraude organizada em diferentes regiões do mundo e para capturar métodos e tecnologias novos e emergentes. Os estudos de caso foram retirados de uma variedade de fontes, incluindo o portal de gerenciamento de conhecimento *Sharing Electronic Resources and Laws on Crime (SHERLOC)*, artigos acadêmicos, relatórios de políticas e pesquisa jurídica.

Pesquisa preliminar sobre legislação de fraude em 37 países em todas as regiões do mundo foi realizada, com foco particular em definições e estruturas legais que orientam as decisões sobre sentenças para infratores condenados. Pode haver elementos de fraude na legislação de outros países que não são considerados aqui.

Limitações da revisão

Em muitas fontes oficiais e artigos de pesquisa, a fraude é examinada através das lentes da aplicação da lei e de dados oficiais. A fraude é amplamente subnotificada e, portanto, é necessário algum cuidado na interpretação do problema e no desenvolvimento de soluções com base em dados incompletos. O presente documento contém uma compilação de pesquisas de uma série de regiões, mas a disponibilidade foi variada e, em algumas regiões, a pesquisa foi mais limitada ou incipiente. Consequentemente, não se sabe até que ponto as evidências incluídas no artigo representam os padrões de fraude organizada em todas as regiões. Também há atualmente uma lacuna nos dados sobre fraude organizada desagregados por fatores como deficiência, idade, gênero e status econômico, o que limita a análise e a compreensão dos facilitadores da segmentação de vítimas e da perpetração da fraude organizada.

Estrutura do Documento Temático

O documento temático está estruturado da seguinte forma:

- O Capítulo I estabelece os princípios para a compreensão da fraude organizada, examinando a definição de fraude e aspectos-chave da Convenção sobre o Crime Organizado.
- O Capítulo II fornece uma tipologia de fraude organizada, com uma descrição aprofundada de cada categoria.
- O Capítulo III contém uma discussão sobre os criminosos de fraude organizada, examinando seus perfis e os caminhos que eles seguem para cometer crimes de fraude organizada.
- O Capítulo IV contém uma descrição dos facilitadores transversais da fraude, incluindo algumas das principais tecnologias e comportamentos que permitem a fraude organizada.
- O Capítulo V discute as respostas nacionais e internacionais, as principais considerações, as lacunas e áreas para melhorar a prevenção e a aplicação da lei.

CAPÍTULO I

Princípios para compreender a fraude organizada

Antes de focar na tipologia da fraude organizada, o presente capítulo aborda algumas considerações gerais em torno da definição de fraude, da Convenção sobre o Crime Organizado e da fraude no contexto do crime organizado.

Definindo fraude

Não há uma única compreensão definitiva dos comportamentos que compõem a fraude. Alguns definiram a fraude em termos muito amplos, por exemplo, "obter algo de valor ou evitar uma obrigação por meio de engano".[19] Outros forneceram definições mais elaboradas para descrever em termos mais específicos os comportamentos compostos que são representados pela fraude, incluindo o destaque da intenção proposital e da violação da confiança.[20] A INTERPOL enfatizou o elemento deliberado implícito no termo "engano", reforçando a importância da intenção na definição de fraude, e define fraude como o "objetivo de obtenção de ganho financeiro por meio de ações deliberadas e enganosas contra indivíduos e em seu detrimento".[21]

Da mesma forma, não existe uma definição legal única de fraude, e as definições variáveis entre jurisdições legais, ou em diferentes estatutos, evocam apenas um conceito amplo de fraude.[22] Nas leis criminais dos países, a fraude é descrita de diferentes maneiras e com diferentes graus de especificidade.[23] Algumas leis fornecem uma descrição generalizada dos comportamentos que constituem fraude[24], enquanto outras fazem referência a certas atividades, produtos ou serviços que são proeminentes em esquemas fraudulentos, como a representação de uma entidade confiável ou a manipulação ou uso não autorizado de dados.[25] Alguns Estados introduziram legislação separada para abordar diferentes facetas da infração de fraude, por exemplo, fraude informática ou fraude contra crédito, empresas e leilões.[26]

19 Grace Duffield e Peter Grabosky, The Psychology of Fraud, Trends and Issues in Crime and Criminal Justice Series, n.º 199 (Canberra, Instituto Australiano de Criminologia, 2001), p.1. Ver também Michael Levi, "Financial crimes", em Oxford Handbook of Crime and Public Policy, Michael Tonry, ed. (Nova Iorque, Oxford University Press, 2009), pp. 223–246.
20 Reurink, Fraude Financeira.
21 INTERPOL, "Avaliação global de fraude financeira da INTERPOL", p. 5.
22 Alan Doig, Fraude (Cullompton, Reino Unido, Willan, 2006); e Reurink, Fraude Financeira.
23 Para os propósitos do presente artigo, foram examinadas as definições legais em 37 países em todas as regiões do mundo.
24 Veja, por exemplo, os exemplos legislativos para Espanha e Uruguai incluídos na presente seção.
25 Por exemplo, na Argélia, a fraude é definida como o recebimento de dinheiro por meio da utilização de uma identidade falsa ou de nomes de terceiros, como autoridades, ou persuasão a um indivíduo de algo que não é verdade, como ganhar na loteria ou a ocorrência de um acidente.
26 Por exemplo, na República da Coreia, há uma legislação separada para fraudes que sejam prejudiciais ao crédito de outra pessoa e para fraudes por uso de computador (por exemplo, a inserção falsa de dados em fraudes de identidade).

Existem alguns elementos centrais de fraude que aparecem na maioria das definições legais: usar o engano para obter uma vantagem ou benefício injusto e causar um prejuízo a outra pessoa ou organização. O engano é descrito de várias maneiras como desonestidade, representação falsa (ou errônea), trapaça, artifício, manobras fraudulentas, abuso de confiança ou ocultação ou omissão de informações. O prejuízo a outro está, em muitos casos, implícito no benefício aos infratores, mas alguns destacam o prejuízo a outro usando termos como afetar ou prejudicar os interesses financeiros de outros, uma perda injusta ou ser fraudado. O prejuízo pode ser para um indivíduo, uma empresa ou um Estado.

As definições abaixo foram retiradas da Espanha e do Uruguai e fornecem exemplos de duas definições amplas de fraude que foram adotadas por lei.

EXEMPLO LEGISLATIVO: ESPANHA

LEI ORGÂNICA Nº 10/1995 – CÓDIGO PENAL

Artigo 248.1. Qualquer pessoa que, com intuito de lucro, usar de artifício suficiente para levar outra pessoa a praticar, por engano, ato de disposição prejudicial a si ou a outrem, será culpado de fraude.

EXEMPLO LEGISLATIVO: URUGUAI

CÓDIGO PENAL Nº 9155

Artigo 347. Qualquer pessoa que, por meio de artifício ou engano, enganar outra pessoa, a fim de obter para si ou para terceiro vantagem indevida, em detrimento de outrem, será punido com pena de prisão de seis meses a quatro anos.

No presente documento temático, uma definição ampla de fraude é adotada para abranger as variantes descritas nas leis de diferentes países. Inclui fraude que usa deliberadamente engano,[27] por qualquer método[28] ou meio[29], com a intenção de obter ganho financeiro ou outro ganho material ilícito,[30] e que cause prejuízo a outrem.[31]

Um último ponto a reconhecer na definição de fraude é a linha tênue que pode separar uma questão criminal de uma civil – particularmente em casos em que a intenção é difícil de discernir – e pode haver desafios para as entidades responsáveis pela aplicação da lei na determinação de que um crime ocorreu.[32] Além disso, um perpetrador pode ser sancionado usando uma série de penalidades criminais, civis ou administrativas, dependendo da natureza da fraude e as disposições regulamentares relacionadas disponíveis no setor público

27 Isso inclui o uso de nomes, qualidades ou empresas falsas ou a realização de declarações falsas que abusem da confiança e inspirem confiança, uma falsa esperança ou medo de um evento que não seja real para induzir outra pessoa a abrir mão de seu próprio dinheiro ou do dinheiro de outra pessoa ou a abrir mão de um direito legal ou de propriedade ou de qualquer benefício material. Isso também inclui a ocultação deliberada de fatos materiais.
28 Por exemplo, através do uso de documentos falsos, da inserção de dados falsos ou da transmissão de comandos não autorizados a um computador.
29 Isso inclui fraudes perpetradas online, por telefone, por correio ou pessoalmente, ou uma combinação destes.
30 Isso inclui a obtenção ou tentativa de obter fundos, acesso a serviços, propriedade fixa ou móvel, títulos, letras, promessas, recibos, ou quitações ou uma liberação de obrigações.
31 Esse prejuízo pode ser causado a um indivíduo, uma empresa ou uma organização e inclui perdas de qualquer valor ou importância para a vítima.
32 Para ilustrar, no contexto de fraude de investimento, a negligência pode variar de engano total a práticas negligentes e fornecimento de informações precárias os clientes. Além disso, o benefício antecipado pode estar muitos anos no futuro e, portanto, pode ser difícil comprovar que não entregará o que foi prometido e, assim, estabelecer intenção criminosa (Michael Skidmore, Protecting People's Pensions: Understanding and Preventing Scams (Londres, The Police Foundation, 2020);

ou privado.[33] Dado o foco no crime organizado, a fraude para aqual há responsabilidade criminal é abordada no presente documento temático, mas observa-se que haverá variabilidade nas diferentes jurisdições nacionais.[34]

O tema mais amplo do crime cibernético se destaca na fraude, embora não haja uma abordagem única para definir fraude no contexto do crime cibernético.[35] Uma maneira de entender o crime cibernético é examinar como e em que extensão um crime foi transformado pelas Tecnologias da Informação e Comunicação (TIC).[36] A fraude relacionada às TIC é comumente descrita como um crime cibernético,[37] pois é um crime tradicional que usa sistemas de TIC para aumentar sua escala e alcance. É, portanto, diferente dos crimes ciberdependentes, que podem ser cometidos apenas por meio do uso de sistemas de TIC e que visam a integridade, disponibilidade e confidencialidade de dados eletrônicos e sistemas de TIC.[38] No entanto, essa dicotomia ignora as várias maneiras pelas quais o crime ciberdependente se cruza com a fraude, particularmente quando visto da perspectiva dos infratores e da sequência de crimes subjacentes na prática da fraude, por exemplo, obter acesso ilegal a um sistema de TIC para perpetrar fraude de comprometimento de e-mail comercial. Existem estruturas que conceituam o crime cibernético como um continuum, variando de crimes que são totalmente baseados em tecnologia a crimes nos quais o uso de sistemas de TIC é incidental.[39] O uso de sistemas de TIC para perpetrar fraudes é altamente variável e abrange grande parte desse continuum. O presente documento temático contém o termo “fraude cibernética”, que representa todos os tipos de fraude nesse continuum.

Grupos criminosos organizados no contexto da fraude

Fraude abrange crimes que são abrangentes em método, sofisticação e impacto. Ela abrange infratores que vão desde indivíduos oportunistas que obtêm ganhos financeiros moderados até criminosos altamente motivados e organizados que se esforçam muito para orquestrar fraudes para obter níveis impressionantes de lucro criminoso.[40] Assim, a linha que separa a fraude organizada da não organizada pode ser difícil de traçar. Portanto, distinções mais claras ajudariam no desenvolvimento de políticas e respostas que estejam mais firmemente alinhadas com o problema designado.

Um “grupo criminoso organizado” é definido no artigo 2(a) da Convenção sobre o Crime Organizado como um grupo estruturado de três ou mais pessoas, existindo por um período de tempo e agindo em conjunto com o objetivo de cometer um ou mais crimes graves ou infrações estabelecidas de acordo com a Convenção, afim de obter, direta ou indiretamente, um benefício financeiro ou outro benefício material. O artigo 2(c) da Convenção também fornece esclarecimentos adicionais quanto ao significado de um “grupo estruturado”. Essas definições incorporam flexibilidade para que as entidades responsáveis pela aplicação da lei identifiquem e abordem grupos criminosos organizados. A estrutura que um grupo precisa ter não é especificada na Convenção, nem o período de tempo durante o qual o grupo precisa ter existido.[41]

Os infratores em grupos criminosos organizados são estruturados de diversas maneiras. Tais grupos incluem aqueles que operam em uma hierarquia mais rígida, aqueles com estruturas horizontais que se unem em torno de um grupo central de indivíduos e redes que envolvem alianças mutáveis de criminosos individuais que não se percebem como um grupo, mas ainda se enquadram na definição.

---

33 Mark Button e outros, Fraude e punição: aumentando a dissuasão por meio de sanções mais eficazes – Relatório principal (Portsmouth, Reino Unido, Universidade de Portsmouth, 2012).
34. Reurink, Fraude Financeira.9201
35. Alisdair A. Gillespie e Samantha Magor, “Combatendo a fraude online”, Fórum ERA: Revista da Academia de Direito Europeu, vol. 20. n. 3 (2019)
36. David S. Wall, Cybercrime: The Transformation of Crime in the Information Age (Cambridge, Reino Unido; Malden, Massachusetts, Estados Unidos, Polity Press, 2007)
37. Os termos “crimes cibernéticos” e “crimes ciberdependentes” são usados apenas para fins ilustrativos. Não há acordo em nível internacional sobre seu conteúdo e uso exatos.
38 Para exemplos de crimes cibernéticos e ciberdependentes, veja Mike McGuire e Samantha Dowling, Cyber Crime: A Review of the Evidence – Summary of Key Findings and Implications, Home Office Research Report, No. 75 (2013)
39 Sarah Gordon e Richard Ford, “Sobre a definição e classificação do crime cibernético”, Journal in Computer Virology, vol. 2, No. 1 (agosto de 2006); e Kirsty Phillips e outros, “Conceituando o crime cibernético: definições, tipologias e taxonomias”, Forensic Sciences, vol. 2, No. 2 (abril de 2022).
40 Ver também Jonathan M. Karpoff, “O futuro da fraude financeira”, Journal of Corporate Finance, vol. 66 (2021); e Levi, “Fraude organizada e organização de fraudes”.
41 Uma infinidade de definições de crime organizado são aplicadas na literatura de pesquisa, algumas das quais especificam atividades como violência, corrupção ou infiltração da economia legítima como intrínsecas à presença do crime organizado. Por exemplo, um estudo destacou a ausência dessas atividades entre os fraudadores cibernéticos e, portanto, questionou o papel que o “crime organizado” desempenhou nesses crimes (Eric Rutger Leukfeldt, Anna Lavorgna eEdward R. Kleemans, “Cibercrime organizado ou cibercrime que é organizado? Uma avaliação da conceitualização do cibercrime financeiro como crime organizado”, European Journal on Criminal Policy and Research, vol. 23, No. 3 (setembro de 2017)).

Os atributos estereotipados convencionais associados ao crime organizado nem sempre são essenciais para a perpetração de fraude organizada,[42] e os modelos e estruturas de negócios adotados por grupos criminosos organizados devem ser considerados em relação aos ambientes onde surgem oportunidades criminosas, os métodos usados e as habilidades necessárias:

- A fraude está principalmente relacionada com o roubo monetário e não com a produção ou distribuição de produtos ilegais, distinguindo-a de outras atividades criminosas organizadas.
- Muitas atividades fraudulentas são realizadas remotamente, facilitadas pela tecnologia que permite a comunicação anônima e a transferência de fundos roubados através de fronteiras nacionais, e vítimas e infratores raramente precisam estar no mesmo lugar ao mesmo tempo.
- A fraude geralmente depende de as vítimas fornecerem voluntariamente acesso aos seus fundos, em vez do uso de força ou coerção, com o sucesso dependendo de táticas enganosas que podem confundir a linha entre entidades legítimas e ilegítimas.
- A fraude de colarinho branco é perpetrada dentro de organizações e ocupações que, de outra forma, seriam legítimas.

Não existe uma estrutura típica para um grupo criminoso organizado envolvido em fraudes e, assim como em outras formas de crime organizado, há variações regionais nos métodos e estruturas empregados por grupos criminosos organizados.[43] Isso ocorre em parte porque há uma gama muito diversificada de oportunidades para perpetrar fraudes graves que surgem em ambientes empresariais, financeiros e comerciais globais e interconectados.

A organização desses crimes e seus perpetradores assumem muitas formas diferentes quando tais grupos buscam explorar essas oportunidades. O surgimento do crime organizado em diferentes regiões reflete as relações contingentes entre diferentes cenários globais, a capacidade de possíveis fraudadores em uma população de identificar e agir sobre oportunidades criminosas e os controles colocados em prática pelo Estado ou outros para prevenir esses crimes.[44]

A pesquisa sobre as formas como os grupos criminosos organizados se formam no contexto da fraude ainda está em desenvolvimento, mas a compreensão de suas diferentes manifestações é um passo importante para identificar e priorizar os fraudadores mais sérios para intervenção policial.[45]

A perpetração de fraude envolve uma série complexa de eventos para planejar, executar e finalizar atividades criminosas para acessar fundos eevitar a detecção pelas autoridades.[46] A fraude pode ser transnacional, ocorrer por um longo período de tempo, atingir uma multidão de vítimas e envolver processos de lavagem de dinheiro e corrupção nos setores público ou privado.[47] Os co-infratores são frequentemente necessários para completar a série complexa de eventos. Alguns são recrutados para fornecer capacidades específicas que podem aumentar a capacidade e o escopo para perpetrar fraudes, enquanto outros são obrigados a realizar tarefas que exigem muito trabalho. Exemplos incluem o recrutamento de facilitadores profissionais legítimos, criminosos cibernéticos com acesso a conhecimento técnico e recursos e operadores de telefonia que realizam telemarketing.[48]

---

42 Kim-Kwang Raymond Choo e Russell G. Smith, "Exploração criminosa de sistemas online por grupos do crime organizado", Asian Journal of Criminology, vol. 3, No. 1 (junho de 2008); Levi, "Fraude organizada e organização de fraudes"; e Di Nicola, "Rumo ao crime organizado digital".
43. INTERPOL, "Avaliação global de fraude financeira da INTERPOL".
44. Levi, "Fraude organizada e organização de fraudes".
45. É importante ressaltar que a perpetração de fraude grave nem sempre depende de haver co-infratores. Exemplos incluem profissionais que abusam de uma posição legítima ou aqueles capazes de explorar a tecnologia para automatizar a infração (Levi, "Fraude organizada e organização de fraudes"; e Wystke van der Wagen e Wolter Pieters, "Do crime cibernético ao crime ciborgue: botnets como redes híbridas de atores criminosos", British Journal of Criminology, vol. 55, No. 3 (maio de 2015)).
46. Por exemplo, veja Amanda Bodker e outros, "Fraude de cartão não presente: usando scripts de crime para informar iniciativas de prevenção ao crime", Security Journal, vol. 36, nº 4 (dezembro de 2022); Claire Seungeun Lee, "Uma análise de script de crime de fraude de identidade transnacional: uso de tecnologia por infratores migrantes na Coreia do Sul", Crime, Law and Social Change, vol. 74, nº 2 (setembro de 2020); e Levi, "Fraude organizada e organização de fraudes."
47. Por exemplo, veja Rutger Leukfeldt e Jurjen Jansen, "Redes criminosas cibernéticas e mulas de dinheiro: uma análise de ataques de fraude de baixa e alta tecnologia na Holanda", International Journal of Cyber Criminology, vol. 9, n.º 2 (dezembro de 2015); Michael Skidmore e Beth Aitkenhead, "Compreendendo as características de crimes graves de fraude no Reino Unido" (Londres, The Police Foundation, 2023); Olayinka Akanle, JO Adesina e EP Akarah, "Rumo à dignidade humana e a internet: o fenômeno do crime cibernético (yahoo yahoo) na Nigéria", African Journal of Science, Technology, Innovation and Development, vol. 8, n.º 2 (2016); e Tiggey May e Bina Bhardwa, Série de grupos de crime organizado envolvidos em fraudes, prevenção ao crime e gestão de segurança (Londres, Palgrave Macmillan, 2018).
48. Por exemplo, veja May e Bhardwa, Organised Crime Groups Involved in Fraud; Usman Adekunle Ojedokun e Ayomide Augustine Ilori, "Tools, techniques and underground networks of Yahoo-boys in Ibadan city, Nigeria", International Journal of Criminal Justice, vol. 3 (2021); Jienan Liu e outros, "Understanding, measuring, and detecting modern technical support scams", no 8º Simpósio Europeu sobre Segurança e Privacidade do Instituto de Engenheiros Elétricos e Eletrônicos (IEEE), artigo apresentado no Simpósio realizado em Delft, Reino dos Países Baixos, de 3 a 7de julho de 2023; e Vaclav Jirovsky e outros, "Cybercrime and organized crime", em ARES 18: Proceedings of the 13th International Conference on Availability, Reliability and Security, art. No. 61 (Hamburgo, Alemanha, 2018).

Os co-infratores em grupos criminosos organizados desempenham várias funções dependendo das necessidades específicss de um esquema de fraude, e podem variar em sua importância, conscientização e envolvimento.[49]

A natureza dos relacionamentos entre co-infratores dentro de diferentes grupos criminosos organizados pode variar dependendo de como os relacionamentos são formados e para qual propósito. Alguns grupos criminosos organizados promovem laços sociais duráveis entre co-infratores, enquanto em outros, os relacionamentos são formados para o propósito mais singular e pragmático de cometer um crime com sucesso.[50] As maneiras pelas quais esses relacionamentos tomam forma podem afetar a estrutura e a estabilidade do grupo criminoso organizado, e essa variação é evidente no contexto da fraude organizada.

Grupos criminosos organizados que se envolvem em outras formas de crimes graves podem ser atraídos pelos altos lucros e riscos relativamente baixos envolvidos na perpetração de fraudes.[51] Eles são frequentemente grupos duráveis que podem alavancar laços e recursos criminosos para facilitar a prática de fraudes em larga escala. Isso pode incluir a capacidade de exercer influência sobre outros tanto na sociedade legítima quanto no submundo criminoso.[52] Em algumas regiões, grupos criminosos organizados oferecem proteção e segurança para isolar os infratores locais de fraudes da ameaça de entidades policiais locais ou outros criminosos.[53] Um exemplo importante são os chamados compostos de golpes operados por grupos policriminosos no Sudeste Asiático, que industrializaram processos para perpetrar certos tipos de fraude (por exemplo, fraude romântica), em parte por vítimas de tráfico que são enganadas ou coagidas a perpetrar fraudes.[54] Em alguns casos, os lucros da fraude podem ser usados por grupos criminosos organizados para financiar outras atividades criminosas sérias. Existem alguns exemplos em que a fraude se apresenta no nexo entre o crime organizado e o terrorismo, por meio dos quais a fraude fornece os meios para financiar as atividades de organizações terroristas.[55]

Muitos grupos criminosos organizados envolvidos em fraudes são formados com o propósito singular de perpetrar fraudes para obter lucro ilícito. Os relacionamentos entre co-infratores podem estar enraizados em laços sociais próximos,[56] mas também é comum que os relacionamentos surjam de mercados nos quais conhecimento e recursos são comprados e vendidos.[57] Isso promove arranjos colaborativos fluidos, com co-infratores se unindo em torno de crimes de "projeto" que são limitados no tempo. Os relacionamentos entre os

49 Skidmore e Aitkenhead, “Compreendendo as características de crimes graves de fraude”; e Neal Shover, Glenn S. Coffey e Clinton Robert Sanders, “Discando por dólares: oportunidades, justificativas e fraude de telemarketing”, Qualitative Sociology, vol. 27, No. 1 (março de 2004).

50 Isto distingue os grupos criminosos organizados que adotam “estruturas criminosas associativas” daqueles que adotam “estruturas criminosas empresariais” (Klaus von Lampe, Organized Crime: Analyzing Illegal Activities, Criminal Structures, and Extra-legal Governance (Los Angeles, Califórnia, Sage Publications, 2016)).

51 Um exemplo ilustrativo éa Black Axe Confraternity, um antigo grupo criminoso organizado que emana da Nigéria, mas tem membros localizados em vários países. Eles estão envolvidos em múltiplas formas de crime organizado que incluem tráfico de pessoas e tráfico de drogas, bem como fraude romântica e outros crimes cibernéticos. Veja Nate Allen, Matthew La Lime e Tomsin Sammer-Nlar, The Downsides of Digital Revolution: Confronting Africa's Evolving Cyber Threats (Genebra, Global Initiative against Transnational Organized Crime, 2022); e Kim-Kwang Raymond Choo, “Grupos de crime organizado no ciberespaço: uma tipologia”, Trends in Organized Crime, vol. 11, No. 3 (setembro de 2008).

52 Além de serem formados com base em laços sociais, alguns grupos podem adotar “estruturas criminosas quase governamentais” impondo estruturas de governança e controle sobre o crime e os criminosos dentro de uma localidade e, em alguns casos, corrompendo funcionários públicos (von Lampe, Organized Crime: Analyzing Illegal Activities).

53 Mortley, “Um crime de oportunidade”; e Akanle, Adesina e Akarah, “Rumo à dignidade humana e a internet”.

54 Escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos (ACNUDH), “Operações de fraude online e tráfico para criminalidade forçada no Sudeste Asiático: recomendações para uma resposta de direitos humanos” (Bangkok, Escritório Regional para o Sudeste Asiático, 2023); UNODC, Escritório Regional para o Sudeste Asiático e Pacífico, Cassinos, Fraude Cibernética e Tráfico de Pessoas para Criminalidade Forçada no Sudeste Asiático: Relatório de Políticas (Bangkok, 2023); e Relatório Global sobre Tráfico de Pessoas 2022 (publicação das Nações Unidas, 2022), p. 102.

55 Nicholas Ryder e Samantha Bourton, “Trocar ou não trocar – eis aquestão: uma análise crítica do uso de inteligência financeira e da troca de informações no Reino Unido”, Journal of Business Law, vol. 3 (2024); e Frank S. Perri e Richard G. Brody, “A tríade obscura: crime organizado, terror e fraude”, Journal of Money Laundering Control, vol. 14, n.º 1 (2011).

56 Eric Rutger Leukfeldt, “Cibercrime e laços sociais: phishing em Amsterdã”, Trends in Organized Crime, vol. 17, n.º 4 (dezembro de 2014); Jonathan Lusthaus, Industry of Anonymity: Inside the Business of Cybercrime (Cambridge, Massachusetts, Harvard University Press, 2018); e Joshua Oyeniyi Aransiola e Suraj Olalekan Asindemade, “Compreendendo os perpetradores de crimes cibernéticos e as estratégias que eles empregam na Nigéria”, Cyberpsychology, Behavior, and Social Networking, vol. 14, n.º 12 (dezembro de 2011).

57 Richet, “Como as comunidades cibercriminosas crescem e mudam”; Lilian Ablon, Martin C. Libicki e Andrea A. Golay, Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar (Santa Monica, Califórnia, RAND Corporation, 2014); e Michael Yip, Nigel Shadbolt e Craig Webber, “Análise estrutural de redes sociais criminosas online”, em 2012 IEEE International Conference on Intelligence and Security Informatics, Daniel Zeng e outros, eds.

membros do grupo podem ser transacionais ou de curta duração, ou podem durar apenas enquanto o esquema fraudulento é bem-sucedido.[58] Alguns grupos criminosos organizados imitam uma estrutura de força de trabalho legítima que ocupa espaço de escritório, com co-infratores empregados como membros assalariados da equipe ou contratados para fornecer um serviço.[59] No entanto, a co-infração no contexto de fraude cibernética também pode estar enraizada em relacionamentos estabelecidos online. Além de criar novas oportunidades criminosas para perpetrar fraudes,[60] a Internet reduziu as barreiras para a formação de relacionamentos com novos possíveis co-infratores: ela criou ambientes mais acessíveis nos quais novos e anônimos infratores podem rapidamente estabelecer confiança e aproveitar o capital criminoso disponível em redes online.[61] Isso é exemplificado pelo modelo de crime como serviço,[62] em que os criminosos se envolvem em trocas on-line de curto prazo com outros na Internet que podem fornecer os recursos técnicos para perpetrar fraudes com sucesso.[63] Alguns grupos criminosos organizados que se envolveram em fraudes cibernéticas são formados a partir de relacionamentos que existem inteiramente online (por exemplo, fóruns online),[64] outros são formados offline e alguns incorporam co-infratores offline e online.[65]

Existem grupos criminosos organizados envolvidos em fraudes corporativas ou de colarinho branco que emergem de dentro de organizações comerciais legítimas.[66] O abuso de uma função legítima para obter lucro ilegal pode servir aos interesses de funcionários específicos dentro da organização ou pode ter a intenção de beneficiar toda a organização.[67] Os grupos criminosos organizados podem surgir das estruturas que já existem no negócio para conduzir sua atividade comercial legítima, como as funções e hierarquia internas à organização ou relacionamentos entre diferentes negócios. Exemplos incluem o envolvimento de funcionários seniores e subordinados dentro do negócio, ouso de profissionais-chave, como contadores ou advogados, e co-infração por diferentes organizações em um setor, como em casos de negociação com informações privilegiadas.[68]

Há sobreposições entre os diferentes tipos de grupos criminosos organizados que estão envolvidos em fraudes, em parte devido à fluidez de acordos de co-infração em certos ambientes online e comerciais.[69] Por exemplo, os ciberempreendedores, ou especialistas em finanças, fornecem conhecimento especializado e recursos que são altamente valorizados por vários grupos criminosos organizados que buscam aumentar suas

58 Skidmore e Aitkenhead, "Compreendendo as características de infrações graves de fraude".
59 Liu e outros, "Compreendendo, medindo e detectando"; Shover, Coffey e Sanders, "Discando por dólares"; e May e Bhardwa, Grupos do crime organizado envolvidos em fraudes.
60 Jay S. Albanese, "Fraude: o crime característico do século XXI", Trends in Organized Crime, vol. 8, No. 4 (junho de 2005); Mark Button e Cassandra Cross, Fraudes cibernéticas, golpes e suas vítimas (Abingdon, Oxon, Reino Unido e Nova York, Routledge, 2017); e Robert B. Fried, "Golpistas cibernéticos: um novo tipo de golpe" (2001).
61 Geralda Odinot e outros, Organised Cybercrime in the Netherlands: Empirical Findings and Implications for Law Enforcement (Haia, Centro de Pesquisa e Dados, Ministério da Segurança e Justiça, 2017); Ablon, Libicki e Golay, Markets for Cybercrime Tools and Stolen Data; e Michael Yip, Craig Webber e Nigel Shadbolt, "Trust among cybercriminals? Carding forums, uncertainty and implications for policing", Policing and Society: An International Journal of Research and Policy, vol. 23, n.º 4 (2013).
62 Os mercados online, sites personalizados e fóruns podem operar em sua própria estrutura organizacional: os administradores, que gerenciam os sites, os moderadores, que regulam o comportamento no site, os vendedores, que fornecem os produtos, serviços e expertise, e os compradores, que fazem compras e se envolvem na troca de informações. Nesse contexto, habilidades e recursos técnicos são valorizados em detrimento da presença física e do poder (Yip, Webber e Shadbolt, "Trust among cybercriminals?"; Ildiko Pete e outros, "A social network analysis and comparison of six dark web forums", em 5th IEEE European Symposium on Security and Privacy Workshops (2020); e Choo e Smith, "Criminal exploration of online systems").
63 Ver também Ugur Akyazi, Michael van Eeten e Carlos H. Gañán, "Medindo ofertas de crime cibernético como serviço (CaaS) em um fórum de crime cibernético" (Delft, Reino dos Países Baixos, Universidade de Tecnologia de Delft, 2021); e Jungkook An e Hee-Woong Kim, "Uma abordagem de análise de dados para a economia subterrânea do crime cibernético", IEEE Access, vol. 6 (2018).
64 Melvin RJ Soudijn e Birgit CHT Zegers, "Cibercrime e cenários de convergência de criminosos virtuais", Tendências no Crime Organizado, vol. 15, Nos. 2 e3 (setembro de 2012).
65 Leukfeldt, Lavorgna e Kleemans, "Organised cybercrime or cybercrime that is organised?"; e E. Rutger Leukfeldt, Edward R. Kleemans e Wouter P. Stol, "Origem, crescimento e capacidades criminais das redes cibercriminosas: uma análise empírica internacional", Crime Law and Social Change, vol. 67, No. 1 (fevereiro de 2017).
66 Alan Wright, Organised Crime (Cullompton, Reino Unido, Willan Publishing, 2006); Gary Slapper e Steve Tombs, Corporate Crime (Harlow, Reino Unido, Pearson, 1999); Albanese, "Crime organizado como crime financeiro"; e Michael Levi e Mike Maguire, "Crime financeiro e organizado na Europa: paradigmas convergentes de controle?", em *Universalis. Liber amicorum Cyrille Fijnaut*, Toine Spapens, Marc Groenhuijsen e Tijs Kooijmans, eds. (Antuérpia, Bélgica, Intersentia, 2011).
67 Por exemplo, grupos criminosos corporativos foram identificados como uma manifestação-chave do crime organizado no contexto do comércio ilegal de vida selvagem: atos criminosos corporativos podem ser o produto de tomada de decisão deliberada ou negligência culpável dentro de uma organização legítima (Tanya Wyatt, Daan van Uhm e Angus Nurse, "Differentiating criminal networks in the illegal wildlife trade: organized, corporate and disorganized crime", Trends in Organized Crime, vol. 23, No. 4 (dezembro de 2020). Veja também Reurink, Financial Fraud).
68 Levi, "Fraude organizada e organizaçaõ de fraudes"; e Ruben Herrera e outros, "A manipulação da Euribor: uma análise com técnicas de classificação de machine learning", Previsão Tecnológica e Mudança Social, vol. 176, art. No. 121466 (março de 2022).
69 Leukfeldt, Kleemans e Stol, "Origem, crescimento e capacidades criminosas das redes cibercriminosas"; e Skidmore e Aitkenhead, "Compreendendo as características de crimes graves de fraude".

capacidades.[70] A natureza fluida e efêmera da co-infração que caracteriza grande parte da fraude organizada significa que muitos grupos criminosos organizados envolvidos nela não exibem as estruturas tradicionais observadas em grupos envolvidos em outras formas de crime organizado.[71] Como resultado, há desafios para identificar, avaliar e fornecer respostas eficazes a grupos que são frouxamente estruturados e transitórios. Por exemplo, em mercados criminosos online (ou ecossistemas), pode ser difícil saber onde um grupo criminoso organizado termina e o próximo começa.[72] No entanto, é importante ser capaz de reconhecer grupos criminosos organizados que adotam essas estruturas diversas para garantir que os perpetradores mais impactantes sejam visados.

É importante ressaltar que nem todos os grupos de co-infratores que cometem fraude constituem um grupo criminoso organizado de acordo com a Convenção sobre o Crime Organizado. Isso ocorre porque a perpetração de fraude grave também é um princípio definidor fundamental do crime organizado. As principais características do crime grave no contexto de crimes de fraude serão discutidas na próxima seção.

70 Botão e Cruz, Fraudes Cibernéticas, Golpes e Suas Vítimas.
71 Di Nicola, "Rumo ao crime organizado digital"; Anita Lavorgna e Anna Sergi, "Sério, portanto organizado? Uma crítica à retórica emergente do 'crime ciberorganizado' no Reino Unido", International Journal of Cyber Criminology, vol. 10, n.º 2 (julho/dezembro de 2016); David S. Wall, "Crime desorganizado: rumo a um modelo distribuído de organização do crime cibernético", European Review of Organised Crime, vol. 2, n.º 2(2015); Leukfeldt, Lavorgna e Kleemans, "Criminalidade cibernética organizada ou cibercrime organizada?"; e Levi, "Fraude organizada e organização de fraudes".
72 Por exemplo, ver Erika Kraemer-Mbula, Puay Tang e Howard Rush, "The cybercrime ecosystem: online innovation in the shadows?", Technological Forecasting and Social Change, vol. 80, n.º 3 (março de 2013).

ESTUDO DE CASO: GOLPE DE SUPORTE TÉCNICO

Os perpetradores do golpe de suporte técnico desenvolveram sites fraudulentos para imitar serviços legítimos de suporte técnico (por exemplo, software de segurança ou conserto de impressoras), que eram anunciados usando mecanismos de busca da web convencionais. Aqueles que visitavam o site eram induzidos a ligar para um número de telefone, em que o manipulador de chamadas persuadia a vítima a pagar quantias significativas de dinheiro por um serviço fabricado ou desnecessário. Os criminosos envolvidos nesses golpes operavam como parte de uma vibrante economia subterrânea, na qual grupos criminosos organizados compravam e vendiam serviços especializados em grupos de bate-papo que operavam em plataformas de mídia social convencionais. Os criminosos operavam como subempresas discretas que forneciam funções específicas na realização do golpe de suporte técnico. Essas funções incluíam os operadores de call center que atendiam as chamadas das vítimas, grupos que se especializavam em lavagem de dinheiro e vendiam seus serviços para os call centers e as pessoas que construíam e promoviam os sites e vendiam e redirecionavam as chamadas das vítimas para os operadores de call center. Embora grande parte da colaboração entre os diferentes subempresas tenha sido estabelecida online, houve uma concentração de infratores na Índia. Muitos dos call centers operavam em escritórios localizados em grandes cidades por toda a Índia, e anúncios de emprego para agentes de atendimento eram regularmente postados em fóruns online, dando detalhes sobre o salário e os benefícios do emprego.

Fonte: Jienan Liu eoutros, "Understanding, measuring, and detecting modern technical support scams", no *8º Simpósio Europeu sobre Segurança e Privacidade do Instituto de Engenheiros Elétricos e Eletrônicos (IEEE),* artigo apresentado no Simpósio realizado em Delft, Reino dos Países Baixos, de 3 a 7 de julho de 2023.

ESTUDO DE CASO: FRAUDE AO CONSUMIDOR

Um infrator criou várias lojas online falsas que foram feitas para parecerem confiáveis por se assemelharem a outros varejistas online tradicionais, embora nenhum dos produtos anunciados no site existisse. Os sites foram amplamente anunciados em um mecanismo de busca da Internet tradicional, em sites de comparação de preços e em jornais. Cada cliente que fizesse um pedido receberia uma confirmação de pedido automatizada, recibo e uma solicitação de pagamento solicitando uma transferência eletrônica. O infrator procurou um cúmplice para ajudar a fornecer as contas bancárias para receber o dinheiro. Ele encontrou um co-infrator em um fórum da darknet. Este co-infrator o aconselhou sobre como lavar os lucros criminosos e evitar a detecção pelas autoridades. Ele ajudou a recrutar várias mulas de dinheiro com contas bancárias estrangeiras que concordaram em receber os pagamentos dos clientes, pegando 15 por cento para si e então encaminhando o restante para os dois principais infratores, que dividiriam o restante dos lucros criminosos. O grupo conseguiu roubar mais de €280.000 (duzentos e oitenta mil euros) dos clientes.

Fonte: Tribunal Distrital de Munique, Sentença, 7 de junho de 2017 (LG München, Urteil vom 07.06.2017, 19 KLs 30 Js 18/15), disponível no portal de gerenciamento de conhecimento Sharing Electronic Resources and Laws on Crime (SHERLOC).

ESTUDO DE CASO: FRAUDE EM LEILÃO ENVOLVENDO UM GRUPO CRIMINAL ORGANIZADO HÍBRIDO (OFFLINE-ONLINE)

Os infratores perpetraram fraudes on-line nas quais itens inexistentes foram anunciados para consumidores nos Estados Unidos da América em sites de leilões tradicionais. Os membros do grupo que planejou e preparou o esquema fraudulento estavam todos localizados na mesma cidade na Romênia. Eles pediram aos consumidores que fizessem pagamentos usando cartões de débito pré-pagos. Esses pagamentos foram coletados por outros associados e lavadores de dinheiro terceirizados localizados nos Estados Unidos. Depois que os pagamentos das vítimas foram coletados, os infratores baseados nos Estados Unidos converteram o dinheiro em bitcoin, que foi transferido para o grupo na Romênia. As bolsas de bitcoin foram usadas para converter o dinheiro na moeda local, o que incluía uma bolsa operada por um cidadão búlgaro que foi cúmplice na facilitação do processo de lavagem de dinheiro.

Fonte: Estados Unidos da América v. Andre-Catalin Stoica et al., disponível no portal de gerenciamento de conhecimento Sharing Electronic Resources and Laws on Crime (SHERLOC).

Crime grave no contexto de fraude

O conceito de crime grave é central na definição do escopo de aplicação da Convenção sobre Crime Organizado. Para que a Convenção seja aplicável, o crime cometido pelo grupo criminoso organizado tem que atender aos critérios definidos (incluindo transnacionalidade e envolvimento de um grupo criminoso organizado) e ser punível com uma pena máxima de privação de liberdade de pelo menos quatro anos na legislação nacional. Portanto, o uso da noção de crime grave com referência à lei nacional dos Estados fornece flexibilidade suficiente para que a Convenção seja aplicada a uma ampla gama de manifestações de crime organizado transnacional, incluindo fraude.

Um "crime grave" é definido no artigo 2(b) da Convenção como "conduta que constitui um delito punível com uma pena máxima privativa de liberdade de pelo menos quatro anos ou uma pena mais grave". O artigo 3, parágrafo 2, da Convenção estabelece os critérios para determinar quando um delito será considerado de natureza transnacional, para fins de aplicação da Convenção.

Internacionalmente, os sistemas legais existentes são ambíguos quanto à seriedade da fraude. Os fatores agravantes específicos que podem aumentar individual ou cumulativamente as penalidades para fraudadores condenados, e a penalidade máxima que pode ser aplicada em um caso de fraude, variam entre diferentes jurisdições legais (veja o cap. V abaixo). Isso se reflete nas penalidades dadas aos infratores de fraude: por exemplo, longas sentenças de prisão impostas a infratores de colarinho branco que fraudam instituições demonstraram ser baixas em número, apesar da prevalência desse delito e dos altos lucros para os infratores.[73] Além disso, alguns dos tipos mais sofisticados de fraude estão nas margens cinzentas que separam práticas legítimas de ilegítimas, e o direito penal (e sua aplicação) pode ser substituído por leis civis aplicadas por órgãos reguladores no setor público mais amplo.[74] O tratamento desigual da fraude na lei promove ambiguidade na identificação de fraudes e fraudadores "sérios".

73 Michael Levi, "Atingindo o ponto de chave: fraudes de sentença", Journal of Financial Crime, vol. 17, No. 1 (2010); e Lisa Marriott, "crime de colarinho branco: o privilégio de fraudes financeiras graves na Nova Zelândia", Estudos Sociais e Legais, vol. 29, No. 4 (agosto de 2020).
74 Button e Cross, Fraudes Cibernéticas, Golpes e Suas Vítimas.

Há duas dimensões principais de seriedade a considerar: [75]

- O dano que pode ser atribuído à fraude, em termos da vítima identificável ou do grupo de vítimas ou do impacto mais amplo que tem nas instituições legítimas [76]
- A culpabilidade moral do(s) perpetrador(es), ou seja, a extensão em que certos comportamentos violam os padrões morais aceitos na sociedade [77]

As várias vítimas, suas experiências, os comportamentos ofensivos e métodos significam que, como uma categoria de crime, a fraude incorpora uma criminalidade que é altamente diversa em relação à gravidade dos danos causados e à ilicitude moral dos comportamentos ofensivos. Vários fatores podem ser percebidos como agravantes de um crime de fraude e, portanto, torná-lo mais sério. Tais fatores incluem o impacto financeiro e o dano à vítima, mas também comportamentos ofensivos específicos, como visar vítimas vulneráveis, ter contato repetido com a mesma vítima para se envolver em métodos mais complexos ou insidiosos (por exemplo, aliciamento), abusar de uma posição de confiança ou autoridade para fraudar vítimas e visar um grande número de vítimas. [78]

Há uma necessidade de considerar as evidências sobre as características de infrações de fraude que podem ser usadas para determinar se certas infrações de fraude devem ser tratadas como crimes graves em termos de sentença e política de justiça criminal mais ampla. Essas características são definidas nas seções abaixo.

Perdas financeiras e impacto

Fraude é um crime aquisitivo, e o valor do dinheiro que é roubado (ou que se pretendia roubar) informa as avaliações de sua seriedade. Isso pode ser visto como o agregado de perdas intencionais ou reais atribuíveis a infratores que fraudam várias vítimas. Diferentes comportamentos ofensivos podem levar a padrões distintos de fraude e perda financeira. Alguns esquemas fraudulentos afetam um número relativamente pequeno de vítimas que são fraudadas em quantias significativas de dinheiro,[79] enquanto outros fraudam um número maior de vítimas em quantias menores de dinheiro.[80] As avaliações de perdas para as vítimas também podem levar em consideração quem são as vítimas (por exemplo, um indivíduo ou empresa), a proporção da riqueza de uma vítima perdida para a fraude e outros danos colaterais mais amplos causados.[81] A fraude pode minar setores legítimos, impondo custos além das perdas diretas para a organização que é alvo.[82]

75 An Adriaenssen e outros, "Public perceptions of the seriousness of crime: weighing the harm and the wrong", European Journal of Criminology, vol. 17, n.º 2 (março de 2020); Jonas Visschers e Letizia Paoli, "A comparison of public and police perceptions of the seriousness of crime", European Journal on Criminal Policy and Research (2024); e Victoria A. Greenfield e Letizia Paoli, "A framework to assess the harms of crimes", The British Journal of Criminology, vol. 53, n.º 5 (setembro de 2013).
76 Tom Sorell, "O escopo do crime grave eda justiça preventiva", Criminal Justice Ethics, vol. 35, No. 3 (2016).
77 Por exemplo, independentemente do dano sofrido, o roubo pode ser interpretado como uma violação maior das normas morais do que o furto devido ao ataque à integridade do domicílio da vítima.
78 Button e outros, "Fraudes online".
79 Por exemplo, veja Skidmore, Protecting People's Pensions.
80 Por exemplo, veja Marguerite DeLiema e Paul Witt, Mixed Methods Analysis of Consumer Fraud Reports of the Social Security Administration Impostor Scam, Documento de Trabalho, nº 2021-434 (Ann Arbor, Universidade de Michigan, Michigan Retirement and Disability Research Center, 2021).
81 Michael Levi, "Fraude organizada", em The Oxford Handbook of Organized Crime, Letizia Paoli, ed. (Oxford, Oxford University Press, 2014); e Xin Qingquan, Jing Zhou e Fang Hu, "As consequências econômicas da fraude financeira: evidências do mercado de produtos na China", China Journal of Accounting Studies, vol. 6, n.º 1 (2018).
82 Por exemplo, a chamada fraude "colisão por dinheiro" contra o setor de seguros de automóveis pode aumentar os prêmios de seguro para o público (David S. Wall, Yulia Chistyakova e Stefano Bonino, "Crash-for-cash e carrosséis de IVA: infiltração do crime organizado no Reino Unido", em Crime organizado em empresas europeias, Ernesto Savona, Michele Riccardi e Giulia Berlusconi, eds. (Londres, Routledge, 2016)).

Danos às vítimas

A fraude ocorre principalmente a portas fechadas e raramente envolve crimes publicamente visíveis ou viscerais, como violência grave, que são um foco convencional para agências de aplicação da lei. Além disso, as políticas de sentenças da justiça criminal podem ter um foco singular na perda financeira, sem considerar o impacto humano da fraude. A pesquisa identificou vítimas que sofrem um efeito prejudicial considerável em seu bem-estar psicológico, emocional e saúde física; em casos extremos, as vítimas tiraram suas próprias vidas como consequência da fraude.[83] As respostas das vítimas são altamente subjetivas e podem ser determinadas por suas circunstâncias pessoais e pelas particularidades da metodologia de fraude.[84] A natureza ampla e subjetiva das experiências das vítimas significa que há desafios para identificar vulnerabilidade e dano entre o alto volume de vítimas de fraude.[85]

Culpabilidade do fraudador

A culpabilidade reflete em parte o nível de intenção criminosa exibido por um perpetrador, como a extensão do planejamento e premeditação e evidências de reincidência. Os processos complexos para perpetrar fraudes geralmente envolvem estágios de planejamento e preparação, e alguns infratores inovam continuamente novos métodos para explorar a gama de oportunidades criminosas disponíveis.[86] O crescimento das TICs "industrializou" a infração por fraude, proporcionando maior escopo para os criminosos perpetrarem fraudes em uma escala sem precedentes, com rapidez e baixo custo.[87] Os criminosos podem aproveitar a tecnologia para atingir muitas vítimas simultaneamente, em alguns casos por meio da automação.[88] Além disso, as TICs são globalizadas de forma padronizada e, em alguns casos, há pouca diferença prática entre perpetrar fraudes locais ou transnacionais.[89] Nesse contexto, a linha que separa criminosos sérios de não sérios pode ser difícil de traçar.

Os métodos específicos empregados para atingir e fraudar vítimas podem determinar a gravidade percebida das ações do fraudador. Isso inclui atingir, às vezes repetidamente, pessoas que são de alguma forma desfavorecidas, como vítimas que são percebidas como vulneráveis (por exemplo, pessoas com deficiência).[90] O abuso de uma posição de poder ou confiança também é considerado um fator agravante em crimes de fraude em algumas jurisdições legais.[91] Por fim, o envolvimento de um grupo criminoso organizado pode, por si só, multiplicar os efeitos adversos da fraude e sinalizar maior intenção criminosa e culpabilidade. Um grupo criminoso organizado que mantém uma "instituição" criminosa com um suprimento pronto de co-infratores para perpetrar fraude de maneira contínua (bem como outros crimes auxiliares, como pirataria ilícita e branque-

83 Por exemplo, veja Button, Lewis e Tapley, "Not a victimless crime"; Cassandra Cross, "(Mis)understanding the impact of online fraud: implications for victim assistance schemes", Victims and Offenders, vol. 13, No. 6 (2018); Raoul Notté e outros, "Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands", International Review of Victimology, vol. 27, No. 3 (setembro de 2021); e Encarnación Sarriá e outros, "Financial fraud, mental health, and quality of life: a study on the population of the city of Madrid, Spain", International Journal of Environmental Research and Public Health, vol. 16, No. 18 (setembro de 2019).
84 Por exemplo, a fraude romântica demonstrou causar sofrimento emocional significativo às vítimas (Tom Buchanan eMonica T. Whitty, "The online dating romance scam: causes and consequences of victimhood", Psychology, Crime and Law, vol. 20, No. 3 (2014). Veja também Katelyn A. Golladay e Jamie A. Snyder, "Financial fraud victimization: an examination of distress and financial complications", Journal of Financial Crime, vol. 30, No. 6 (2023)).
85 Michael Skidmore, Janice Goldstraw-White e Martin Gil, "Vulnerabilidade como um driver da resposta policial à fraude", Journal of Criminological Research, Policy and Practice, vol. 6, No. 1 (2020); e Sara Correia, "Vítimas de crimes cibernéticos: política de vítimas através de uma lente de vulnerabilidade ", Social Science Research Network Working Paper (2021). No Reino Unido, há um foco crescente na identificação de vítimas vulneráveis, particularmente aquelas em risco de serem alvos repetidamente.
86 Por exemplo, ver Kraemer-Mbula, Tang e Rush, "O ecossistema do cibercrime"; e Skidmore e Aitkenhead, "Compreendendo as características de infrações graves de fraude"
87 Button and Cross, Fraudes cibernéticas, golpes e suas vítimas; e Michael Levi eoutros, As implicações do crime cibernético econômico para o policiamento, Relatório de pesquisa (Londres, City of London Corporation, 2015).
88 Wall, "Crime desorganizado"; e van der Wagen e Pieters, "Do cibercrime ao crime ciborgue".
89 Levi e outros, As implicações do crime cibernético econômico para o policiamento.
90 Uma pesquisa sobre as opiniões do público no Reino Unido mostrou que métodos insidiosos, como aliciamento financeiro, eram percebidos como tipos mais sérios de fraude (ver Jane Kerr eoutros, Research on Sentencing Online Fraud Offenses (Londres, Sentencing Council, 2013)).
91 Marriott, "White-collar crime"; ver também capítulo V do presente documento.

amento de capitais),[92] podem envolver-se em crimes considerados mais graves.[93] Além disso, a criminalidade pode tornar-se ainda mais grave quando o grupo é capaz de desafiar ou minar a autoridade e os sistemas do Estado e dos setores legítimos (por exemplo, por meio da corrupção).[94]

As estruturas de condenação no sistema de justiça criminal fornecem orientação importante para as agências de aplicação da lei na decisão de onde direcionar os recursos disponíveis. O escopo aumentado da complexidade dos delitos de fraude, particularmente aqueles possibilitados pela tecnologia, cria desafios na identificação de fraudes graves, mas estruturas robustas são necessárias para atingir os casos de fraude mais flagrantes. As dimensões precisas da fraude organizada em cada Estado-Membro precisarão ser levadas em consideração nas decisões políticas sobre recursos para a aplicação da lei e estratégias mais amplas de prevenção ao crime para combater a fraude. Historicamente, no entanto, a fraude cometida por grupos criminosos organizados não recebeu os mesmos níveis de prioridade dados a outras manifestações do crime organizado,[95] e a fraude organizada tem sido frequentemente percebida como uma atividade suplementar de grupos criminosos organizados envolvidos em outros crimes mais graves (por exemplo, tráfico de drogas).[96]

Interseccionalidade

Um conceito fundamental para entender as experiências das pessoas com fraudes organizadas é a interseccionalidade. A interseccionalidade constitui uma estrutura para analisar como o poder e a identidade se cruzam para influenciar as relações sociais e as experiências individuais. Ela enfatiza que as experiências de homens, mulheres e indivíduos de gênero diverso interagem com sua classe, raça, idade, etnia e identidades sexuais e outras, moldando assim as maneiras pelas quais as pessoas são percebidas na sociedade. No contexto da fraude organizada, uma análise interseccional é uma ferramenta útil para entender as diferentes tendências e motivadores para participar e se tornar uma vítima de fraude organizada. Isso não quer dizer que certas características de identidade levam uma pessoa a ser inerentemente vulnerável à fraude organizada, mas que, devido a fatores estruturais, históricos e contextuais, o privilégio e o poder de uma pessoa podem ser afetados em circunstâncias específicas, levando a experiências diferenciadas de fraude organizada. O estudo de caso abaixo destaca como grupos criminosos organizados podem tirar vantagem da exclusão social e histórica enfrentada por pessoas com deficiência para realizar fraude organizada.

92 Leukfeldt e Jansen, “Redes cibercriminosas e mulas de dinheiro”; Jonathan Lusthaus e outros, “Redes cibercriminosas no Reino Unido e além: estrutura de rede, cooperação criminal e interações externas”, Trends in Organized Crime (2023); David S. Wall, “Realismo digital e a governança do spam como crime cibernético”, European Journal on Criminal Policy and Research, vol. 10, No. 4 (dezembro de 2004); e Michael Yip, Nigel Shadbolt e Craig Webber, “Por que fóruns? Uma análise empírica dos fatores facilitadores dos fóruns de carding”, em Anais da 3ª Conferência Anual de Ciência da Web da ACM (Paris, 2013).
93 Sorell, “O escopo do crime grave”.
94 Por exemplo, grupos criminosos organizados que operam no Sudeste Asiático se envolvem em criminalidade sistêmica e geram lucros com fraudes estimados em bilhões de dólares. Esses grupos têm um envolvimento de longa data em várias formas de crime organizado, e a capacidade de perpetrar fraudes nessa escala está ligada a desenvolvimentos paralelos em bancos clandestinos e lavagem de dinheiro, especificamente cassinos. Os cassinos podem facilitar a lavagem de dinheiro, mas também fornecem uma fachada e uma facilidade para empregar uma grande força de trabalho para co-infração de dentro de compostos de golpes. Além disso, alguns grupos operam propositalmente de dentro de países onde a governança e o estado de direito são fracos e funcionários públicos são suscetíveis à corrupção (veja OHCHR, “Online scam operations and trafficking into forced criminality in Southeast Asia”; e UNODC, Regional Office for South-East Asia and the Pacific, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, Technical Policy Brief (Bangkok, 2024)).
95 Alan Doig e Michael Levi, “Um caso de desenvolvimento interrompido? Entregando a Estratégia Nacional de Fraude do Reino Unido dentro de prioridades de política de policiamento concorrentes”, Public Money and Management, vol. 33, No. 2 (2013); e Cassandra Cross e Dom Blackshaw, “Melhorando a resposta da polícia à fraude online”, Policing, vol. 9, No. 2 (junho de 2015).
96 Levi, “Fraude organizada”, em The Oxford Handbook of Organized Crime.

ESTUDO DE CASO: FRAUDE EM PRODUTOS E SERVIÇOS DE CONSUMO E INVESTIMENTO

No Reino Unido, um indivíduo que sofria de uma condição neurológica progressiva foi preparado ao longo de vários anos por um pequeno grupo criminoso organizado de base familiar. O principal infrator era aparentemente um comerciante que conheceu a vítima quando procurava por clientes em potencial. O grupo concluiu e cobrou a mais por uma infinidade de reparos e trabalhos de manutenção de baixo padrão na casa da vítima. Além disso, eles o persuadiram a entregar £240.000, o que incluía dinheiro para uma suposta oportunidade de investimento. A vítima não reconheceu que era uma vítima porque os perpetradores tinham se esforçado muito para fazer amizade com ele e, consequentemente, ele pensou que estava ajudando pessoas que eram seus amigos. A fraude foi eventualmente relatada por seu cuidador, e os agentes da lei tiveram que explicar cuidadosamente como e por que ele tinha sido vítima de fraude. Este exemplo ilustra como alguns grupos criminosos organizados têm como alvo pessoas com deficiência devido à probabilidade de pessoas com deficiência vivenciarem isolamento social enão terem acesso adequado ao suporte social.

Fonte: Coretta Phillips, "De 'comerciantes desonestos' a grupos do crime organizado: fraude porta a porta de idosos", *The British Journal of Criminology,* vol. 57, No. 3 (maio de 2017).

É importante reconhecer que não há características específicas de identidade que tornem uma pessoa mais vulnerável à fraude organizada. Isso se deve às suas muitas manifestações e tipologias. Por exemplo, um indivíduo com alta renda pode ser alvo de fraude de investimento, enquanto um indivíduo em uma faixa socioeconômica mais baixa pode ser alvo de fraude de emprego. Por esse motivo, e para poder desenvolver medidas preventivas eficazes, é importante coletar dados interseccionais e desagregados por gênero e realizar análises para identificar por que certas populações podem ser alvos de diferentes tipos de fraude.

CAPÍTULO II
Categorias de fraude organizada

A infração por fraude é altamente diversificada, tanto nos métodos empregados, quanto nas entidades visadas e no impacto sobre as vítimas e os sistemas em geral. O presente artigo concentra-se em fraudes que são direcionadas a indivíduos de instituições públicas ou privadas com o propósito de obter um benefício financeiro ou outro benefício material.

As categorias na tipologia são organizadas de acordo com as narrativas ou artifícios abrangentes e predominantes que são apresentados[97] às vítimas de fraude; por exemplo, a divulgação de uma oportunidade de emprego em uma fraude de emprego. No entanto, a categoria de fraude contra empresas e organizações também é incluída para abranger a variedade de fraudes contra tais entidades,[98] incluindo o abuso de sistemas por perpetradores que são internos ou externos à organização.[99] Dessa forma, as categorias de fraude são organizadas principalmente a partir de uma perspectiva centrada na vítima, e não nos processos subjacentes à execução do crime, como os métodos de roubo de dados pessoais ou os meios de marketing e outras formas de comunicação em massa.

As principais categorias que serão descritas nas seções seguintes do documento são:

97 Veja, por exemplo, Beals, DeLiema e Deevy, "Framework for a taxonomy of fraud".
98 Esta categoria foi incluída para garantir que empresas e organizações sejam reconhecidas como um grupo de vítimas-chave. Outras categorias, como fraudes em produtos e serviços de consumo e fraudes de identidade também podem levar aperdas financeiras para empresas e organizações.
99 Veja a introdução do presente documento para uma discussão mais detalhada sobre o desenvolvimento da tipologia.

Ao organizar as categorias de acordo com as diversas narrativas ou artifícios apresentados às vítimas, esta tipologia destaca outras distinções amplas nas técnicas utilizadas para manipulá-las a entregar seu dinheiro. As principais distinções incluem o uso de vendas e incentivos em fraudes relacionadas a produtos e serviços de consumo, emprego e investimentos; o medo e a autoridade que caracterizam muitos tipos de fraude em que o criminoso se faz passar por uma pessoa ou organização confiável; a manipulação de informações e sistemas comerciais e financeiros na fraude de identidade; e o aliciamento financeiro e exploração na fraude baseada em relacionamentos e confiança. Outros elementos da interação com os criminosos que podem afetar a experiência das vítimas (por exemplo, o modo de contato ou o período ao longo do qual são alvo da fraude) serão discutidos conforme relevante em cada categoria.

As categorias descritas nesta seção não são exaustivas devido à enorme variedade de metodologias que podem ser empregadas pelos criminosos, que continuamente se adaptam a novos contextos socioeconômicos, sistemas e tecnologias. Cada categoria principal é complementada por subcategorias relevantes, descritas em cada seção. Nem todas as fraudes são cometidas exclusivamente por grupos criminosos organizados, mas a discussão será focada na fraude organizada.

A linha que separa a fraude de comportamentos não criminosos pode ser tênue. Por exemplo, nem sempre um produto ou serviço que não atenda às expectativas do consumidor configura fraude de acordo com a legislação; conforme discutido no capítulo I, isso dependerá da existência de intenção criminosa de enganar. No contexto do crime organizado, a intenção criminosa é evidente em várias ações-chave, como o planejamento e a preparação para a implementação do engano, além do uso da técnica fraudulenta para atingir múltiplas vítimas. Todas as categorias e casos discutidos nesta seção são considerados fraudes conforme a definição apresentada no capítulo I: aqueles que as praticam são criminalmente responsáveis devido ao uso deliberado do engano para obter um benefício financeiro ou material.

Fraude em produtos e serviços de consumo

A fraude em produtos e serviços de consumo representa um tipo de fraude prevalente, com um grande número de pessoas relatando terem sido enganadas, alvo de fraudes ou expostas a comunicações que vendem produtos ou serviços fraudulentos.[100] Muitas vezes, os fraudadores comercializam produtos de alta demanda ou oferecem produtos e serviços a um custo abaixo ao do mercado legítimo. A fraude de produtos e serviços ao consumidor envolve a venda de produtos ou serviços que são inexistentes ou diferem significativamente do que é anunciado (incluindo produtos falsificados vendidos como genuínos).[101] A fraude de não entrega ocorre quando um produto ou serviço é anunciado e pago, mas é totalmente fictício ou não há intenção por parte do fraudador de fornecê-lo.[102] A venda enganosa de produtos e serviços envolve fraudadores que deturpam os produtos ou serviços que estão fornecendo. Pode haver desafios na confirmação da fraude quando o produto ou serviço é recebido, mas é considerado enganoso, exigindo julgamento sobre como e até que ponto ele difere do que foi anunciado ou vendido.[103] Alguns fraudadores direcionam anúncios a grupos considerados mais suscetíveis a um esquema específico.[104] Às vezes, os fraudadores exploram a falta de conhecimento financeiro e técnico da vítima para

100 Por exemplo, a fraude por não pagamento ou não entrega é um dos crimes cibernéticos mais comumente relatados nos Estados Unidos (Estados Unidos, Federal Bureau of Investigation, "Internet crime report 2023" (2023); veja também Comissão Europeia, "Survey on 'scams and fraud experienced by consumers': final report" (Bruxelas, 2020)).
101 Botão e Cruz, Fraudes Cibernéticas, Golpes e Suas Vítimas; ver também A Globalização do Crime: Uma Avaliação da Ameaça do Crime Organizado Transnacional (publicação das Nações Unidas, 2010), cap. 8.
102 United States Federal Bureau of Investigation, "Como podemos ajudá-lo: golpes de férias", disponível em http:///www.fbi.gov.
103 Em algumas regiões, os reguladores do setor público podem ser responsáveis por identificar e responder a fraudes. Esses reguladores incluem agências com a missão de proteger os consumidores ou regular práticas profissionais.
104 Keith B. Anderson, "Fraude de consumo de massa: quem é mais suscetível a se tornar uma vítima?", Working Paper, No. 332 (Washington DC, Bureau of Economics, Federal Trade Commission, 2016). Veja também a discussão sobre marketing de massa no capítulo IV do presente artigo.

vender serviços financeiros, como empréstimos, planos de seguro ou produtos de pensão.[105] Esses casos geralmente estão relacionados a produtos cujo valor está no futuro, e as vítimas recebem uma projeção excessivamente otimista do desempenho futuro ou não recebem uma explicação adequada sobre os riscos. Os fraudadores também podem deixar de divulgar taxas, comissões ou requisitos legais para a vítima, o que pode resultar em perdas e penalidades adicionais.[106]

Produtos e serviços que têm sido comumente apresentados em fraudes de produtos e serviços de consumo incluem pedras preciosas, animais de estimação, ingressos para eventos, produtos médicos, alimentos, seguros, produtos e serviços de clarividência ou psíquicos, empréstimos e alívio de dívidas.[107] No entanto, há uma variedade quase infinita de produtos e serviços que podem ser usados em esquemas fraudulentos, pois os fraudadores buscam se adaptar continuamente ecapitalizar novos mercados edemandas dos consumidores. Isso foi exemplificado durante a pandemia da doença do coronavírus (COVID-19), quando produtos médicos falsos ou inexistentes estavam sendo anunciados.[108]

Este aumento na variedade foi facilitado pelo crescimento de sites comerciais on-line, particularmente sites de vendas e leilões *peer-to-peer* e, cada vez mais, plataformas de mídia social nas quais todos os tipos de produtos são vendidos.[109] Produtos e serviços são comercializados por meio de várias mídias, incluindo sites falsos, sites legítimos de compras e leilões e e-mails de spam. Outras abordagens incluem correio postal, chamadas de marketing evendas de alto volume de "*boiler rooms*", vendas porta a porta, mala direta e chamadas telefônicas não solicitadas.[110] Alguns infratores tiram vantagem de um mercado vibrante em "listas de *leads*" que são compiladas por meios legítimos ou ilegítimos (como uma violação de dados ou campanha de *phishing* on-line), ou mesmo diretórios de indivíduos que foram vítimas no passado ("suckers lists").[111] As TICs aumentaram muito a capacidade de comercializar evender produtos e serviços em escala global e aum custo comparativamente baixo. Em alguns casos, o consumidor individual pode perder dinheiro, mas, dependendo das circunstâncias e métodos empregados pelos infratores, uma plataforma de vendas ou provedor de serviços financeiros também pode incorrer em perda financeira. Metodologias-chave incluem:

- Desenvolver sites falsos com a finalidade de comercializar e/ou vender produtos e serviços. Os infratores podem comercializar o site usando canais digitais, como mídias sociais ou e-mails de spam, ou podem manipular mecanismos de busca na Internet para aumentar a probabilidade de que aqueles que procuram produtos ou serviços relevantes acessem seu site.[112]
- Criar vendedores falsos em plataformas legítimas de vendas, leilões ou mídias sociais que usam contas abertas com identidades falsas ou roubadas. Esses vendedores exploram plataformas legítimas que fornecem acesso a um grande volume de usuários que buscam produtos e serviços. Por exemplo, um grupo criminoso organizado postou centenas de milhares de listagens de itens de alto valor, como automóveis, em vários sites de leilão.[113]

A fraude online ao consumidor não precisa ser sofisticada ou complexa. O abuso de um site legítimo de vendas ou leilões pode exigir pouco mais do que uma única pessoa abrindo uma conta em um site de leilões

105 A fraude de investimento é incluída como uma categoria separada abaixo (veja também Reurink, Fraude Financeira).
106 Veja, por exemplo, Skidmore, Protecting People's Pensions.
107 Os investimentos do consumidor são incluídos como uma categoria separada abaixo (veja também Beals, DeLiema e Deevy, "Framework for a taxonomy of fraud"; e Mark Button, Chris Lewis e Jacki Tapley, "Fraud typologies and the victims of fraud: literature review" (Londres, National Fraud Authority, 2009)).
108 Reino Unido, Agência Nacional do Crime, "Cuidado com fraudes e golpes durante a pandemia de COVID-19", 26 de março de 2020.
109 Emma Fletcher, "Mídias sociais: uma galinha dos ovos de ouro para golpistas", Comissão Federal de Comércio, 6 de outubro de 2023.
110 Marguerite DeLiema e Lynn Langton, "Vítimas mais velhas de golpes de marketing de massa: uma análise de dados apreendidos de golpistas", Innovation in Aging, vol. 5, Supl. No. 1(2021); Coretta Phillips, "De 'comerciantes desonestos' a grupos de crime organizado: fraude porta a porta de adultos mais velhos", The British Journal of Criminology, vol. 57, No. 3(maio de 2017); eShover, Coffey e Sanders, "Discando por dólares".
111 Levi, "Fraude organizada", em The Oxford Handbook of Organized Crime, p. 460; e Skidmore e Aitkenhead, "Compreendendo as características de crimes graves de fraude"
112 O fraudador pode pagar a empresa de tecnologia ou perpetrar "fraude de clique", em que bots são usados para clicar repetidamente em um link de site para inflar sua classificação de pesquisa, fazendo com que o site pareça mais legítimo.
113 Ver Estados Unidos da América v. Bogdan Nicolescu, Tiberiu Danet e Radu Miclaus, disponível no portal de gestão de conhecimento SHERLOC

e postar um anúncio para vender um produto inexistente. O papel do crime organizado raramente é revelado na troca com a vítima, mas sim na compreensão do planejamento e preparação que estão por trás disso. Por exemplo, a produção, transporte, venda e distribuição de produtos falsificados são partes de um processo complexo que requer o envolvimento de grupos criminosos organizados com altos níveis de coordenação entre co-infratores.[114] No contexto da fraude cibernética, os principais estágios incluem o estabelecimento e o marketing do perfil do site ou plataforma, o envolvimento da vítima para manter o engano (ou obter mais pagamentos) e a movimentação de dinheiro. Os perpetradores podem adotar uma variedade de métodos para receber pagamentos, que incluem convencer um provedor de serviços de pagamento de que sua empresa é legítima, desviar clientes para sites de pagamento falsos, pedir às vítimas que paguem usando cartões de débito pré-pagos e/ou usar contas de terceiros de mulas de dinheiro ou contas abertas usando identidades roubadas ou falsas. Alguns fraudadores transnacionais recrutam correligionários no país-alvo para facilitar a lavagem de dinheiro.[115] Contas bancárias são comumente registradas para identidades falsas, roubadas ou emprestadas (por exemplo, mulas de dinheiro), deixando assim um rastro financeiro limitado.

ESTUDO DE CASO: FRAUDE AO CONSUMIDOR EM COMPRAS ONLINE

Um site independente de vendas on-line anunciou bens de consumo de alta demanda ao público no Reino Unido da Grã-Bretanha e Irlanda do Norte e recebeu milhares de pedidos de consumidores ao longo de um período de aproximadamente três meses, a maioria dos quais não foi atendida. O grupo criminoso organizado assumiu a forma de uma cadeia de suprimentos na qual havia um infrator no exterior que era ostensivamente o fornecedor dos bens, e um centro de distribuição ev arejista on-line localizados em regiões separadas no Reino Unido. A adoção de uma estrutura formal de cadeia de suprimentos criou um verniz de legitimidade que poderia ser usado para enganar o provedor de serviços de pagamento a fornecer acesso à sua facilidade de pagamento on-line para receber pedidos de clientes. A maioria dos produtos vendidos nunca existiu, e o dinheiro das compras foi transferido para oexterior para ofornecedor fictício e sacado como dinheiro.

Fonte: Michael Skidmore e Beth Aitkenhead, "Compreendendo as características de crimes graves de fraude no Reino Unido" (Londres, The Police Foundation, 2023).

ESTUDO DE CASO: FRAUDE AO CONSUMIDOR EM LEILÃO ONLINE

Um grupo criminoso organizado publicou anúncios de produtos de alto valor em vários sites de leilão online. Os arquivos de imagem postados em cada anúncio estavam infectados com malware e, quando clicados, o malware infectava o dispositivo do cliente. O objetivo do malware era redirecionar imperceptivelmente os clientes para páginas falsas que eram idênticas às do site legítimo. As páginas incluíam uma função de chat ao vivo que permitia ao comprador falar com agentes de atendimento ao cliente que eram cúmplices do grupo. Os clientes eram instruídos a pagar pelos itens por meio de um 'agente de custódia', que supostamente manteria o dinheiro do comprador até que ele confirmasse o recebimento do item. No entanto, o dinheiro era transferido para contas controladas pelos criminosos, e as vítimas não recebiam os itens encomendados nem reembolsos.

Fonte: Estados Unidos da América v. Bogdan Nicolescu, Tiberiu Danet e Radu Miclaus, disponível no portal de gerenciamento de conhecimento Sharing Electronic Resources and Laws on Crime (SHERLOC).

114 Hulme, Disley e Blondes, eds., Mapeando o risco de crimes graves e organizados.
115 Christine Conradt, "Fraude em leilões online e teorias criminológicas: o caso Adrian Ghighina", International Journal of Cyber Criminology, vol. 6, No. 1(2012); eJack M. Whittaker eMark Button, "Compreendendo golpes de animais de estimação: um estudo de caso de fraude de taxa antecipada e não entregue usando contas de vítimas", Journal of Criminology, vol. 53, No. 4(dezembro de 2020).

Fraude de emprego

Fraude de emprego envolve o marketing em massa de oportunidades de emprego ou negócios falsas ou enganosas para membros do público.[116] Esse tipo de fraude envolve anunciar uma oportunidade que é totalmente fictícia ou muito menos lucrativa do que a anunciada, e as vítimas perdem dinheiro sem receber o emprego ou remuneração prometidos. Os fraudadores geralmente solicitam pagamentos iniciais das vítimas antes de assumir uma posição ou abrir seu negócio; esse pagamento é explicado de várias maneiras diferentes, incluindo ser para a compra ou aluguel de produtos ou equipamentos necessários para estabelecer o negócio, arranjos de viagem, fornecimento de treinamento ou conclusão de verificações de pontuação de crédito.[117] Em outros esquemas, os fraudadores enviam pagamentos adiantados usando cheques fraudulentos para cobrir os custos iniciais de uma vítima, antes de alegar que fizeram um pagamento a maior e pedir às vítimas que transfiram o dinheiro de volta.[118] Pessoas que precisam de oportunidades econômicas podem ser particularmente vulneráveis a esse tipo de fraude.

O crescimento substancial no recrutamento online traz muitas vantagens para empresas legítimas, incluindo a capacidade de direcionar comunicações e avaliar um alto volume de candidatos a emprego. No entanto, essas mesmas vantagens podem ser exploradas por fraudadores que usam sites de empregos legítimos, fóruns online e mídias sociais para disseminar anúncios de empregos fraudulentos. É um desafio considerável para sites de empregos identificar anúncios fraudulentos que são postados em suas plataformas.[119]

Os fraudadores exploram a demanda por posições desejáveis, particularmente entre os candidatos a emprego com menos habilidades ou qualificações, oferecendo condições de trabalho (por exemplo, trabalho em casa ou trabalho flexível) ou níveis de pagamento normalmente fora de alcance. Um estudo nos Estados Unidos da América descobriu que encontrar anúncios de emprego online fraudulentos era uma ocorrência regular para muitos trabalhadores envolvidos em trabalho temporário ou inseguro (como na economia sob demanda).[120] A incerteza econômica e o alto desemprego são um terreno fértil para fraudes trabalhistas, em que a ausência de oportunidades na economia legítima leva a uma tomada de decisão mais desesperada e arriscada entre aqueles que procuram emprego.[121]

As vítimas também correm o risco de serem alvos repetidamente porque muitas são solicitadas a fornecer informações pessoais ou documentos de identidade durante o processo de inscrição fraudulento.[122] A principal motivação em algumas fraudes de emprego é roubar dados pessoais das vítimas. Em outros casos, as próprias vítimas são atraídas para facilitar a criminalidade. Por exemplo, oportunidades de negócios fraudulentas podem operar como esquemas de pirâmide ilegais nos quais os lucros para a vítima vêm do recrutamento de outras pessoas para se registrarem no esquema.[123] Vítimas que aceitam empregos como entregadores podem se envolver na entrega de contrabando ou bens roubados, e outras podem se envolver como mulas de dinheiro para facilitar a lavagem de dinheiro.[124]

---

116 Beals, DeLiema e Deevy, “Estrutura para uma taxonomia de fraude”.
117 Alexandrea J. Ravenelle, Erica Janko e Ken Cai Kowalski, “Bons empregos, empregos fraudulentos: detecção, normalização e internalização de golpes de emprego online durante a pandemia da COVID-19”, New Media and Society, vol. 24, n.º 7(julho de 2022); e Cassandra Cross e Deanna Grant-Smith, “Fraude de recrutamento: maiores oportunidades de exploração em tempos de incerteza?”, Social Alternatives, vol. 40, n.º 4(2021).
118 Beals, DeLiema e Deevy, “Estrutura para uma taxonomia de fraude”.
119 Mohammed A. Sofy, Mohammed H. Khafagy e Rasha M. Badry, “Um modelo árabe inteligente para detecção de fraudes em recrutamento usando aprendizado de máquina”, Journal of Advances in Information Technology, vol. 14, No. 1(fevereiro de 2023); e Syed Mahbub e Eric Pardede, “Usando recursos contextuais para detecção de fraudes em recrutamento online”, 27ª Conferência Internacional sobre Desenvolvimento de Sistemas de Informação (ISD2018), realizada em Lund, Suécia, em 2018.
120 Ravenelle, Janko e Cai Kowalski, “Bons empregos, empregos fraudulentos”.
121 Cross and Grant-Smith, “Recruitment fraud”; and Delali Kwasi Dake, “Online recruitment fraud detection: a machine learning-based model for Ghanaian job websites”, International Journal of Computer Applications, vol. 184, No. 51 (March 2023)
122 Sofy, Khafagy e Badry, “Um modelo árabe inteligente”.
123 Beals, DeLiema e Deevy, “Estrutura para uma taxonomia de fraude”.
124 Ravenelle, Janko e Cai Kowalski, “Bons empregos, empregos fraudulentos”; e Mohanamerry Vedamanikam, Saralah Devi Mariamdaran Chethiyar e Norruzeyati bt Che Mohd Nasir, “Modelo para recrutamento de mulas de dinheiro na Malásia: perspectiva de conscientização”, PEOPLE: International Journal of Social Sciences, vol. 6, nº 2(2020).

Fraude de investimento do consumidor

A fraude de investimento do consumidor geralmente envolve a comercialização e venda de títulos, incluindo ações e imóveis, títulos governamentais ou corporativos, commodities como metais preciosos e moedas estrangeiras.[125] Os perpetradores enganam intencionalmente os investidores, fornecendo informações que deturpam grosseiramente os ganhos potenciais que podem ser obtidos com um investimento[126] ou se relacionam com um investimento que não existe.[127]

A comissão desses tipos de fraude pode exigir uma profunda consciência dos contornos da regulamentação e controles relacionados que governam os mercados. A linha entre prática legítima e ilegítima pode ser permeável e difícil de perceber. Em alguns casos, os infratores exploram mecanismos de confiança registrando-se como uma entidade regulamentada ou explorando outros atores legítimos com status regulamentado. Ao ocupar essa margem cinzenta entre prática legítima e ilegítima, eles criam barreiras para a aplicação da lei e reguladores que são obrigados a navegar e produzir evidências suficientes e robustas de engano e demonstrar que um crime ocorreu.[128] De fato, embora antiéticos, alguns podem empregar esquemas que causam danos aos investidores, mas transparecem não ser criminosos. Os esquemas de pirâmide e Ponzi[129] são modelos operacionais comuns para os infratores, em que o esquema de investimento é sustentado pela manutenção de um fluxo contínuo de investimento de novos investidores em vez de retornos de um produto ou investimento real que pode nunca ter existido.[130] Pesquisas descobriram que gênero e idade podem afetar a vulnerabilidade a tais esquemas, com muitos esquemas aproveitando a disparidade salarial de gênero e alegando ajudar as mulheres por meio da provisão de oportunidades econômicas e um senso de comunidade.[131]

Os infratores de fraude de investimento fazem grandes esforços para cultivar um verniz de legitimidade e comumente adotam as estruturas, processos e linguagem de uma organização formal e legítima, incluindo uma divisão clara de trabalho, com uma hierarquia e funções designadas atribuídas ao pessoal.[132] A complexidade da operação é variável e pode depender de sua duração pretendida. As chamadas operações de rasgar e rasgar podem operar por um curto período antes de desaparecer com o dinheiro dos investidores, enquanto outros esquemas podem operar sem serem detectados por muitos anos.[133]

As vítimas de fraude de investimento sofrem as maiores perdas quando comparadas com vítimas de outros tipos de fraude que visam membros individuais do público. As vítimas são enganadas e preparadas com ex-

125 Beals, DeLiema e Deevy, "Estrutura para uma taxonomia de fraude".
126 Por exemplo, a venda de investimentos em "penny stocks" em empresas menores que oferecem retornos anormais a investidores em potencial. Uma abordagem comum é o esquema "pump and dump", no qual um produto é promovido ativamente para inflar artificialmente (ou "pump") a demanda por uma ação desconhecida ou pouco conhecida, antes que o fraudador então "despeje" suas ações para obter para si um grande lucro e outros investidores consequentemente experimentem perdas (Bill Hu, Thomas McInish e Li Zeng, "Gambling in penny stocks: the case of stock spam e-mails", International Journal of Cyber Criminology, vol. 4, Nos. 1 e 2(julho/dezembro de 2010); e Beals, DeLiema e Deevy, "Framework for a taxonomy of fraud").
127 Por exemplo, os esquemas Ponzi comercializam oportunidades de investimento, mas nenhum dinheiro é realmente investido, e os pagamentos aos investidores existentes são retirados do dinheiro recebido de novos investidores (Surendranath Rakesh Jory eMark J. Perry, "Ponzi schemes: a critical analysis", Journal of Financial Planning (2011)).
128 Branislav Hock e Mark Button, "Por que as pessoas aderem a esquemas de pirâmide?", Journal of Financial Crime, vol. 30, No. 5(2023); e Skidmore, Protegendo as pensões das pessoas.
129 Os esquemas Ponzi e Pyramid operam com princípios semelhantes, usando dinheiro atraído de novos investidores para pagar investidores anteriores, mas os esquemas de pirâmide são distintos porque os investimentos são vendidos como uma oportunidade de negócio e os próprios investidores são recompensados por recrutar novos investidores (veja, por exemplo, Claire Nolasco, Michael Vaughn e Rolando V. del Carmen, "Revisiting the choice model of Ponzi and Pyramid schemes: analysis of case law", Crime, Law and Social Change, vol. 60, No. 4(novembro de 2013)).
130 Hock e Button, "Por que as pessoas aderem a esquemas de pirâmide?"; e Skidmore e Aitkenhead, "Compreendendo as características de crimes graves de fraude".
131 Li Huang e outros, "Gender and age-based investor affinities in a Ponzi scheme", Humanities and Social Sciences Communications, vol. 8, art. No. 60 (2021); Delano Law Offices, "Pyramid schemes target females", 1 de fevereiro de 2022; e Taylor Walsh, "Multilevel marketing, an unwinnable lottery: how MLMs illegally target women and minorities using deceptive and predatory recruitment practices and the need for specific and expanded legal protections", Georgetown Journal of Gender and the Law, No. XXIV-1 (2002).
132 Shover, Coffey e Sanders, "Discando por dólares".
133 Levi, "Fraude organizada e fraudes organizacionais"; e Skidmore e Aitkenhead, "Compreendendo as características de infrações graves de fraude".

pectativas de um retorno financeiro que são inteiramente falsos ou grosseiramente exagerados. Muitos investidores perdem todo ou uma grande parte de seu dinheiro. Independentemente de qual método específico é empregado, as vítimas geralmente são vendidas com uma expectativa do valor que será ganho com seu investimento no futuro, o que significa que pode levar anos após o investimento inicial antes que percebam que foram fraudadas. As particularidades dos diferentes esquemas e do engano subjacente variam amplamente, mas podem incluir:

- Um engano completo em que o serviço ou produto de investimento nunca existiu;
- Venderam intencionalmente ações inúteis ou supervalorizadas para investimentos de alto risco que provavelmente não renderão o retorno prometido;
- Técnicas de manipulação de mercado que inflacionam artificialmente o valor dos investimentos para pessoas desavisadas investidores (veja a descrição de um golpe de saída abaixo);

As perdas e o impacto sobre as vítimas podem depender das metodologias empregadas pelos infratores. Se, por exemplo, as economias de pensão das pessoas forem visadas, isso pode ter um impacto transformador na vida da vítima individual, enquanto alguns investimentos em criptomoedas podem ser focados em receber quantias menores, mas de um número maior de vítimas (veja o estudo de caso abaixo). Uma vez que o dinheiro tenha sido roubado, a vítima pode ser visada novamente pelos mesmos ou outros infratores, que em alguns casos alegam ter uma afiliação a um órgão legítimo que é capaz de rastrear e recuperar o dinheiro perdido, mas a vítima é solicitada apagar uma taxa inicial (a chamada fraude de recuperação).[134]

Fraude de investimento em criptomoeda

Os padrões de fraude em investimentos têm visto mudanças na resposta às novas tecnologias digitais e formas de financiamento, especialmente nos setores financeiros descentralizados que usam criptomoedas e tecnologia de blockchain para conduzir transações financeiras sem a necessidade da função intermediária de uma instituição financeira (por exemplo, um banco).

Assim, a fraude de investimento do consumidor parece estar aumentando, em parte devido ao aumento da fraude que envolve investimentos em criptomoedas. Este novo meio para fraude de investimento capitaliza a velocidade e agilidade oferecidas pelos espaços digitais, permitindo que os infratores se envolvam em marketing de massa com rapidez e a um custo relativamente baixo e, em alguns casos, aproveitem tecnologias automatizadas (ou bots) para ofender repetidamente.[135] Em novos mercados financeiros, como omercado de criptomoedas, os desafios na regulamentação criam lacunas maiores para explorar. Os perpetradores comumente exploram mídias sociais e aplicativos de comunicação digital para comercializar seus produtos, em alguns casos utilizando imagens de celebridades ou imagens da cultura popular para persuadir as vítimas a investir seu dinheiro. Esses novos métodos de marketing têm potencialmente expandido o alcance da fraude de investimento para enredar um volume maior de investidores mais diversos, incluindo um grande número de investidores na faixa dos 30 ou 40 anos.[136]

Os métodos empregados em fraudes de criptoinvestimentos variam tanto em complexidade técnica quanto em novidade, com algumas técnicas, como as seguintes, transpostas de outros métodos, como manipulação de mercado e aliciamento financeiro:

- Plataformas fraudulentas de investimento em criptomoedas são desenvolvidas e comercializadas para persuadir as vítimas a investir em uma criptomoeda. Assim como as formas tradicionais de fraude de investimento, a confiança da vítima pode ser cultivada ao longo do tempo, às vezes com o uso de técnicas de preparação financeira (veja a seção sobre fraude de relacionamento e confiança abaixo). Em

134 Por exemplo, ver Estados Unidos, Federal Bureau of Investigation, "Aumento de empresas que alegam falsamente a capacidade de recuperar fundos perdidos em golpes de investimento em criptomoedas", 11 de agosto de 2023.
135 Arianna Trozze, Toby Davies e Bennett Kleinberg, "De degenerados e fraudadores: usando ferramentas investigativas de código aberto para investigar fraudes financeiras descentralizadas e lavagem de dinheiro", Journal of Forensic Science International: Digital Investigation, vol. 46 (setembro de 2023).
136 Estados Unidos, Departamento de Justiça, Gabinete de Relações Públicas, "O Departamento de Justiça apreende mais de US$ 112 milhões em fundos vinculados a criptomoedas". Esquemas de investimento de renda", comunicado de imprensa, 3de abril de 2023.

alguns casos, um site ou aplicativo fraudulento é desenvolvido para mostrar que o investimento das vítimas está tendo um bom desempenho, servindo para encorajar mais investimentos e o recrutamento de outros investidores de dentro de sua rede social.[137]

- Golpes de saída, ou "rug pulls", envolvem a criação de um token de golpe que pode ser negociado com outras criptomoedas em uma bolsa descentralizada. Uma vez que um número suficiente de vítimas tenha negociado suas moedas pelo token, o infrator pode sacar todo o dinheiro investido, deixando as vítimas com um token sem valor. Uma técnica específica de "pump and dump" segue uma lógica semelhante a uma pirâmide tradicional ou esquema Ponzi, em que os fraudadores inflacionam artificialmente o valor do token por meio do uso de seus próprios fundos e atraem investidores que, por sua vez, incentivam outros investidores. Este processo pode ser concluído em minutos ou horas e, ao retirar o dinheiro, o mesmo infrator pode então estabelecer outro token para atingir outros investidores desavisados.[138]

ESTUDO DE CASO: INVESTIMENTO FRAUDULENTO EM CRIPTOMOEDA

Membros de um grupo criminoso organizado, a maioria dos quais estava localizada na Bélgica, foram descobertos envolvidos em um golpe de saída que a polícia acreditava ter fraudado 223.000 indivíduos de 177 países. Os perpetradores operavam a partir de um site de recompensa social legítimo e incentivavam o investimento em uma criptomoeda específica. Eles empregavam uma técnica de venda em pirâmide que recompensava os membros por recrutar novos membros para se registrar. Dessa forma, os fraudadores inflaram artificialmente (ou "bombearam") o valor do investimento. O grupo criminoso organizado saiu com uma grande quantidade de fundos antes do estouro da bolha ou uso de desinformação para inflar o valor da criptomoeda antes de vendê-la para obter um ganho de capital substancial. Membros do grupo criminoso organizado foram encontrados em posse de €1,1 milhão em dinheiro e €1,5 milhão em criptomoedas.

Fonte: Agência da União Europeia para a Cooperação Policial (Europol), Criptomoedas: *Rastreando a evolução das finanças criminosas, Europol Spotlight Report Series (Luxemburgo, Serviço de Publicações da União Europeia, 2021).*

Fraude por personificação de um indivíduo ou organização de confiança.

Fraude por personificação de um indivíduo ou organização confiável geralmente envolve a manipulação de comunicações para parecer ser de uma pessoa ou organização com quem as vítimas têm, ou acreditam ter, um relacionamento legítimo existente. Isso inclui órgãos públicos como a polícia ou autoridade fiscal, prestadores de serviços no setor privado e até mesmo amigos ou familiares.[139] Uma característica distintiva fundamental de muitos (mas não todos) tipos de fraude nesta categoria é o uso de técnicas de persuasão que apelam menos aos desejos e necessidades das vítimas (como na fraude ao consumidor) e, em vez disso, evocam medo, pavor, ansiedade ou preocupação.[140] Induzir um estado emocional elevado serve para impedir a tomada de decisões e torna as vítimas mais suscetíveis à manipulação.

137 Por exemplo, ver Estados Unidos, Federal Bureau of Investigation, "Scammers target and exploit owners of cryptocurrencies in liquidity mining scam", 21 de julho de 2022.
138 Pengcheng Xia et al., "Desmistificando tokens fraudulentos na bolsa descentralizada Uniswap" (2021).
139 Estados Unidos, Comissão Federal de Comércio, Dados e visualizações, Destaque de dados, "Golpes de representação: não são mais oque costumavam ser", 1º de abril de 2024.
140 DeLiema e Witt, Análise de métodos mistos de relatórios de fraude ao consumidor.

A fraude por personificação envolve uma série de pretextos e cenários, como:

- Personificar autoridades públicas. Os perpetradores empregam uma série de técnicas para se disfarçarem como autoridades públicas que representam agências como entidades de aplicação da lei, autoridades fiscais ou departamentos de imigração, previdência social ou saúde. Essa fraude geralmente envolve ameaças de repercussões legais ou outras formas de prejuízo caso a vítima não envie um pagamento.[141]
- Personificar serviços legítimos. Os perpetradores empregam uma série de pretextos, que vão desde cobrança de dívidas e entregas de encomendas até o fornecimento de suporte de TIC. Eles podem até se passar por funcionários de banco buscando evitar a perda de dinheiro para fraudadores. Os fraudadores podem alegar representar um provedor de serviços com o qual a vítima tem um relacionamento estabelecido (por exemplo, um banco ou serviço de entrega), ou podem adotar um verniz de aparência oficial para convencer a vítima de que são legítimos; por exemplo, fraudadores[142] que alegam representar um escritório de advocacia responsável por cobrar uma dívida inexistente da vítima.[143] Outros exemplos importantes incluem fraude de loteria e prêmio, em que as vítimas são informadas de que ganharam na loteria ou outro jogo e são persuadidas a fazer um pagamento antes de terem acesso aos fundos.[144] Vários motivos são dados, incluindo uma suposta taxa de processamento, transferência ou administração ou encargos fiscais. No entanto, uma vez que o pagamento foi feito, as vítimas não recebem o prêmio prometido. Técnicas comuns incluem a representação de uma autoridade pública, uma loteria conhecida ou organização de prêmios ou um esquema de loteria no exterior. Em outros exemplos, fraudadores alegam representar instituições de caridade em campanhas de marketing de massa para obter doações de vítimas.[145] Pessoas em contextos vulneráveis, incluindo idosos e pessoas com deficiência, podem estar particularmente em risco desses tipos de fraude devido à sua dependência de serviços sociais e níveis mais altos de isolamento social, como visto no estudo de caso sobre produtos e serviços de consumo e fraude de investimento no capítulo anterior.
- Fraude de suporte técnico. Isso é altamente prevalente em certas regiões, como América do Norte e Europa, com grande parte das infrações emanando da Índia.[146] Eles geralmente envolvem o fraudador se passando por uma empresa de software legítima para convencer as vítimas de que suas máquinas estão em risco e precisam de suporte técnico (por exemplo, uma infecção por malware). As vítimas são então persuadidas a fornecer acesso remoto à sua máquina, antes de serem solicitadas a pagar uma taxa para fornecer um serviço fictício.[147] Em alguns casos, cobranças adicionais são feitas nas contas das vítimas, malware é instalado em suas máquinas ou seus dados pessoais podem ser roubados. Algumas empresas fraudulentas adotam métodos semelhantes à fraude ao consumidor, comercializando em massa serviços de suporte técnico por meio de sites que imitam provedores de serviços legítimos.
- Personificar um amigo ou membro da família. Isso normalmente envolve mensagens que inventam um cenário em que a pessoa está em alguma dificuldade aguda, como estar no hospital, sofrer um acidente ou ser presa, e afirma que isso pode ser resolvido se a vítima enviar uma quantia de dinheiro específica. Muitas vezes o operador finge ser o filho ou neto da vítima.[148]

141 Um exemplo envolveu uma mensagem enviada por e-mail e nas redes sociais, alegando ser da Europol, informando às vítimas que elas tinham sido vistas acessando material de abuso sexual infantil e precisavam fazer um pagamento entre € 3.000 e €7.000 para evitar o processo (Europol, " Esquemas de fraude online: uma rede de enganos", Europol Spotlight Report Series (Luxemburgo, Serviço de Publicações da União Europeia, 2023), p. 11).
142 Veja, por exemplo, Estados Unidos, Comissão Federal de Comércio, "Cobradores de dívidas fantasmas permanentemente banidos da indústria na FTC acordo", comunicado de imprensa, 13 de dezembro de 2021.
143 Mortley, "Um crime de oportunidade". Em um caso, comunicações fraudulentas foram enviadas alegando ser de uma empresa que havia sido nomeada pela Organização Mundial da Saúde (OMS) para administrar um esquema de compensação de loteria. Os destinatários foram informados de que haviam sido selecionados como beneficiários ou vencedores de um pagamento de prêmio de compensação de loteria por perdas e danos sofridos durante a pandemia de COVID-19 (OMS, "Fraudulent 'COVID-19 Compensation Lottery Prize' scam, falsely alleges association with WHO and others", press release, 6 de agosto de 2021).
144 Veja também Estados Unidos, Federal Trade Commission, "Fake prize, sweepstakes, and lottery scams", maio de 2021.
145 Por exemplo, esquemas fraudulentos comercializados através de páginas web e e-mails fraudulentos, pretendendo apoiar a Ucrânia ou os ucranianos afetados pelo conflito armado, em alguns casos falsificando domínios de organizações humanitárias (ver Europol, "Esquemas de fraude online").
146 Liu e outros, "Entendendo, medindo e detectando". Veja também Estados Unidos, Escritório de Relações Públicas, "Dezenas de indivíduos indiciado em golpe multimilionário de call center indiano visando vítimas dos EUA", comunicado à imprensa, 27 de outubro de 2016.
147 Najmeh Miramirkhani, Oleksii Starov e Nick Nikiforakis, "Disque um para golpes: uma análise em larga escala de golpes de suporte técnico", artigo de conferência, Simpósio de Segurança de Redes e Sistemas Distribuídos realizado em San Diego, Califórnia, de 26 de fevereiro a 1º de março de 2017.
148 Estados Unidos, Federal Bureau of Investigation, "O golpe dos avós: não deixe que aconteça com você", 2 de abril de 2012.

Alguns esquemas de fraude Alguns esquemas de fraude envolvem o uso de detalhes pessoais de postagens de mídia social do amigo ou parente para tornar a comunicação mais convincente, como saber que eles estão de férias em um determinado local. Exemplos emergentes incluem infratores usando inteligência artificial generativa para clonar a voz de um amigo ou parente em uma chamada telefônica para a vítima, criando uma resposta ainda mais convincente ou visceral da vítima.[149]

Os tipos de fraude mencionados acima geralmente envolvem comunicação em massa por meio de e-mail de spam, mídia social, mensagens de texto ou "robodialling", em que as chamadas telefônicas são automatizadas usando uma mensagem gravada. Essas tecnologias facilitam o contato quase simultâneo com milhares de vítimas ao mesmo tempo, dando a elas um alcance imenso.[150] Alguns grupos criminosos organizados operam em call centers, com operadores de chamadas alegando representar órgãos governamentais ou marcas de empresas conhecidas. Há algumas evidências que sugerem que os adultos mais velhos são alvos e particularmente vulneráveis a fraudes, como representação do governo ou fraude de suporte técnico.[151]

Fraude de identidade

Fraude de identidade envolve o uso de informações de identidade roubadas ou falsas para obter acesso direto a bens, serviços ou dinheiro das vítimas. Informações roubadas podem ser usadas para fazer compras ou acessar contas financeiras. Fraude de identidade pode ser perpetrada sem qualquer comunicação direta ou ação tomada pelo indivíduo cuja identidade está sendo abusada, porque o engano é frequentemente direcionado ao fornecedor dos bens, serviços ou dinheiro (por exemplo, banco ou fornecedor comercial). Desta forma, o dano é distribuído entre diferentes atores, incluindo a vítima cuja identidade é abusada, o provedor de serviços financeiros ou outra empresa de quem o dinheiro é retirado e, em alguns casos, o fornecedor dos bens ou serviços adquiridos usando os fundos roubados.

A manipulação e o abuso de identidade podem servir a uma variedade de funções diferentes na prática do crime organizado, além de perpetrar fraudes, principalmente para obstruir tentativas de rastrear a criminalidade até os perpetradores.[152] Da mesma forma, desempenha um papel fundamental na facilitação dos enganos empregados em tipos de fraude, como fraude romântica e fraude ao consumidor.[153] O foco da presente seção são as metodologias específicas como parte das quais informações de identidade roubadas ou falsas são usadas para obter acesso direto a bens, serviços ou dinheiro das vítimas, como o uso de informações roubadas para fazer compras ou acessar contas financeiras. A vítima em muitos desses casos é a empresa que é enganada para fornecer financiamento, bens ou serviços ao fraudador.

É importante ressaltar que a perpetração de fraude de identidade não depende do envolvimento de grupos criminosos organizados. Por exemplo, a personificação de um portador de cartão requer pouco mais do que uma bolsa roubada e uma loja local para fazer uma compra rápida. No entanto, a capacidade de perpetrar fraude de identidade em escala e obter altos lucros é amplamente aumentada pelas habilidades e recursos disponíveis para organizações grupos criminosos. Essa ameaça se torna particularmente aguda pela proliferação de alvos disponíveis dentro de economias digitais em crescimento.

---

149 Alvaro Puig, "Golpistas usam IA para aprimorar seus esquemas de emergência familiar", Comissão Federal de Comércio, 20 de março de 2023.
150 Um exemplo comum consiste no uso de mensagens fraudulentas que alegam ser da administração da previdência social. Em 2020, tal esquema teve como alvo quase metade de todos os adultos nos Estados Unidos ao longo de um período de três meses (DeLiema eWitt, Mixed Methods Analysis of Consumer Fraud Reports, p. 2)
151 Liu e outros, "Compreendendo, medindo e detectando"; Lei Yu e outros, "Vulnerabilidade de adultos mais velhos a golpes de representação do governo", JAMA Network Open, vol. 6, No. 9 (setembro de 2023); e DeLiema e Langton, "Vítimas mais velhas de golpes de marketing de massa".
152 Baechler, "Fraude de documentos".
153 Veja, por exemplo, Cassandra Cross e Rebecca Layt, "'Suspeito que as fotos sejam roubadas': fraude romântica, crime de identidade e respondendo a suspeitas de identidades inautênticas", Social Science Computer Review, vol. 40, No. 4(agosto de 2022).

Existem diferentes formas de informação de identidade que podem ser adquiridas, e cada uma pode ser explorada de diferentes maneiras: informações pessoais que compõem identidades digitais em diferentes ambientes online, como nomes ou datas de nascimento; dados de contas financeiras, como números de cartão de crédito; informações de contas online, como nomes de usuário e senhas; e dados biométricos, como uma impressão digital roubada de um dispositivo eletrônico.[154]

Dados roubados podem ser usados para comprar bens e serviços, enviar solicitações de empréstimos e outros financiamentos ou acessar e transferir dinheiro das contas das vítimas. Os recursos e técnicas que podem ser empregados por fraudadores para obter acesso a informações pessoais incluem o seguinte:

- Intrusão no sistema. Alguns fraudadores são ativos na aquisição de informações pessoais por meio de técnicas ilícitas de hacking, implantação de malware ou phishing (veja a seção sobre roubo de identidade abaixo para mais detalhes).
- Mercados criminosos online. Há uma vibrante economia subterrânea envolvida na compra e venda de dados pessoais que podem ser explorados por fraudadores de identidade.[155] A oportunidade de adquirir informações dessa forma remove algumas das barreiras técnicas para fraudadores que, de outra forma, não teriam essas capacidades de roubar informações pessoais.
- Engenharia social. Isso geralmente é alcançado por um anúncio ou outra comunicação não solicitada por e-mail ou outros meios online, mensagem de texto ou uma chamada telefônica não solicitada, por meio da qual as vítimas são enganadas a fornecer informações pessoais. O grau de sofisticação é variável, mas métodos mais complexos, como falsificar sites legítimos, podem fornecer aos infratores acesso direto a contas online (veja o estudo de caso abaixo).

Uma série de técnicas são empregadas para perpetrar fraude de identidade. Os métodos principais são apropriação indébita de conta, cartão não presente e fraude de aplicação.

Fraude de apropriação indébita de conta

Na fraude de apropriação indébita de conta, os criminosos adquirem credenciais legítimas para acessar contas de usuários. Isso pode incluir contas bancárias, mas também outros tipos de contas financeiras (por exemplo, provedores de moeda virtual), sites de varejo ou quaisquer provedores de bens e serviços. O uso das credenciais de conta roubadas das vítimas significa que as transações ou outras atividades do infrator se tornam difíceis de distinguir daquelas do titular real da conta. A conta pode ser alavancada para vários propósitos, incluindo uma transferência direta de fundos para contas controladas pelos infratores e o uso da conta para comprar bens ou serviços fraudulentamente. Em alguns casos, a aquisição de informações para acessar a conta de uma vítima é a primeira de uma sequência de etapas necessárias para acessar o dinheiro, bens ou serviços, incluindo formas subsequentes de invasão do sistema. Essas etapas incluem adaptações para superar a autenticação de dois fatores destinada a impedir o acesso ilegítimo às contas. Isso levou os infratores a implantar técnicas e tecnologias adicionais, incluindo:

- Troca de SIM, que envolve enganar um provedor de telecomunicações para portar o número de telefone de uma vítima para um cartão SIM em posse do infrator. Isso fornece os meios para que os infratores contornem as proteções de autenticação de dois fatores dos provedores de serviços financeiros para obter acesso direto a uma conta. Um grupo na Espanha conseguiu fazer transferências fraudulentas no valor de 3 milhões de euros, através da implementação de um trojan bancário ou outro malware para obter acesso às credenciais bancárias online das vítimas, solicitando aos fornecedores de telecomunicações uma cópia dos cartões SIM das vítimas para interceptar os códigos de autenticação enviados pelo banco e, em seguida, transferindo fundos para as contas das mulas de dinheiro.[156]

154 Europol, “Online fraud schemes”; and Bert-Jaap Koops, Katja de Vries and Mireille Hildebrandt, eds., D7.14b: Idem-Identity and Ipse-Identity in Profiling Practices, Future of Identity in the Information Society Report, No. 507512 (2009).
155 Yip, Shadbolt e Webber, “Por que fóruns?”.
156 Europol, Avaliação da ameaça do crime organizado na Internet 2020 (Luxemburgo, Serviço das Publicações da União Europeia, 2020), p. 44.

- Visar métodos de pagamento alternativos, como os cartões de crédito "tokenizados" usados em serviços de pagamento móvel e em carteiras digitais, por meio dos quais os infratores conseguem interceptar as senhas de uso único enviadas por instituições bancárias para autorizar uma transferência de fundos e, assim, fazer compras ou obter dinheiro.[157]

É comum que fundos sejam retirados de contas usando transferências digitais para contas controladas por infratores. No entanto, grupos criminosos organizados também podem obter a posse de identificadores físicos, como cartões bancários ou identificação falsa, para comparecer fisicamente ao banco e sacar dinheiro.[158]

ESTUDO DE CASO: FRAUDE BANCÁRIA

No Reino dos Países Baixos, um grupo atacou dois bancos com o objetivo de obter acesso às contas bancárias dos clientes. O grupo era composto por oito membros principais e outros indivíduos periféricos que facilitavam a fraude. Um e-mail de phishing foi enviado solicitando que os clientes fornecessem informações ou clicassem em um link que os enviava para um site controlado pelos infratores que falsificava o site oficial do banco. Dessa forma, eles obtiveram os detalhes dos clientes para acessar suas contas bancárias on-line. Poucos dias depois, os infratores fizeram uma ligação telefônica para as vítimas e disseram que uma nova medida de segurança havia sido implementada no banco e solicitaram que fornecessem o código de transação única para garantir que sua conta estivesse segura. Depois que o código foi fornecido, o infrator fez uma série de transferências bancárias das contas dos clientes. O dinheiro foi transferido para as contas de mulas de dinheiro para quebrar o rastro financeiro, e o dinheiro foi então rapidamente sacado.

Fonte: Eric Rutger Leukfeldt, "Cibercrime elaços sociais: phishing em Amsterdã", *Trends in Organized Crime,* vol. 17, No. 4 (dezembro de 2014).

Fraude de cartão não presente

Transações com cartão não presente são compras não autorizadas feitas remotamente de um fornecedor, seja online ou por telefone. A aquisição das credenciais financeiras de uma vítima é suficiente para enganar tanto o provedor de serviços financeiros quanto o fornecedor comercial, sem necessidade de interação direta com a vítima ou para obter acesso ao cartão de pagamento físico. Há uma economia subterrânea em expansão na qual os criminosos cibernéticos com a capacidade de adquirir essas informações em massa (por exemplo, por meio de uma violação de dados) podem vendê-las a possíveis fraudadores para obter lucro. Para ilustrar, um site investigado pela polícia continha 150.000 números de cartão de crédito roubados de 1.300 bancos, obtidos principalmente por meio de invasão de sistema; a venda desses dados para fraudadores resultou na perda de US$ 20 milhões de contas mantidas nos Estados Unidos.[159] Uma série de etapas importantes são normalmente exigidas por identidade fraudadores para explorar as credenciais financeiras de uma vítima, algumas das quais podem envolver outros co-infratores, incluindo aqueles online ou que vivem na mesma localidade.

157 Europol, "Esquemas de fraude online", p. 15.
158 Ver, por exemplo, UK Finance, "Grupo de crime organizado condenado após conspiração de fraude de mais de £ 1 milhão", comunicado de imprensa, 6 de novembro de 2023.
159 Estados Unidos da América v. Burkov, disponível no portal de gerenciamento de conhecimento SHERLOC.

Os principais estágios incluem:

- Adquirir conhecimento e recursos de outros membros de grupos online.
- Adquirir credenciais financeiras de grupos online.
- Disfarçar pedidos para evitar o acionamento de algoritmos de detecção de fraude em um site comercial. Isso pode implicar em fazer vários pedidos menores para se misturar com pedidos legítimos.
- Receber os pedidos em um endereço que não pode ser rastreado até os fraudadores – pode ser uma propriedade desocupada ou o endereço de uma "mula". Alternativamente, um insider dentro da empresa de entrega pode ser usado para interceptar o item.
- Revenda dos itens como vendedor individual ou venda em grandes quantidades, representando um vendedor legítimo comerciante em mercados online tradicionais.[160]

ESTUDO DE CASO: FRAUDE DE CARTÃO NÃO PRESENTE

Uma rede de infratores usou dados de cartão de crédito roubados para fazer compras fraudulentas em sites comerciais. Eles adquiriram esses dados de duas maneiras: (a) obtendo e comprando-os de fóruns de carding online; e(b) roubando as informações de um antigo empregador. Os infratores também foram encontrados em posse de skimmers de caixa eletrônico (ATM) que poderiam ser usados para coletar mais detalhes do cartão. Uma etapa preparatória fundamental era invadir contas de clientes em sites comerciais e alterar seus contatos informações, oque significa que os portadores de cartão não seriam notificados sobre as compras feitas pelos infratores. Os produtos eram comprados e entregues em pontos de coleta de encomendas e coletados usando carteiras de identidade falsas ou "mulas" alistadas para coletar os pacotes. A polícia identificou aproximadamente 2.000 pedidos feitos em sites de compras, com um valor estimado de até €60.000. Os produtos eram então revendidos em sites comerciais. Um hardware conectado a um caixa eletrônico para roubar informações de cartão.

Fonte: Paris Tribunal de grande instance, Acórdão, 20 de novembro de 2018 (TGI Paris, 13e ch. corr., jugement du 20 novembre 2018), disponível no portal de gestão de conhecimento Sharing Electronic Resources and Laws on Crime (SHERLOC).

Fraude de aplicação

De forma semelhante à fraude de cartão não presente, a fraude de solicitação explora a ampla disponibilidade de informações pessoais, mas com o objetivo de solicitar crédito em nome da vítima. Isso é comumente feito com o objetivo de obter um empréstimo de um provedor de serviços financeiros. Os infratores precisam acessar um composto de informações pessoais (por exemplo, nome, endereço e data de nascimento) para poder se passar por outro indivíduo de forma confiável. Um padrão emergente é ouso de tecnologia para criar identidades sintéticas combinando identificadores reais e fabricados; uma vez estabelecidas, essas identidades podem ser cultivadas para se tornarem mais dignas de crédito antes de serem usadas para enviar solicitações de produtos financeiros de alto valor. A associação entre crime organizado e fraude hipotecária é reconhecida há muito tempo e é comumente facilitada por profissionais como corretores de hipotecas, avaliadores imobiliários, contadores, advogados e agentes de custódia. A fraude hipotecária[161] fornece um meio de lavar os rendimentos de outro crime (por exemplo, fornecimento de drogas), mas também pode ser usada para gerar lucro criminoso. Os métodos comuns incluem tirar hipotecas usando os dados de outra pessoa ou os dados de uma pessoa falecida, ou contraindo múltiplas hipotecas em um único endereço.[162]

160 Bodker e outros, "Fraude de cartão não presente".
161 May e Bhardwa, Grupos do crime organizado envolvidos em fraudes; e Reurink, Fraude financeira.
162 May e Bhardwa, grupos do crime organizado envolvidos em fraudes.

Fraude de relacionamento e confiança

Os processos para estabelecer confiança desempenham um papel crítico em qualquer tipo de fraude. No entanto, no caso de fraude de relacionamento e confiança, os fraudadores usam técnicas específicas para promover e explorar o poder de um relacionamento pessoal para desenvolver a confiança necessária para manipular e enganar as vítimas.[163] Nesse tipo de fraude, a vítima não espera receber um produto ou serviço, mas tem a expectativa de formar um relacionamento genuíno com o infrator.[164] A complexidade da fraude está menos na exploração de sistemas técnicos ou tecnológicos e mais na dinâmica do relacionamento entre a vítima e o perpetrador.

Muitos fraudadores estabelecem relacionamentos on-line e usam uma variedade de técnicas de engenharia social ao longo de meses ou até anos para ganhar a confiança da vítima. As vítimas geralmente esperam um relacionamento romântico, mas o relacionamento também pode assumir outras formas, como uma amizade confiável ou até mesmo o desejo de um relacionamento com um membro da família da vítima. Vários estudos identificaram vulnerabilidades dentro do envelhecimento e da demografia idosa relacionadas a fatores como solidão, isolamento social e desejo de formar novos relacionamentos. Outras características interseccionais, como status de cidadania ou status de deficiência, podem levar ao aumento da vulnerabilidade a tais crimes. Os criminosos visam e exploram essa vulnerabilidade por meio de um processo de amizade ou envolvimento romântico, visitando a vítima pessoalmente (por exemplo, se passando por comerciantes), falando ao telefone ou se comunicando on-line.[165]

Independentemente das características das vítimas, o impacto da fraude de relacionamento e de confiança pode ser considerável. Embora as vítimas sofram perdas financeiras, elas também sofrem como resultado da quebra de confiança e da perda de um relacionamento pessoal significativo.[166] Além disso, elas podem sofrer danos psicológicos e emocionais significativos. Algumas podem até se recusar a aceitar que são ou foram vítimas de fraude.

Fraude romântica

Uma forma comum de fraude de relacionamento e confiança é a fraude romântica, na qual os infratores constroem relacionamentos on-line para facilitar o engano com a intenção de enganar as vítimas para que lhes enviem dinheiro.[167] As perdas financeiras para indivíduos podem ser significativas (veja o estudo de caso abaixo). Ela afeta vítimas em muitas regiões diferentes do mundo e capitaliza o crescimento das redes sociais online e, mais especificamente, uma tendência social mais ampla para encontrar relacionamentos românticos online. A abordagem inicial é comumente em mídias sociais ou sites ou aplicativos de namoro por um infrator usando uma identidade falsa, junto com uma narrativa de perfil correspondente.[168] Um único infrator pode alternar entre identidades para atingir e atrair vítimas em potencial; por exemplo, uma imagem de perfil feminina sedutora para atrair homens heterossexuais ou um ou um perfil masculino que apresenta o indivíduo como alguém de elite, glamoroso e confiável (como um membro das forças armadas).[169]

163 Cassandra Cross, "Isca romântica, criptorom e 'abate de porcos': um passo evolutivo na fraude romântica", Current Issues in Criminal Justice, vol. 36, No. 3(2024).
164 Beals, DeLiema e Deevy, "Estrutura para uma taxonomia de fraude".
165 Cassandra Cross, "'Eles são muito solitários': compreender a vitimização por fraude de idosos", International Journal for Crime, Justice and Social Democracy, vol. 5, No. 4 (2016); e Phillips, "De 'comerciantes desonestos' a grupos do crime organizado".
166 Monica T. Whitty e Tom Buchanan, "O golpe do romance online: um crime cibernético sério", Cyberpsychology, Behavior and Social Networking, vol. 15, No. 3(março de 2012).
167 Coluccia e outros, "Golpes de romance online".
168 Cross e Layt, "'Suspeito que as fotos foram roubadas'".

Os sete estágios principais a seguir são comumente vistos na fraude romântica:

- O desejo da vítima de encontrar um parceiro
- A apresentação de um perfil ideal à vítima
- O processo de manipulação emocional (*grooming*)
- O golpe em si (*sting*)
- A continuação do golpe
- Abuso sexual
- Visar novamente a vítima (*retargeting*)[170]

Uma vez que o relacionamento é estabelecido, o infrator pode inicialmente pedir uma pequena quantia de dinheiro, antes de pedir quantias maiores, frequentemente citando um cenário de crise que serve para aplicar pressão e urgência à vítima (por exemplo, uma emergência de saúde ou necessidade urgente de viagem).[171] Se imagens sexuais foram trocadas, dinheiro também pode ser extorquido da vítima. As vítimas são comumente solicitadas a transferir dinheiro para países terceiros ou usando um cartão-presente ou cartão pré-pago e podem posteriormente ser alvos de outros tipos de fraude ou até mesmo alistadas para ajudar a fraudar outras vítimas (por exemplo, usadas como uma mula de dinheiro).[172]

Fraude de investimento em criptoconfiança

Um tipo mais recente de fraude é a convergência da fraude romântica com a fraude de investimento em criptomoedas. Esquemas de investimento em criptoconfiança (ou, como muitos na mídia os chamaram, fraude de "açougue de porcos")[173] envolvem um infrator promovendo um relacionamento pessoal com uma vítima online. Em vez de fabricar um cenário de crise, os infratores estabelecem um relacionamento íntimo com a vítima e então exploram a confiança conquistada para atraí-la para um esquema de investimento fraudulento. Os infratores podem desenvolver um site ou aplicativo fraudulento que pode ser acessado pela vítima e até mesmo fornecer "atendimento ao cliente" para investidores.[174] A integração de investimentos em criptomoeda no engano tem uma série de consequências: amplia o grupo potencial para incluir vítimas de faixas etárias mais jovens, apresenta às vítimas um mercado desconhecido, volátil e de alto risco, oque significa que elas podem ter menos probabilidade de reconhecer que são vítimas de fraude e introduz mais dificuldades para os investigadores criminais rastrearem os fundos até os infratores.[175]

Grande parte da pesquisa sobre fraude romântica tem se concentrado nas vítimas e suas experiências, não nos infratores, que são menos visíveis.[176] Muitos são crimes transnacionais, e são frequentemente (mas nem sempre) perpetrados por grupos criminosos organizados. O estudo de caso sobre fraude romântica abaixo fornece um exemplo em que um grupo criminoso organizado teve como alvo uma vítima através de fronteiras internacionais por um longo período de tempo.

169 Suleman Lazarus e outros, "O que sabemos sobre estudos de fraudes românticas online? Uma revisão sistemática da literatura empírica (2000 a 2021)", Journal of Economic Criminology, vol. 2 (2023).
170 Monica T. Whitty, "The scammer's persuasive techniques model: development of a stage model to explain the online dating romance scam", The British Journal of Criminology, vol. 53, No. 4 (julho de 2013).
171 Cassandra Cross eThomas J. Holt, "O uso de perfis militares em esquemas de fraude romântica", Victims and Offenders, vol. 16, No. 3(2021).
172 Europol, "Esquemas de fraude online".
173 O uso desta frase não é recomendado devido às conotações negativas para as vítimas.
174 Fangzhou Wang e Xiaoli Zhou, "Esquemas persuasivos para exploração financeira em golpes de romance online: uma anatomia sobre sha zhu pan (ÿÿÿ) na China", Vítimas e Infratores, vol. 18, nº 5(2023).
175 Cross, "Provocação romântica, criptorom e 'abate de porcos'".
176 Lazarus eoutros, "O que sabemos sobre estudos de fraude romântica online?".

ESTUDO DE CASO: FRAUDE ROMÂNTICA

Três criminosos atacaram uma mulher que vivia na Austrália durante um período de três anos. O contato inicial foi feito em um site de encontros antes de manter contato por e-mail e telefone. Os infratores adotaram aidentidade de um cidadão alemão que vivia na Austrália, mas trabalhava em Gana. Para obter fundos da vítima, eles apresentaram vários cenários ao longo do tempo, variando de uma necessidade de assistência para desembaraço de mercadorias importadas em um porto aproblemas de saúde. Em vários estágios, o infrator inicial apresentou a vítima a outros infratores, alegando que eram seus associados comerciais; ela se comunicou com cada um deles e foi solicitada a fornecer assistência financeira para remediar uma situação urgente. A vítima foi motivada a ajudar o infrator inicial, com quem ela acreditava estar em um relacionamento, a retornar à Austrália. No total, a vítima foi fraudada em quase 450.000 dólares australianos.

Fonte: Republic v. Mohammed Libabatu, Charles Mensah eNurudeen Alhassan, disponível no portal de gerenciamento de conhecimento Sharing Electronic Resources and Laws on Crime (SHERLOC).

Fraude contra empresas ou organizações

Fraude contra empresas ou organizações normalmente envolve o abuso de sistemas internos ou um relacionamento comercial para fraudar a vítima. A fraude pode ser perpetrada por alguém interno ou externo à organização, como pessoal, clientes ou fornecedores, insiders em conluio com perpetradores externos ou criminosos externos que exploram os serviços ou sistemas da empresa ou organização.[177] Esse tipo de fraude pode ser perpetrado de dentro de empresas, atores ou produtos legítimos, em vez de serem esquemas projetados desde o início para perpetrar fraudes.

Fraude perpetrada por pessoal interno normalmente envolve o abuso de sistemas internos ou um relacionamento comercial para fraudar um empregador, parceiro de negócios ou outra parte interessada. Esse tipo de fraude inclui grandes fraudes corporativas, que são comumente perpetradas por pessoal em cargos de gestão que enganam investidores ou outras partes interessadas importantes.[178] A fraude de demonstrações financeiras encapsula uma variedade de métodos para deturpar a verdadeira natureza ou saúde financeira de uma empresa, fundo ou produto de investimento, afim de enganar e distorcer as percepções de outros, como investidores, reguladores e outros atores do mercado, sobre sua saúde financeira e perspectivas futuras.[179] Tipos semelhantes de fraude contábil também podem encobrir a apropriação indébita, aplicação indevida ou apropriação indébita de fundos. Essa fraude pode ser perpetrada em resposta a pressões para atender às expectativas de desempenho e pode ser realizada por executivos corporativos, traders financeiros ou gestores de fundos de hedge que relatam o desempenho financeiro.

A motivação criminosa para esse tipo de fraude pode advir de uma variedade de circunstâncias, algumas das quais surgem das condições na empresa ou setor. Exemplos incluem diretores da empresa respondendo a dificuldades financeiras ou uma cultura de local de trabalho que promove uma atitude permissiva à fraude ou que impõe altas expectativas e pressão para atingir resultados financeiros. Em muitos casos de fraude contra empresas ou organizações, delinear práticas fraudulentas e legítimas (embora eticamente duvidosas) pode ser um desafio.

177 Duffield e Grabosky, A psicologia da fraude.
178 Paolo Campana, "Quando a racionalidade falha: dando sentido à 'ladeira escorregadia' da fraude corporativa", Criminologia Teórica, vol. 20, n.º 3(agosto de 2016). Veja também Estados Unidos, Departamento de Justiça, Divisão Criminal, "Fraude de títulos e commodities", 11 de agosto de 2023.
179 Reurink, Fraude Financeira.

A fraude contra empresas ou organizações visa frequentemente fraudar uma empresa ou organização específica, mas pode, em alguns casos, ter um impacto mais abrangente no setor, incluindo os consumidores no mercado. Não é incomum que esse tipo de fraude ocorra por períodos prolongados de tempo, e pode levar a perdas financeiras substanciais para empresas e organizações. No entanto, as baixas sentenças impostas a fraudadores de colarinho branco e a maior capacidade entre fraudadores em posições legítimas e confiáveis de perpetrar fraudes sérias sem recorrer a co-infratores podem limitar o papel de grupos criminosos organizados em certos contextos.[180]

Fraudes envolvendo atores externos que exploram relações comerciais ou outras relações comerciais com a empresa ou organização vítima incluem:

- Fraude de empresa de longo ou curto prazo, que pode ser cometida por empresas comerciais já existentes ou por empresas adquiridas ou criadas para fins fraudulentos. Essas empresas estabelecem um histórico de crédito, confiança ou credibilidade, que é usado para enganar um comprador, vendedor ou credor a fornecer bens ou financiamento. Isso é feito sabendo que elas não podem pagar ou não têm intenção de efetuar o pagamento.[181] Alguns fraudadores abusam dos sistemas de confiança que facilitam o comércio internacional. Cartas de crédito são comumente usadas para efetuar pagamentos no comércio internacional, nas quais um banco atua como fiador para o comprador em uma transação. Compradores fraudulentos criam suas próprias instituições bancárias falsas para atuar como seus fiadores e enganar os vendedores.[182] Os bens são enviados pelos vendedores, que acabam não recebendo pagamento.
- Fraude em aquisições ou fornecedores, que engloba uma variedade de métodos para obter contratos comerciais ou pagamentos por bens e serviços. Isso pode envolver fornecedores apresentando declarações falsas[183] ou, em alguns casos, a corrupção de funcionários que esperam pagamento para fornecer contratos e fundos, adquirindo assim bens e serviços por meio de engano. Em um exemplo, uma construtora no Reino dos Países Baixos celebrou um contrato imobiliário com um fundo de pensão, mas, ao longo de um período de 10 anos, os gerentes de contrato inflaram os contratos em milhões de euros.[184]

ESTUDO DE CASO: FRAUDE NAS DEMONSTRAÇÕES FINANCEIRAS

Perpetradores de vários bancos na Alemanha, França eReino Unido da Grã-Bretanha eIrlanda do Norte tentaram manipular a Euro Interbank Offered Rate (Euribor). Essas taxas publicadas são as estimativas fornecidas pelos bancos sobre o custo de empréstimos de outros bancos no mercado interbancário em um dia específico. As taxas são então usadas como referência para suas operações de empréstimo e influenciam as taxas de juros dos empréstimos, hipotecas e contas de poupança fornecidas aos clientes. Os infratores condenados apresentaram estimativas falsas de taxas de juros com a intenção de movendo o benchmark na direção que mais beneficiaria seu empregador ou eles mesmos. Os lucros criminosos foram consideráveis, com um co-infrator ganhando pessoalmente £57,8 milhões com a manipulação das taxas. Além disso, suas ações serviram para minar aintegridade do sistema financeiro.

Fontes: Reino Unido, Serious Fraud Office, "Senior bankers sentenced to 9 years for rigging EURIBOR rate", 1 de abril de 2019; eRuben Herrera eoutros, "The manipulation of Euribor: an analysis with machine learning classification techniques", Technological Forecasting and Social Change, vol. 176, art. No. 121466 (março de 2022).

180 Levi, "Fraude organizada e fraudes organizacionais"; e Levi, "Acertando no ponto da suíte".
181 Michael Levi, "O ofício do fraudador de longa data: habilidades criminosas erespostas comerciais", em Crime no Trabalho: Aumentando o Risco para Infratores, vol. 2, Martin Gill, ed. (Londres, Palgrave Macmillan, 1998).
182 Reurink, Fraude Financeira.
183 Por exemplo, um grupo de quatro fraudadores fraudou sistematicamente uma plataforma de comércio eletrônico manipulando o sistema de fornecedores para induzir a empresa a pagar por produtos que não havia encomendado (Gabinete do Procurador dos Estados Unidos, Distrito Sul de Nova York, "Quatro indivíduos acusados de esquema de faturamento fraudulento de US$ 19 milhões visando o sistema de fornecedores da Amazon", comunicado à imprensa, 19 de agosto de 2020).
184 Philip Gounev, Tihomir Bezlov e Comissão Europeia, Direcção-Geral das Migrações e Assuntos Internos, Examinando a Ligações entre o crime organizado e a corrupção (Bruxelas, Serviço das Publicações, 2010), p. 121.

ESTUDO DE CASO: FRAUDE DE LONG FIRM

O diretor executivo edois executivos seniores de uma empresa de comércio de aço no Reino Unido da Grã-Bretanha eIrlanda do Norte fraudaram 20 bancos de financiamento comercial de vários países em US$ 500 milhões. Durante um período de dois anos, eles garantiram empréstimos de curto prazo fornecendo informações enganosas e contratos falsos para pedidos de remessa de aço inexistentes . Eles usaram uma empresa de transporte interna registrada no exterior para certificar os documentos de embarque falsos. Os empréstimos reforçaram as finanças da empresa, o que lhes permitiu continuar negociando. A empresa evitou fazer os pagamentos dos empréstimos até que finalmente entrou em colapso, deixando grandes quantias de dívidas não pagas com os bancos. Os co-infratores foram condenados e o diretor executivo recebeu uma sentença de prisão de seis anos e meio.

Fonte: Reino Unido, Serious Fraud Office, "Serious Fraud Office garante três condenações em fraude de financiamento comercial de US$ 500 milhões", 2 de fevereiro de 2023.

Grupos criminosos organizados também podem fraudar empresas sem ocupar uma posição legítima ou ostensivamente legítima nos negócios. Em vez disso, esses tipos de fraude são perpetrados por meio de invasão de sistema por criminosos cibernéticos ou pelo abuso dos serviços que a organização vítima fornece aos clientes.

Fraude de comprometimento de e-mail comercial

A fraude de comprometimento de e-mail comercial tem como alvo corporações, pequenas empresas e organizações de uma variedade de setores. É uma das formas mais prevalentes de fraude organizada globalmente.[185] Os fraudadores empregam várias técnicas de engenharia social para persuadir o pessoal afazer transferências não autorizadas de fundos para contas controladas pelos infratores. O primeiro passo é infiltrar os sistemas de comunicação de uma organização para ajudar a persuadir os destinatários de que os e-mails enviados são legítimos: os principais métodos incluem hackear as contas de e-mail dos funcionários, enviar e- mails de phishing para obter os detalhes da conta dos funcionários e explorar provedores de comunicação para personificar nomes de domínio que são familiares à organização-alvo.[186] Várias narrativas são adotadas pelos infratores, incluindo explorar um relacionamento existente entre duas empresas emitindo uma fatura falsa, enviando um e-mail supostamente de um funcionário sênior que apresenta uma solicitação urgente de fundos e se passando por um advogado solicitando uma transferência eletrônica para tratar de um assunto delicado.[187] A comunicação pode ocorrer ao longo de um período de tempo e os infratores podem investir tempo para entender a organização e seus sistemas para fraudá-la em várias ocasiões (veja os estudos de caso abaixo).

Fraude de colisão por dinheiro

A fraude Crash-for-cash envolve grupos criminosos que fraudam sistematicamente as seguradoras de veículos.[188] São utilizados vários métodos, incluindo a apresentação de relatórios falsos de acidentes para reclamar dinheiro do seguro e, em casos mais graves, causar acidentes de viação envolvendo membros inocentes do público para reclamar contra o seu seguro.[189]

185 INTERPOL, "Avaliação global de fraude financeira da INTERPOL".
186 Norah S. Al-Musib e outros, "Ataques de comprometimento de e-mail comercial (BEC)", Materials Today: Proceedings, vol. 81, parte 2(2023); e Geoffrey Simpson, Tyler Moore e Richard Clayton, "Dez anos de ataques a empresas que usam representação visual de nomes de domínio", em 2020 Anti-Phishing Working Group (APWG) Symposium on Electronic Crime Research (eCrime) (Boston, Estados Unidos, 2020).
187 Alessandro E. Agazzi, "Compromisso de e-mail comercial (BEC) e ciberpsicologia" (2020).
188 Mark Button e outros, "Quase todo mundo fazendo negócios? Explicando a fraude de seguro 'dinheiro por acidente' no Reino Unido", The Australian and New Zealand Journal of Criminology, vol. 50, No. 2(junho de 2017).
189 Mark Button e Graham Brooks, "Do policiamento 'superficial' ao 'profundo': investigação de fraude de seguros 'crash-for-cash' na Inglaterra e País de Gales e a necessidade de maior regulamentação", Policing and Society, vol. 26, No. 2(2016).

ESTUDO DE CASO: COMPROMISSO DE E-MAIL COMERCIAL

Uma fraude de comprometimento de e-mail comercial visando uma empresa nos Estados Unidos resultou na perda de US$ 1 milhão para a empresa. Os fraudadores eram um grupo de três co-infratores, dois dos quais estavam localizados na Nigéria. Os infratores se passaram por outra empresa sediada nos Estados Unidos com a qual a vítima tinha um relacionamento comercial existente. Eles enviaram um e-mail inicial solicitando o pagamento por serviços que a empresa havia fornecido e um segundo e-mail solicitando que o dinheiro fosse enviado para uma conta bancária alternativa, supostamente por motivos fiscais. A conta bancária era de propriedade de um indivíduo localizado em outro país. Acredita-se que os lucros tenham sido compartilhados entre os três co-infratores.

Fonte: Nigerian Financial Intelligence Unit, "Nigéria divulga tipologias de lavagem de dinheiro por meio de relatório de fraude", 12 de agosto de 2023.

ESTUDO DE CASO: COMPROMISSO DE E-MAIL COMERCIAL

Os infratores enviaram um e-mail de phishing ao diretor financeiro de uma empresa que parecia fornecer um link para a página de login do serviço de ICT da empresa. Ao clicar no link, a vítima era levada para uma página da web que se assemelhava à página legítima. O diretor financeiro inseriu suas credenciais de login, que foram capturadas pelos infratores e usadas para acessar sua conta de e-mail. Eles conseguiram então se passar pela vítima e enviar e-mails para outros membros da equipe financeira, solicitando uma série de transferências eletrônicas para contas sob seu controle. Além disso, eles observaram e aprenderam sobre as políticas e práticas da empresa e conseguiram imitar um e-mail e uma fatura que normalmente seriam recebidos de um fornecedor legítimo. As faturas falsas foram pagas para contas controladas pelos infratores. A empresa sofreu perdas financeiras de aproximadamente US$ 11 milhões.

Fonte: Estados Unidos da América v. Okeke, disponível no portal de gerenciamento de conhecimento Sharing Electronic Resources and Laws on Crime (SHERLOC).

A fraude é altamente diversa, abrangendo uma gama assustadora de métodos e técnicas para empregar o engano para obter um ganho criminoso. Além disso, os métodos empregados pelos fraudadores evoluem continuamente para explorar oportunidades criminosas que surgem dos avanços nas comunicações, comércio, finanças e tecnologia. Reunir os diversos métodos em uma única estrutura para entender o problema é um desafio considerável, mas essencial para o desenvolvimento de políticas públicas abrangentes e coesas para lidar com a fraude organizada. Essa tipologia fornece uma etapa importante no desenvolvimento de uma estrutura para conceituar esse crime multifacetado.

CAPÍTULO III

Infratores de fraude organizada

Criminosos envolvidos em fraude organizada variam tanto em suas características quanto nos caminhos que eles tomam para cometer crimes. Essa variedade está enraizada nos métodos abrangentes (e capacidades necessárias) que são usados para perpetrar fraudes, na gama de diferentes cenários nos quais a fraude pode surgir, incluindo os diferentes ambientes sociais, econômicos e políticos em diferentes regiões globais, ena variedade de papéis e motivações de fraudadores individuais. É importante entender quem perpetra fraude organizada e os caminhos que são tomados para esse tipo de crime, de modo a direcionar intervenções que sejam eficazes para dissuadir e desviar indivíduos desses crimes.

Os infratores de fraude são uma população oculta e difícil de alcançar, e as pesquisas sobre eles ainda estão em desenvolvimento. A presente seção contém uma compilação de evidências para discutir, primeiro, a importância da co-infração, segundo, as características dos criminosos de fraude organizada e, terceiro, as motivações para perpetrar esses crimes.

Papel e importância da co-infração

Os caminhos para o crime organizado são em parte determinados pelas oportunidades criminosas que emergem de atividades cotidianas e próximas, ambientes e relacionamentos de confiança (por exemplo, redes sociais e profissionais).[190] A capacidade de se encontrar e forjar relacionamentos de confiança com pessoas com ideias semelhantes pode aumentar o escopo para ofensas de maneiras que, de outra forma, estariam fora de alcance.[191] Isso inclui co-infratores que têm recursos ou capacidades que são mais limitados em disponibilidade (por exemplo, facilitadores profissionais ou cibercriminosos com conhecimento técnico)[192] e outros com capacidades mais generalizadas (por exemplo, operadores de call center ou mulas de dinheiro). Identificar os recursos e capacidades necessários para perpetrar diferentes tipos de fraude pode ajudar a identificar grupos que são vulneráveis a serem atraídos para o crime organizado: exemplos incluem o potencial de profissionais jurídicos serem corrompidos e de estudantes serem recrutados como mulas de dinheiro.[193]

190 Edward R. Kleemans e Henk G. van de Bunt, "Crime organizado, ocupações e oportunidade", Global Crime, vol. 9, n.º 3 (2008); Edward R. Kleemans e Henk G. van de Bunt, "A inserção social do crime organizado", Transnational Organized Crime, vol. 5, n.º 1(1999); e Markus Felson, O ecossistema do crime organizado, Instituto Europeu para a Prevenção e Controle do Crime, afiliado às Nações Unidas, Documento, n.º 26 (Helsínquia, 2006).
191 Edward R. Kleemans e Christianne J. de Poot, "Carreiras criminosas no crime organizado e estrutura de oportunidades sociais", European Journal of Criminology, vol. 5, n.º 1(janeiro de 2008).
192 Jason RC Nurse e Maria Bada, "O elemento de grupo do crime cibernético: tipos, dinâmicas e operações criminosas", em The Oxford Handbook of Cyberpsychology, Alison Attrill-Smith e outros, eds. (Oxford, Oxford University Press, 2019).
193 Australian Transaction Reports and Analysis Centre, "Combate à exploração de estudantes internacionais como mulas de dinheiro: guia de crimes" (2024); e May e Bhardwa, Grupos do crime organizado envolvidos em fraudes.

Os locais em que possíveis co-infratores podem se encontrar são significativos, porque sem tais pontos de convergência, os co-infratores têm menos probabilidade de se encontrar e o crime organizado tem menos probabilidade de ocorrer. A disponibilidade e acessibilidade desses pontos de convergência são significativas para determinar quem se envolve no crime organizado e como ele toma forma.[194] Particularmente saliente no contexto da fraude cibernética é o crescimento das comunicações online tanto na web aberta quanto na dark web, que fornecem espaços para os infratores convergirem, se comunicarem e negociarem com outros criminosos (veja o estudo de caso abaixo). Os mercados e fóruns criminosos online que fornecem um lugar para criminosos (incluindo fraudadores) trocarem recursos e conhecimento são um exemplo importante disso.[195] A partir dessas configurações, surgiu o modelo de crime como serviço , uma economia subterrânea na qual empreendedores cibercriminosos podem lucrar com o fornecimento de ferramentas técnicas, recursos e serviços para fraudadores (e outros infratores).[196] Os principais produtos e serviços disponíveis para compra ou contratação incluem dados pessoais roubados, serviços de phishing e spam, serviços de lavagem de dinheiro (incluindo mulas de dinheiro), invasão de contas e fornecimento de Os principais produtos e serviços disponíveis para compra ou aluguel incluem: dados pessoais roubados, serviços de phishing e spam, serviços de lavagem de dinheiro (incluindo "mulas de dinheiro"), invasão de contas e fornecimento de botnets.[197]

A tecnologia criou novas oportunidades para possíveis fraudadores formarem grupos criminosos organizados a partir de um conjunto global de possíveis co-infratores.[198] Além disso, ela fornece uma porta de entrada para a co-infração e o crime organizado que é acessível a possíveis fraudadores. O anonimato dos espaços online atenua os riscos envolvidos na cooperação com atores desconhecidos, e novos membros podem se estabelecer rapidamente e construir status nessas comunidades online.[199] As alianças podem ser efêmeras, existindo apenas para facilitar a conclusão de uma tarefa específica, ou essas novas tecnologias podem promover uma colaboração mais duradoura.

Os relacionamentos formados offline continuam sendo uma característica fundamental dos grupos criminosos organizados que se envolvem em fraudes cibernéticas e frequentemente representam os elementos mais estáveis e duráveis de um grupo.[200] Isso inclui grupos criminosos organizados que expandem seu repertório criminoso para incluir fraudes, ou associados que se unem com o propósito de perpetrar fraudes. Esses grupos podem se tornar hibridizados ao se integrarem à economia subterrânea online para acessar recursos criminosos eco-infratores.[201] A fraude organizada envolve métodos complexos de ofensa, comumente envolvendo uma sequência estendida de ações e eventos que são frequentemente separados uns dos outros no tempo e no espaço,[202] o que pode, por sua vez, atenuar as relações entre os diferentes infratores posicionados ao longo dessa sequência.[203] O resultado é que as tarefas são distribuídas entre uma multidão de atores criminosos vagamente conectados, o que aumenta sua capacidade de se especializar e obter experiência. Além disso, uma distribuição mais uniforme de tarefas e papéis entre os membros de um grupo criminoso organizado serve para espalhar a culpabilidade e o risco de detecção por entidades policiais.

194 Felson, O ecossistema do crime organizado; e Kleemans e de Poot, "Carreiras criminosas no crime organizado".
195 Soudijn e Zegers, "Criminalidade cibernética e cenários de convergência de criminosos virtuais"; e Yip, Webber e Shadbolt, "Confiança entre criminosos cibernéticos?".
196 INTERPOL, "Avaliação global de fraude financeira da INTERPOL", p. 11.
197 Akyazi, van Eeten e Gañán, "Medindo o cibercrime como um serviço (CaaS)"; An e Kim, "Uma abordagem de análise de dados"; Jirovsky e outros, "Cibercrime e crime organizado"; e INTERPOL, "Avaliação global de fraude financeira da INTERPOL", p. 11.
198 Soudijn e Zegers, "Cibercrime e configurações de convergência de infratores virtuais".
199 Odinot e outros, Crime cibernético organizado na Holanda; eYip, Shadbolt eWebber, "Por que fóruns?".
200 Leukfeldt, Lavorgna e Kleemans, "Cibercrime organizado ou cibercrime organizado?"; Lusthaus e outros, "Cibercrime redes no Reino Unido e além"; e Odinot e outros, Crime Cibernético Organizado na Holanda.
201 Roderic Broadhurst e outros, "Crime no ciberespaço: infratores e opapel dos grupos criminosos organizados", Documento de Trabalho (Canberra, Observatório de Cibercrime da Universidade Nacional Australiana, 2013); e Choo, "Grupos do crime organizado no ciberespaço".
202 Klaus von Lampe, "Prevenção situacional do 'crime organizado': prevenção de concepções fantasmas com meios fantasmas?", em Cross- border Crime Inroads on Integrity in Europe, Petrus C. van Duyne e outros, eds. (Nijmegen, Reino dos Países Baixos, Wolf Legal Publishers, 2010).
203 Por exemplo, a fraude de identidade requer o roubo de dados pessoais, o estabelecimento de um fórum online para vender as informações, a aquisição de dados por fraudadores, a seleção e compra de produtos e serviços de uma plataforma, o alistamento de mulas para receber os itens roubados e a revenda dos itens para ganho financeiro (Bodker e outros, "Fraude de cartão não presente").

ESTUDO DE CASO: MERCADO CRIMINAL

O Genesis Market forneceu um ponto de encontro online para criminosos negociarem identidades digitais. O mercado oferecia para venda bots que infectaram os dispositivos das vítimas por meio de malware ou um ataque de aquisição de conta. O preço de cada bot variava dependendo da quantidade e qualidade dos dados coletados (os detalhes da conta para acessar contas bancárias online eram os mais valorizados). Os criminosos que compraram os bots receberam os dados e um software chamado "impressões digitais do navegador", que os permitiu imitar o comportamento das vítimas ao acessar a conta e contornar as medidas de segurança antifraude na plataforma. Criminosos de todo o mundo acessaram o mercado, e foi estimado que 80 milhões de credenciais roubadas de 2 milhões de pessoas foram hospedadas no site.

Fonte: Agência da União Europeia para a Cooperação Policial (Europol), "Remoção de notório mercado de hackers que vende sua identidade a criminosos", 5 de abril de 2023.

ESTUDO DE CASO: CRIME COMO SERVIÇO

Um site criminoso forneceu o software iSpoof, que permitiu que criminosos fizessem ligações telefônicas que pareciam vir de entidades confiáveis, como bancos, empresas de varejo e instituições governamentais. Isso permitiu que criminosos personificassem organizações legítimas de forma mais confiável ao contatar vítimas, facilitando assim oengano. O site foi comercializado para criminosos por meio do aplicativo de mensagens criptografadas Telegram e, em um momento, teve até 59.000 usuários em todo o mundo que pagavam uma taxa mensal para acessar seus serviços. Havia vários administradores, mas um indivíduo baseado no Reino Unido da Grã-Bretanha eIrlanda do Norte desempenhou um papel de liderança na criação do software e na administração do site. Em um período de 16 meses, o site arrecadou mais de € 3,7 milhões, e uma grande proporção desses ganhos foi para o administrador principal.

Fontes: Agência da União Europeia para a Cooperação Policial (Europol), "Ação contra site criminoso que oferecia serviços de 'spoofing' a fraudadores: 142 prisões", 24 de novembro de 2022; e "Fraudador preso por administrar site multimilionário iSpoof", The Guardian, 19 de maio de 2023.

Características dos infratores de fraude organizada

Não existe um fraudador típico. À medida que as oportunidades criminosas se expandem, particularmente no contexto de fraude cibernética, os caminhos e perfis em todo o mundo continuam a se diversificar. Os vários métodos para perpetrar fraudes surgem de diferentes cenários sociais, comerciais, financeiros e tecnológicos, cada um exigindo recursos ou capacidades particulares, o que significa que os caminhos e características dos fraudadores também podem variar dentro da multidão de cenários.

Historicamente, a maioria das fraudes foi cometida em ambientes de colarinho branco. Neste contexto, os perpetradores são tipicamente indivíduos cumpridores da lei que escolhem explorar oportunidades que surgem dentro de um ambiente de trabalho legítimo – por exemplo, peculato, falência ou fraude fiscal.[204] No contexto do crime organizado, os infratores de fraude de colarinho branco normalmente têm pouca experiência anterior

204 Victor R. van der Geest, David Weisburd e Arjan AJ Blokland, "Trajetórias de desenvolvimento de infratores condenados por fraude: um acompanhamento até os 50 anos em uma coorte de condenação holandesa", European Journal of Criminology, vol. 14, No. 5(setembro de 2017). Deve-se notar que a fraude fiscal não está dentro do escopo do presente artigo.

contato com sistemas de justiça criminal antes de sua condenação por fraude organizada e tendem a ser mais velhos do que outras pessoas envolvidas no crime organizado.[205] Isso provavelmente ocorre porque as oportunidades de perpetrar fraude de colarinho branco são mais restritas a indivíduos dentro de ocupações legítimas estabelecidas que são capazes de cruzar as margens tênues que separam práticas lícitas e ilícitas.[206] Os fraudadores de colarinho branco continuam a representar um elemento significativo do problema da fraude organizada (veja a seção sobre fraude contra empresas ou organizações no capítulo II acima); no entanto, as evidências sugerem uma diversidade muito maior nos caminhos tomados para a fraude organizada e nas características dos perpetradores. Também é importante reconhecer o envolvimento de homens e mulheres na fraude organizada. Devido aos estereótipos predominantes relacionados ao crime organizado, as mulheres são vistas predominantemente como vítimas e raramente como perpetradoras. No entanto, a pesquisa indicou que a realidade é mais complexa e que homens e mulheres podem ser perpetradores e vítimas de fraude organizada.[207]

As conceituações de crimes de colarinho branco tornaram-se menos enraizadas em certas categorias de infratores, por exemplo, aqueles das classes altas) e, em vez disso, focaram em certos tipos de delitos que envolvem a violação de confiança.[208] Existem muitos tipos de fraude organizada em que um negócio é estabelecido (ou passa a ser usado) com o único propósito de perpetrar fraude. Um negócio fornece uma fachada legítima para facilitar o engano das vítimas e das autoridades; exemplos proeminentes incluem call centers (ou "boiler rooms") para interagir com o público e negócios comerciais que são estabelecidos para vender produtos ou serviços fraudulentos e/ou para facilitar a lavagem de dinheiro.[209] Isso pode envolver o estabelecimento de uma força de trabalho assalariada com uma divisão de trabalho bem definida e imitando efetivamente as estruturas vistas em empresas legais. Os negócios podem operar à vista de todos, camuflados dentro de setores legítimos e, em alguns casos, podem ocupar áreas cinzentas que estão nas periferias de negócios regulamentados ou práticas comerciais (veja o estudo de caso abaixo).

O crime cibernético resultou na diversificação das características dos infratores de fraude. A tecnologia está mudando as noções tradicionais de "crime de rua", com tecnologias cada vez mais acessíveis criando oportunidades para criminosos se envolverem em atividades criminosas, como phishing e fraude online.[210] Muitas ocorrências de fraude cibernética são perpetradas de fora de ambientes comerciais legítimos ou pseudolegítimos, muitas vezes empregando tecnologia para personificar uma entidade com a qual a vítima tem um relacionamento legítimo.[211] A tecnologia fornece aporta de entrada para o envolvimento nesses crimes, que podem envolver várias formas de crime cibernético (por exemplo, ataques de ransomware), o que significa que as noções tradicionais de um fraudador podem não mais representar infratores com capacidade de se envolver em uma variedade de crimes cibernéticos para ganho criminoso.[212]

---

205 Um estudo realizado no Reino Unido descobriu que a idade média dos fraudadores organizados identificados pelas entidades responsáveis pela aplicação da lei no Reino Unido era de 41 anos (May eBhardwa, Organised Crime Groups Involved in Fraud, p. 113. Ver também Russell G. Smith, "Responding to organized crime through intervention in recruitment pathways", Trends and Issues in Crime and Criminal Justice Series, n.º 473 (Canberra, Instituto Australiano de Criminologia, 2014); e M. Vere van Koppen e outros, "Criminal trajectories in organized crime", The British Journal of Criminology, vol. 50, n.º 1(janeiro de 2010)).
206 Van Koppen e outros, "Trajetórias criminais no crime organizado".
207 UNODC, Crime Organizado e Gênero: Questões Relacionadas à Convenção das Nações Unidas contra o Crime Organizado Transnacional (Viena, 2022).
208 Anna Gekoski, Joanna Ruth Adler e Tim McSweeney, "Perfil do fraudador: descobertas de uma avaliação rápida de evidências", Global Crime, vol. 23, No. 4 (2022); e David O. Friedrichs, Criminosos de confiança: crimes de colarinho branco na sociedade contemporânea, 4ª ed. (Belmont, Califórnia, Wadsworth, 2010).
209 Veja, por exemplo, Miramirkhani, Starov e Nikiforakis, "Dial one for scam"; Shover, Coffey e Sanders, "Dialing for dollars"; e UNODC, Escritório Regional para o Sudeste Asiático e Pacífico, Cassinos, Lavagem de Dinheiro, Bancos Subterrâneos e Crime Organizado Transnacional no Leste e Sudeste Asiático.
210 Leukfeldt, "Cibercrime elaços sociais"; e Robert A. Roks, Eric Rutger Leukfeldt e James A. Densley, "A hibridização da infração de rua na Holanda", The British Journal of Criminology, vol. 61, No. 4 (julho de 2021).
211 Skidmore e Aitkenhead, "Compreendendo as características de infrações graves de fraude".
212 Para ilustrar, há relatos de que grupos criminosos organizados envolvidos em fraudes cibernéticas no Sudeste Asiático diversificaram seu modelo de negócios para incluir o desenvolvimento de malware ou aplicativos maliciosos para dispositivos móveis ou da web e ofornecimento de vários crimes cibernéticos como um serviço (UNODC, Escritório Regional para o Sudeste Asiático e Pacífico, Cassinos, Lavagem de Dinheiro, Bancos Subterrâneos e Crime Organizado Transnacional no Leste e Sudeste Asiático).

Esta diversificação é facilitada em parte pela disponibilidade cada vez mais generalizada de tecnologias recursos de conhecimento por meio de redes criminosas online que podem servir para expandir as capacidades de um grupo criminoso organizado.[213]

Essa expansão de oportunidade criminosa é evidente em muitos países e regiões. Estudos destacaram um fenômeno no qual concentrações de metodologias específicas de fraude emanam de certas regiões globais.[214] Exemplos importantes incluem a concentração de romance, investimento e outras fraudes de marketing de massa de alto impacto perpetradas na África Ocidental que têm fortes associações com a cultura jovem local;[215] fraude de loteria visando os Estados Unidos, mas emanadas da Jamaica;[216] "centros geográficos de crimes cibernéticos " na Europa Oriental que se envolvem em fraudes como fraude de leilão online, em que recursos e aprendizado são compartilhados entre os envolvidos;[217] e compostos de golpes no Sudeste Asiático que industrializaram processos para perpetrar romance e fraude de investimento em criptomoeda.[218]

ESTUDO DE CASO: DELITOS DE COLARINHO BRANCO – FRAUDE DE INVESTIMENTO

No Reino Unido da Grã-Bretanha e Irlanda do Norte, criminosos criaram uma empresa com o propósito de fraudar os detentores de pensão de suas economias. Eles adquiriram status regulamentado para parecerem um provedor legítimo e passaram a comercializar seus serviços financeiros fazendo ligações não solicitadas ao público. Eles tinham conhecimento e entendimento detalhados do setor de pensão do Reino Unido, das leis e regulamentações relevantes, investimentos eoutros instrumentos financeiros. Equipados com esse conhecimento, os criminosos conseguiram explorar as consideráveis lacunas de conhecimento do público. Eles empregaram um engano multifacetado que primeiro envolveu enganar as vítimas sobre suas obrigações fiscais para incentivá-las a liberar dinheiro. O dinheiro então passou pelas mãos de vários co-infratores, que desempenharam o papel de intermediários financeiros e cobraram taxas de comissão excessivamente altas para processar a transferência de fundos. O dinheiro restante foi então supostamente investido em uma empresa estrangeira legítima, mas de alto risco. O dinheiro foi perdido após ofracasso do investimento ou pode nunca ter sido investido, mas sim roubado pelos criminosos.

Fonte: Michael Skidmore, Protegendo as pensões das pessoas: entendendo e prevenindo golpes (Londres, The Police Foundation, 2020), p. 15.

Motivações dos fraudadores

A tecnologia "democratizou" a prática de fraudes ao abrir oportunidades criminosas a pessoas de qualquer estrato social, incluindo aquelas de origens pobres e desfavorecidas, que não necessitam de funções ocupacionais específicas nem de competências e conhecimentos relacionados para poderem perpetrar fraudes organizadas.[219] Esta criminalidade pode estar enraizada em subculturas locais, nas quais as atitudes criminogénicas, o conhecimento especializado

213 Para ilustrar, um grupo criminoso organizado no Reino Unido esteve envolvido em várias categorias de fraude cibernética (fraude de identidade e fraude de comprometimento de e-mail comercial). Ele também se especializou em facilitar a lavagem de dinheiro e esteve envolvido em um ataque de ransomware contra empresas locais. Os principais infratores não eram tecnicamente proficientes, mas conseguiram acessar recursos técnicos de outros criminosos, inclusive online, como em fóruns de carding (Skidmore e Aitkenhead, "Understanding the characteristics of serious fraud offending", p. 30).
214 INTERPOL, "Avaliação global de fraude financeira da INTERPOL", p. 11.
215 Suleman Ibrahim, "Taxonomia social e contextual do crime cibernético: teoria socioeconômica dos criminosos cibernéticos nigerianos", International Journal of Law, Crime and Justice, vol. 47 (2016); e Monica T. Whitty, "419: é só um jogo – caminhos para a fraude cibernética", International Journal of Cyber Criminology, vol. 12, No. 1(janeiro/junho de 2018).
216 Mortley, "Um crime de oportunidade".
217 Jonathan Lusthaus e Federico Varese, "Offline e local: a face oculta do cibercrime", Policing: A Journal of Policy and Practice, vol. 15, No. 1(março de 2017).
2018 UNODC, Escritório Regional para o Sudeste Asiático e Pacífico, Cassinos, Fraude Cibernética e Tráfico de Pessoas para Criminalidade Forçada no Sudeste Asiático.
219 Van der Geest, Weisburd e Blokland, "Trajetórias de desenvolvimento de infratores condenados por fraude"; e Wall, "Crime desorganizado".

e metodologias são propagadas.[220] A fraude cibernética em alguns contextos é dotada de legitimidade social, com racionalizações ou atitudes particulares compartilhadas por membros de uma comunidade ou grupo e fraudadores bem-sucedidos recebem um alto status social.[221]

A obtenção de lucro criminoso (benefício financeiro ou outro benefício material) é a principal motivação na fraude, como em praticamente qualquer crime aquisitivo, que pode ser em resposta a uma situação financeira adversa, como a ausência de oportunidades legítimas e privação.[222] Na Nigéria, muitos fraudadores cibernéticos são estudantes universitários ou graduados, geralmente na faixa dos 20 e poucos anos, com conhecimento avançado e habilidades em tecnologia.[223] A lacuna entre os níveis crescentes de treinamento e educação e as perspectivas na economia legítima pode significar que os indivíduos recorrem a saídas ilegítimas, como a fraude cibernética, para ganhar a vida.[224] Um padrão semelhante foi observado entre os recrutas de compostos fraudulentos no Sudeste Asiático: grupos criminosos organizados recrutam milhares de trabalhadores, muitos dos quais estão na faixa dos 20 anos e são graduados universitários com habilidades em TIC, mídia social, criptomoeda e idiomas.[225] Muitos se candidatam a essas funções devido à falta de oportunidades de trabalho legítimas, embora, o mais importante, muitos sejam enganados a aceitar o que é apresentado como uma posição legítima antes de serem traficados e coagidos a perpetrar fraude.[226]

Criminosos que se envolvem em grupos criminosos organizados podem fazer a escolha consciente e intencional de se envolver em fraudes ou podem ser recrutados para um grupo criminoso organizado sem ter tido qualquer intenção prévia de se envolver em crime organizado.[227] Para aqueles que fazem uma escolha intencional, pode ser por vários motivos, como ser movido pela ganância ao ver uma oportunidade de ganhar dinheiro rápido, a influência de colegas ou associados em um grupo criminoso organizado existente ou outro grupo (offline ou online), ou necessidade ou dificuldade financeira.[228]

Entre os indivíduos sem intenção prévia de se envolver, muitos são recrutados por grupos criminosos organizados para papéis periféricos, mas importantes, facilitadores. Isso pode incluir indivíduos recrutados porque têm conhecimento técnico especializado adquirido ao trabalhar em uma determinada profissão que pode habilitar alguma parte do processo criminal (por exemplo, advogados ou contadores), jovens profissionais recrutados para a "força de trabalho" e membros do público alistados em papéis como o de uma mula de dinheiro. O conhecimento e a cumplicidade entre esses indivíduos podem ser variáveis e mudar ao longo do tempo: alguns não têm consciência do propósito fraudulento subjacente da atividade, outros se contentam em aceitar o dinheiro sem fazer muitas perguntas e outros vêm a participar conscientemente do crime.[229] Alguns co-infratores são explorados pelo grupo criminoso organizado; eles são frequentemente os mais expostos à aplicação da lei e, assim, servir para distanciar os principais crimi-

220 Veja, por exemplo, Alice Hutchings, "Crime do teclado: crime cibernético organizado, co-infração, iniciação e transmissão de conhecimento", Crime, Law and Social Change, vol. 62, n.º 1(agosto de 2014); Lusthaus e Varese, "Offline e local"; Jegede Ajibade Ebenezer, "Fraude cibernética, comércio global e carga criminal juvenil: experiência nigeriana", Afro Asian Journal of Social Sciences, vol. 5, n.º 4(2014); e Ojedokun ellori, "Ferramentas, técnicas e redes subterrâneas".
221 Shover, Coffey e Sanders, "Discando por dólares"; Whitty, "419: é só um jogo"; e Oludayo Tade e Ibrahim Aliyu, "Organização social de fraude na Internet entre estudantes universitários na Nigéria", International Journal of Cyber Criminology, vol. 5, No. 2(julho/Dezembro de 2011).
222 Mortley, "Um crime de oportunidade".
223 Aransiola e Asindemade, "Compreendendo os perpetradores de crimes cibernéticos"; e Tade e Aliyu, "Organização social da fraude na Internet".
224 Akanle, Adesina e Akarah, "Rumo à dignidade humana e a internet"; e Suleman Lazarus e Geoffrey U. Okolorie, "A bifurcação dos cibercriminosos nigerianos: narrativas dos agentes da Comissão de Crimes Econômicos e Financeiros (EFCC)", Telematics and Informatics, vol. 40 (2019).
225 Organização Internacional para as Migrações (OIM), Escritório Regional para a Ásia e o Pacífico, "Relatório de situação regional da OIM sobre o tráfico de pessoas para a criminalidade forçada em um centro de golpes online no Sudeste Asiático" (2024); e UNODC, Escritório Regional para o Sudeste Asiático e o Pacífico, Cassinos, Fraude Cibernética e Tráfico de Pessoas para a Criminalidade Forçada no Sudeste Asiático.
226 ACNUDH, "Operações fraudulentas online e tráfico para criminalidade forçada no Sudeste Asiático".
227 Smith, "Respondendo ao crime organizado através da intervenção nas vias de recrutamento".
228 Veja, por exemplo, W. Steve Albrecht e Chad O. Albrecht, Fraud Examination and Prevention (Mason, Ohio, Estados Unidos, Thompson South-Western, 2004); Hutchings, "Crime from the keyboard"; Yetunde O. Ogunleye, Usman A. Ojedokun e Adeyinka A. Aderinto, "Pathways and motivations for cyber fraud involvement among female undergraduates of selected university in South-West Nigeria", International Journal of Cyber Criminology, vol. 13, No. 2(julho/dezembro de 2019); e May e Bhardwa, Grupos de Crime organizado envolvidos em fraude.
229 Shover, Coffey e Sanders, "Discando por dólares"; Leukfeldt e Jansen, "Redes criminosas cibernéticas e mulas de dinheiro"; Levi, "Fraude organizada e fraudes organizacionais"; Skidmore e Aitkenhead, "Compreendendo as características de crimes graves de fraude"; e May e Bhardwa, Grupos de crime organizado envolvidos em fraudes.

nosos da fraude e, em alguns casos, receber pouco ou nenhum ganho financeiro com seu envolvimento.[230] No Sudeste Asiático, um exemplo pungente recente é o dos jovens que aceitaram emprego em complexos fraudulentos e foram então sujeitos ao tráfico de pessoas e à exploração. [231]

Um ponto final a considerar é como os fraudadores chegam a tomar a decisão de mirar e roubar dinheiro das vítimas, observando que algumas podem não estar envolvidas em crimes.[232] O processo de racionalização para justificar ou neutralizar o impacto do crime é importante, porque pode distorcer narrativas pessoais ou baseadas em grupo sobre a gravidade das ações ou até mesmo servir para legitimá-las. Exemplos importantes incluem:

- A percepção de uma relação adversarial com as vítimas. Um fraudador bem-sucedido demonstra habilidade, maestria e poder para controlar e manipular as vítimas, que podem ser consideradas indignas (por exemplo, estúpidas ou gananciosas) e culpadas por cair na fraude.[233]
- A percepção do crime como sem vítimas ou causando dano mínimo. Tal percepção pode estar presente, por exemplo, quando fraudadores empregam um método que envolve o roubo de pequenas quantias de dinheiro de um grande número de pessoas ou quando as perdas são sofridas por corporações e empresas em vez de indivíduos.[234]
- A natureza anônima e remota da fraude, com trocas impessoais que não envolvem contato face a face com a vítima. Os infratores não observam diretamente o dano que está sendo causado, o que pode permitir que neutralizem seus crimes mais prontamente.[235] Além disso, no contexto do crime cibernético, a capacidade de permanecer fisicamente invisível, de separar a ação online da identidade offline e de perceber o mundo online como não conectado à "realidade" desinibe aqueles que, de outra forma, não cometeriam crimes.[236]
- As influências sociais eculturais que podem servir para racionalizar afraude. Elas podem incluir narrativas sociopolíticas e percepções de vítimas no exterior: alguns fraudadores legitimam suas ações com base em desigualdades ou injustiças sociais atuais ou históricas percebidas (por exemplo, "ocidentais gananciosos").[237] Em algumas culturas, a perpetração de fraude pode até ser reforçada por meio de crenças espirituais locais.[238]

Os padrões de infrações por fraude passaram por mudanças substanciais nos últimos 10 a 20 anos e continuam a evoluir em ritmo acelerado. A pesquisa e a base de conhecimento na área ainda estão se desenvolvendo e acompanhando essas mudanças. As características dos infratores e seus caminhos para a fraude organizada são altamente variáveis, mas há padrões de comportamento que começaram a surgir nas diferentes regiões do mundo e nos diferentes cenários comerciais, financeiros e tecnológicos que fomentam a oportunidade criminosa. Entender quem são esses criminosos esuas rotas para a fraude organizada é um passo importante na concepção de políticas sociais e de justiça criminal eficazes para lidar com esses comportamentos ofensivos.

230 Skidmore e Aitkenhead, "Compreendendo as características de infrações graves de fraude".
231 UNODC, Escritório Regional para o Sudeste Asiático e Pacífico, Cassinos, Fraude Cibernética e Tráfico de Pessoas para Criminalidade Forçada no Sudeste Asiático.
232 Por exemplo, o "triângulo da fraude" é uma teoria proeminente para explicar o crime de colarinho branco. Ele identifica três condições para um infrator perpetrar fraude: (a) um incentivo ou pressão que fornece um motivo para cometer fraude; (b) uma oportunidade para a fraude ser perpetrada; e (c) uma atitude que permite ao indivíduo cometer fraude ou ter a capacidade de racionalizar a fraude (veja Albrecht e Albrecht, Fraud Examination and Prevention).
233 Duffield e Grabosky, A psicologia da fraude; e Shover, Coffey e Sanders, "Discando por dólares".
234 Heath Copes e Lynne Vieraitis, "Roubo de identidade: avaliando as motivações eestratégias dos infratores", em In Their Own Words: Criminals on Crime, 6ª ed., Michael L. Birzer e Paul Cromwell, eds. (Oxford, Oxford University Press, 2014), pp. Duffield eGrabosky, A psicologia da fraude; e May e Bhardwa, Grupos do crime organizado envolvidos em fraudes.
235 Duffield e Grabosky, The Psychology of Fraud; e Alice Hutchings, "Trajetórias do cibercrime: uma teoria integrada de iniciação, manutenção e desistência", em Crime Online: Correlates, Causes, and Context, Thomas J. Holt, ed. (Durham, Carolina do Norte, Estados Unidos, Carolina Academic Press, 2010).
236 John Suler, "O efeito de desinibição online", Cyberpsychology and Behavior, vol. 7, No. 3(2004).
237 Mortley, "Um crime de oportunidade"; eWhitty, "419: é apenas um jogo".
238 Na Nigéria, alguns acreditam que a aquisição de riqueza, seja por meios legítimos ou ilegítimos, está enraizada no reino espiritual (Lazarus e Okolorie, "The bifurcation of the Nigerian cybercriminals").

CAPÍTULO IV
Facilitadores transversais da fraude organizada

Conforme destacado no capítulo II acima, há uma diversidade considerável nos métodos empregados por diferentes criminosos para fraudar vítimas; no entanto, há algumas semelhanças nos comportamentos e técnicas usadas em diferentes tipos de fraude. Isso ocorre pois, independentemente da narrativa fraudulenta específica apresentada às vítimas, muitos tipos de fraude precisam realizar as mesmas etapas abrangentes: estabelecer comunicação com as vítimas, empregar métodos de comunicação que facilitem o engano e acessar fundos roubados sem deixar um rastro de evidências.[239] Desenvolver uma compreensão dos elementos comuns da economia legítima e ilegítima que são explorados por fraudadores permite a introdução de novas estratégias e intervenções para prevenir fraudes organizadas. A presente seção contém uma descrição das seguintes técnicas, recursos e tecnologias subjacentes principais que foram identificados na literatura de política e pesquisa: marketing de massa, roubo de identidade, lavagem de dinheiro e as funções facilitadoras da tecnologia (incluindo tecnologias emergentes, como inteligência artificial).

Marketing em massa

O sucesso de muitos tipos de fraudes de consumidor, emprego e investimento depende de comunicações eficazes, usando várias técnicas para persuadir investidores em potencial. Tais técnicas incluem campanhas de marketing direcionadas ou de massa, técnicas de vendas agressivas e a produção de recursos para estabelecer e manter credibilidade e confiança, incluindo *branding*, sites e outros materiais de marketing. Os infratores podem utilizar canais de comunicação específicos, ou uma combinação deles, que são implantados em diferentes estágios da infração. Por exemplo, o contato inicial com uma vítima pode ser por meio de um site de *phishing*, seguido por uma chamada de vendas subsequente por telefone e, então, envolvimento contínuo por meio de um site fraudulento (veja o estudo de caso abaixo).

Telemarketing

O uso de *call centers* ou "*boiler rooms*" para empregar marketing e vendas agressivos, muitas vezes na forma de chamadas não solicitadas que são direcionadas usando "listas de *leads*" criadas ou compradas de outros atores legítimos ou ilegítimos que compilam e vendem essas informações pessoais sobre os consumidores.[240]

239 As três etapas principais do processo de ciberfraude foram descritas em um relatório: a) a via de comunicação "de entrada"; (b) a "interação" com a vítima; e (c) o "saque" (Reino Unido, Câmara dos Lordes, Lei de Fraude de 2006 e Comitê de Fraude Digital, Combate à Fraude: Quebrando a Cadeia, Relatório da Sessão 2022–23, Documento da Câmara dos Lordes, nº 87 (Londres, 2022))
240 Shover, Coffey e Sanders, "Discagem para dólares"; Levi, "Fraude organizada e fraudes organizadoras"; e Skidmore e Aitkenhead, "Entendendo as características de crimes graves de fraude".

Em alguns casos, essas listas incluem indivíduos conhecidos por terem sido fraudados anteriormente e, portanto, potencialmente vulneráveis a abordagens semelhantes; esse problema é particularmente grave para vítimas mais velhas em contextos vulneráveis.[241] Os *call centers* podem ser gerenciados diretamente pelos infratores que administram o esquema fraudulento ou tercerizados a especialistas que são capazes de fornecer esses serviços de *"boiler room*". Esses centros podem estar localizados em países além dos das vítimas, por vezes em jurisdições conhecidas por terem controles menos robustos sobre essas atividades.[242]

Comunicações on-line

Houve um aumento substancial em fraudes para as quais o contato inicial com as vítimas é estabelecido por meio de comunicações on-line, como mídias sociais e sites e aplicativos fraudulentos.[243] A capacidade de se envolver em marketing em larga escala e direcionado é bastante aprimorada pela acessibilidade de tecnologias digitais e grandes conjuntos de dados sobre os consumidores. Por exemplo, sites e anúncios on-line podem ser usados para coletar dados sobre indivíduos com interesse no produto ou serviço que está sendo oferecido, fornecendo um meio de direcionar a comunicação subsequente.[244]

Outras comunicações

Outros métodos incluem fraudes comercializadas por meio do serviço postal ou pessoalmente.[245] Algumas categorias, como fraudes de investimento, comumente envolvem grandes somas de dinheiro que são altamente significativas para as vítimas, e o contato face-a-face continua sendo importante em alguns casos para atingir níveis suficientes de confiança para garantir um investimento. Alguns fraudadores visam vítimas com as quais têm conexões sociais ou comerciais existentes para explorar uma relação de confiança pré-existente.[246]

Roubo de identidade

Em uma sociedade da informação onde as transações digitais cada vez mais tomam o lugar das interações face a face, os instrumentos e mecanismos para verificar a identificação são críticos.[247] O roubo de identidade e a fraude de identidade representam duas atividades discretas: o roubo de identidade se relaciona aos processos de acesso e roubo de dados, e a fraude de identidade envolve a aplicação dos dados roubados para enganar as vítimas e acessar fraudulentamente fundos ou outros benefícios materiais. As ICT/TIC e *big data* facilitam a transferência de informações em uma escala sem precedentes, e essa capacidade é explorada por criminosos. A tecnologia atua como um multiplicador de força para roubo de identidade, aumentando a capacidade de acessar rapidamente grandes volumes de informações pessoais em nível global.[248] Os métodos para perpetrar roubo de identidade incluem:

241 Age UK," Only the Tip of the Iceberg: Fraud against Older People – Evidence Review" (Londres, 2015); e Mark Button e outros, "Fear and phoning: telephones, fraud, and older adults in the UK", International Review of Victimology (2024).
242 Shover, Coffey e Sanders, "Dialing for Dollars".
243 Ver, por exemplo, Estados Unidos, Federal Bureau of Investigation, «The FBI warns of a spike in cryptocurrency investment schemes", 14 de março de 2023; e Reino Unido, Financial Conduct Authority, "FCA warns of increased risk of online investment fraud, as investors lose £87k a day to binary options scams", 12 de abril de 2024.
244 Ver, por exemplo, Liu e outros, "Compreendendo, medindo e detectando".
245 Ver, por exemplo, DeLiema e Langton, "Older victims of mass marketing scams"; e Phillips, "From 'rogue traders' to organized crime groups".
246 Frank S. Perri e Richard G. Brody, "A ótica da fraude: afiliações que aumentam a credibilidade do infrator", Journal of Financial Crime, vol. 19, nº 3 (2012).
247 Bert-Jaap Koops e outros, "Uma tipologia de crime relacionado à identidade", Information Communication and Society, vol. 12, No. 1 (2009).

- Uso de técnicas de engenharia social. Isso inclui ataques de phishing, smishing e spear phishing[249] que usam comunicações direcionadas para pressionar um destinatário a tomar uma decisão rápida de responder (por exemplo, uma suposta ameaça à segurança de uma conta).[250] As campanhas de phishing são uma tática usada para enganar indivíduos a divulgar informações pessoais, bem como um veículo para iniciar ataques baseados em malware em dispositivos eletrônicos.
- Coleta de dados de código aberto. Criminosos podem explorar os dados que são postados por usuários em plataformas de mídia social. Grandes volumes de dados podem ser coletados usando software automatizado, ou um fraudador pode criar um perfil de uma vítima pretendida para facilitar a farsa.
- Intrusão em (ou infecção de) um computador ou dispositivo. Fraudadores infectam o computador de uma vítima com malware que permite que eles monitorem atividades e coletem detalhes pessoais e informações de conta. Em um dos métodos, o navegador da Internet é manipulado para que, quando uma pessoa tenta acessar um site legítimo, ela seja redirecionada para um site falsificado que permite que os infratores coletem informações de conta.[251] Botnets e outros softwares de vigilância aumentam a capacidade dos invasores de infectar um alto volume de computadores com malware que pode ser controlado remotamente pelo invasor e usado para pesquisar informações pessoais, incluindo informações para acessar contas.
- *Skimming* digital. O uso de malware para infiltrar sites legítimos, como os de varejistas on-line, é conhecido como skimming digital. As informações de pagamento (por exemplo, credenciais de cartão de crédito) podem ser obtidas diretamente do formulário de pagamento legítimo, ou um comprador pode ser redirecionado para uma página de checkout falsa para inserir seus dados.[252]
- Violação de dados por meio de *hacking* ou outros meios de intrusão nos sistemas de TIC de organizações que armazenam grandes quantidades de dados pessoais.[253] A análise de violações de dados de 2005 a 2018 revelou 9.000 violações de dados que levaram à perda de 11,5 bilhões de registros individuais, com o hacking desempenhando um papel cada vez mais central.[254] O roubo em larga escala de dados pessoais pode permitir vários tipos de fraude, embora a proporção dos dados que são usados dessa forma não seja conhecida.

O roubo de identidade é um evento precursor vital em muitos tipos de fraude eum facilitador essencial de outros. Por exemplo, ele facilita a fraude de identidade, o marketing em massa e a abertura de contas bancárias para facilitar a lavagem de dinheiro. O roubo de identidade e a atividade fraudulenta resultante não são necessariamente perpetrados como parte de um único processo criminal, com mercados criminosos online, como fóruns de carding, fornecendo aos criminosos cibernéticos canais convenientes e eficientes para fornecer dados roubados a possíveis fraudadores.[255]

248 David S. Wall, “Policing identity crimes”, Policing and Society: An International Journal of Research and Policy,, vol. 23, nº 4 (2013).
Phishing é uma forma de comunicação que parece vir de uma fonte respeitável ou confiável que se destina a solicitar informações pessoais ou pagamento, ou pode conter anexos que instalam malware se abertos; smishing é uma forma de phishing recebida por mensagens de texto ou aplicativos de mensagens; spear phishing é um ataque mais direcionado no qual os perpetradores usam informações sobre o destinatário para tornar a mensagem mais realista e persuasiva. Ver, por exemplo, Europol, "Esquemas de fraude online"; e Europol, Centro Europeu de Cibercrime, "Spear phishing: uma perspectiva de aplicação da lei e intersetorial (Haia, 2019).
250 Zainab Alkhalil e outros, “Phishing attacks: a recent comprehensive study and a new anatomy”, Frontiers in Computer Science,e, vol. 3, art. Nº 563060 (março de 2021).
251 Wall, "Policiamento de crimes de identidade".
252 Europol, «Esquemas de fraude em linha».
253 Spencer Wheatley, Thomas Maillart e Didier Sornette, "O risco extremo de violações de dados pessoais e a erosão da privacidade",
The European Physical Journal B, vol. 89, art. Nº 7 (janeiro de 2016).
254 Hicham Hammouchi e outros, "Aprofundando-se nas violações de dados: uma análise exploratória de dados de violações de hackers ao longo do tempo",
Procedia Ciência da Computação, vol. 151 (2019).
255 Europol, Avaliação da Ameaça da Criminalidade Organizada na Internet (IOCTA) 2023 (Luxemburgo, Serviço das Publicações da União Europeia).

ESTUDO DE CASO: VIOLAÇÃO DE DADOS

Um grupo criminoso organizado invadiu as redes de computadores de várias corporações, resultando em uma violação de dados em larga escala na qual 160 milhões de números de cartão de crédito foram roubados. O grupo usou *malware* para atacar e se infiltrar nos sistemas corporativos. Eles ocultaram essa atividade implantando *malware* que não podia ser detectado pelo software antivírus e alugando servidores que eram inacessíveis às autoridades policiais ("*hosts* à prova de balas"). Os números de cartão de crédito roubados e as informações pessoais associadas foram vendidos em lotes. Os compradores codificaram os dados roubados nas tarjas magnéticas de cartões bancários de plástico e os usaram para sacar dinheiro de contas ou fazer compras não autorizadas.

Fonte: Estados Unidos v. Drinkman, Kalinin, Kotov, Rytikov, Smilianets, disponível no portal de gerenciamento de conhecimento Sharing Electronic Resources and Laws on Crime (SHERLOC).

Lavagem de dinheiro

Para qualquer perpetrador de fraude, uma consideração fundamental é como disfarçar as origens ilegais dos fundos roubados. Lavagem de dinheiro é a aquisição, posse, uso, ocultação, conversão ou transferência de qualquer propriedade, sabendo que tal propriedade é produto do crime.[256]

Grupos criminosos organizados exigem processos para acessar fundos roubados sem acionar controles nos setores financeiro ou outros ou ainda deixar um rastro financeiro que possa ser rastreado pela polícia.[257] Além das transferências eletrônicas por meio de bancos tradicionais e empresas de tecnologia financeira, os lucros da fraude, como qualquer outro crime que gere ganho ilícito, podem ser lavados por meio de mulas de dinheiro e empresas de fachada,[258] pela compra de imóveis ou bens de alto valor, como carros, ou pelo uso de casas de câmbio, cassinos, empresas de fachada ou serviços bancários clandestinos, como transações hawala.[259]

A globalização do comércio e das finanças, facilitada pelo crescimento, diversificação e avanços tecnológicos no setor financeiro, introduziu novos e evoluídos canais para exploração por criminosos que buscam lavar os lucros do crime.[260] Os criminosos se adaptam continuamente e exploram novos e evolutivos canais que facilitam a rápida movimentação de fundos e capital através das fronteiras nacionais.[261] Exemplos incluem criminosos que usam a lavagem de dinheiro baseada no comércio como um método, ou seja, "o processo de disfarçar os lucros do crime e mover valor por meio do uso de transações comerciais em uma tentativa de legitimar suas origens ilícitas". A lavagem de dinheiro baseada no comércio é normalmente efetuada por meio do faturamento incorreto de transações comerciais internacionais. Ao relatar de forma fraudulenta o preço, a quantidade ou a qualidade dos bens, os criminosos podem mover rapidamente quantias substanciais de dinheiro ou valor de uma jurisdição para outra.[262]

256 Convenção contra o Crime Organizado, art. 6. Ver também Benjámin Villányi, "Money laundering: history, regulations, and techniques", Criminology and Criminal Justice, 26 de abril de 2021.
257 INTERPOL, "INTERPOL global financial fraud assessment", p. 18.
258 Financial Action Task Force, INTERPOL e Egmont Group of Financial Intelligence Units, Illicit Financial Flows from Cyber-Enabled Fraud (Paris, 2023).
259 Unidade de Inteligência Financeira da Nigéria, "Nigeria releases money-laundering typologies through fraud report"; e UNODC, Escritório Regional para o Sudeste Asiático e o Pacífico, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia.
260 Emilia A. Isolauri e Irfan Ameer, "Money laundering as a transnational business phenomenon: a systematic review and future agenda", Critical Perspectives on International Business, vol. 19, n.º 3 (abril de 2023); Europol, The Other Side of the Coin: An Analysis of Financial and Economic Crime, European Financial and Economic Crime Threat Assessment 2023 (Luxemburgo, Publications Office of the European Union, 2023); e Pierre Bardin e outros, "Money laundering poses a risk to financial sector stability", International Monetary Fund Blog, 4 de setembro de 2023.
261 Isolauri e Ameer, "Money laundering as a transnational business phenomenon".
262 Financial Action Task Force, "Trade based money laundering" (Paris, 2006).

Acordos e transações comerciais complexos e transfronteiriços criam desafios consideráveis para as entidades responsáveis pela aplicação da lei e para a indústria ao rastrear as origens dos produtos e distinguir atividades financeiras e comerciais ilegítimas das legítimas.[263] Pode ser necessária uma cooperação internacional eficaz para rastrear fundos roubados e lavados dessa forma.

As criptomoedas são cada vez mais usadas para lavar os lucros do crime organizado, sendo essa uma das formas mais comuns de lavagem de dinheiro.[264] A compra de criptomoedas e seu uso para transferir fundos ajudam a fornecer anonimato, facilitando a transferência internacional de valores de forma que ofusca o rastreamento financeiro e oculta as origens criminosas do dinheiro. Isso geralmente envolve a transferência de criptomoedas e outros ativos digitais por diferentes redes de blockchain (ou "moedas") para obscurecer o rastro, antes de sacar o dinheiro e convertê-lo novamente em moeda fiduciária.[265] Isso ajuda a contornar os rigorosos controles antilavagem de dinheiro implementados por instituições financeiras tradicionais. Existem desafios para impor uma regulamentação robusta, particularmente devido ao crescimento das finanças descentralizadas.[266] Esses serviços facilitam a transferência de criptomoedas para outros ativos virtuais sem a necessidade de um intermediário centralizado que possa identificar a atividade suspeita e alertar as autoridades.[267] Os sites de câmbio de criptomoedas são numerosos e podem ser usados para transferir ativos virtuais entre plataformas ou converter criptomoedas em moeda fiduciária. Alguns desses sites não são licenciados ou estão localizados em países com pouca regulamentação em vigor e/ou que optam por implementar poucos controles para evitar a lavagem de dinheiro (veja o estudo de caso abaixo).[268]

As capacidades e os recursos de lavagem de dinheiro são altamente valorizados pelos criminosos envolvidos em fraudes organizadas, e os processos de lavagem de dinheiro podem representar um elemento-chave na formação de grupos criminosos organizados.[269] Facilitadores profissionais desempenham um papel fundamental em alguns esquemas de fraude, particularmente aqueles que exploram estruturas comerciais legais para lavar os lucros criminosos.[270] Estudos destacaram o papel proeminente de advogados, contadores, consultores financeiros, gerentes de banco e corretores de hipoteca na facilitação da lavagem de dinheiro oriundo de fraudes.[271] Isso inclui o uso de redes profissionais de lavagem de dinheiro por fraudadores,[272] além de profissionais que são corrompidos e aqueles que, involuntariamente, facilitam a lavagem de dinheiro ao negligenciar procedimentos de *due diligence*. É importante conduzir investigações autônomas sobre lavagem de dinheiro envolvendo profissionais que oferecem serviços a vários grupos criminosos organizados por uma taxa.

Alguns grupos criminosos organizados alistam criminosos com capacidades especializadas em lavagem de dinheiro, incluindo aqueles que anunciam seus serviços em mercados criminosos online. Isso pode ser especialmente valioso para facilitar fraudes transnacionais, onde os co-infratores estão em diferentes paí-

263 Ver, por exemplo, James Treadwell, "From the car boot to booting it up? eBay, online counterfeit crime and the transformation of the criminal marketplace", Criminology and Criminal Justice, vol. 12, n.º 2 (abril de 2012).
264 Este é o modus operandi mais prevalente entre fraudadores que operam na Europa (INTERPOL, "INTERPOL global financial fraud assessment", p. 17; e Europol, Cryptocurrencies: Tracing the Evolution of Criminal Finances, Europol Spotlight Report Series (Luxemburgo, Publications Office of the European Union, 2021)).
265 Vladlena Benson, Umut Turksen e Bogdan Adamyk, "Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities", Journal of Financial Regulation and Compliance, vol. 32, n.º 1 (janeiro de 2024).
266 Finanças descentralizadas são um sistema de produtos e serviços financeiros que utilizam contratos inteligentes em blockchains para gerenciar transações financeiras entre duas partes. Essa tecnologia permite trocas automatizadas, nas quais indivíduos podem negociar diretamente entre si, eliminando a necessidade de uma instituição centralizada ou de um terceiro intermediário (por exemplo, um banco ou provedor de criptomoeda). Ver, por exemplo, Organisation for Economic Co-operation and Development, Why Decentralised Finance (DeFi) Matters and the Policy Implications (2022).
267 Benson, Turksen e Adamyk, "Dark side of decentralised finance".
268 Ver, por exemplo, United States Attorney's Office, Southern District of New York, "Tornado cash founders charged with money laundering and sanctions violations", comunicado de imprensa, 23 de agosto de 2023.
269 Skidmore e Aitkenhead, "Understanding the characteristics of serious fraud offending".
270 Europol, The Other Side of the Coin.
271 Michael Levi, "Making sense of professional enablers' involvement in laundering organized crime proceeds and of their regulation", Trends in Organized Crime, vol. 24, n.º 1 (março de 2021); e May e Bhardwa, Organised Criminal Groups Involved in Fraud.
272 Financial Action Task Force, INTERPOL e Egmont Group of Financial Intelligence Units, Illicit Financial Flows from Cyber-Enabled Fraud, p. 15.

ses (i.e., onde as vítimas estão localizadas) recebem e transferem os fundos roubados para o exterior.[273] O recrutamento de mulas de dinheiro envolve o pagamento de uma taxa a indivíduos para receber fundos ilícitos em suas próprias contas bancárias e, em seguida, transferir o dinheiro para uma conta controlada pelo infrator. Isso serve para dispersar os fundos roubados e, assim, reduzir o risco de detecção por um provedor de serviços financeiros. Os fraudadores empregam vários métodos para recrutar mulas de dinheiro, incluindo a publicação de anúncios on-line e o recrutamento dentro da comunidade local.[274] Eles podem ser recrutados dentro de uma rede social existente ou entre grupos que estão em necessidade financeira (por exemplo, crianças e jovens ou estudantes universitários) ou em contextos vulneráveis que também podem ser alvos de fraude.[275]

ESTUDO DE CASO: FACILITAÇÃO DE LAVAGEM DE DINHEIRO

Uma bolsa de moeda virtual registrada na Costa Rica foi acusada de ter facilitado a lavagem de US$ 06 bilhões. Por uma pequena taxa, os usuários puderam depositar e converter moeda fiduciária em moeda digital etransferir esse dinheiro para outros usuários. A empresa registou dados mínimos sobre os utilizadores do serviço e as autoridades acreditavam que a empresa foi projetada com a intenção de ocultar as identidades de seus usuários e torná-los indetectáveis. O serviço foi utilizado por criminosos cibernéticos envolvidos em uma série de crimes predicados, incluindo fraude de cartão de crédito e roubo de identidade.

Fonte: Yongyu Zeng e David Buil-Gil, "Criminalidade cibernética organizacional e organizada", em *Oxford Research Encyclopedia of Criminology and Criminal Justice,* H. Pontell, ed. (Oxford, Oxford University Press, 2023).

ESTUDO DE CASO: FRAUDE ROMÂNTICA

Na Nigéria, dois irmãos foram identificados como envolvidos em fraude romântica que provavelmente teve como alvo uma multidão de vítimas. Um dos irmãos facilitou o acesso a várias contas bancárias estrangeiras, várias das quais foram registradas para empresas que transpiraram ser empresas de fachada. As empresas e contas foram estabelecidas em colaboração com o gerente de um banco local e um co-infrator localizado na China. Quantias significativas foram depositadas nessas contas da empresa, com uma empresa registrada como tendo um faturamento multimilionário. Os fraudadores na Nigéria venderam criptomoedas para o co-infrator na China, que então fez os pagamentos nas contas da empresa.

Fonte: Nigerian Financial Intelligence Unit, "Nigéria divulga tipologias de lavagem de dinheiro por meio de relatório de fraude", 12 de agosto de 2023.

273 Manny Aston e outros, "A preliminary profiling of internet money mules: an Australian perspective", em Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing (2009); Conradt, "Online auction fraud and criminological theories"; e Whittaker e Button, "Understanding pet scams".
274 Leukfeldt e Jansen, "Cyber criminal networks and money mules"; e Soudijn e Zegers, "Cybercrime and virtual offender convergence settings".
275 Skidmore e Aitkenhead, "Understanding the characteristics of serious fraud offending".

Tecnologia facilitadora

Tecnologia para ocultar a criminalidade

A maior disponibilidade de ferramentas de criptografia desempenha um papel importante na viabilização de crimes cibernéticos, como fraudes, incluindo o uso de redes privadas virtuais, criptografia de ponta a ponta para comunicações, a dark web e serviços de hospedagem à prova de balas.[276] Muitas dessas tecnologias são legais e legitimamente disponíveis (por exemplo, serviços de rede privada virtual), embora algumas sejam projetadas e fornecidas por criminosos.[277] Embora algumas dessas ferramentas possam ter usos legítimos pela população em geral, elas também podem ajudar a esconder identidades e facilitar a comunicação segura e as trocas entre criminosos online. A dark web é uma camada criptografada da Internet que permite que os usuários permaneçam ocultos e indetectáveis. Criptomoedas são um método de pagamento preferido na troca de bens e serviços ilícitos na dark web, o que adiciona outra camada de ofuscação para torná-los mais difíceis de rastrear.[278] Para ilustrar, um grande mercado criminoso operava usando um serviço oculto na rede Tor[279] que ocultava as identidades dos usuários e os locais dos servidores.[280] Em um momento, o site tinha 200.000 usuários e, desde sua criação, as transações no mercado foram estimadas em um total de US$ 1 bilhão; as transações geralmente envolviam bitcoin ou outras criptomoedas. Uma variedade de ferramentas e recursos criminosos foram listados no site, incluindo documentos de identidade e dispositivos de acesso fraudulentos, produtos falsificados e outros serviços fraudulentos.

Tecnologia para facilitar a farsa

A tecnologia moderna industrializou metodologias de fraude que existem há muito tempo.[281] Ambientes digitais aumentam as capacidades de comunicação com vítimas, envolvimento em transações comerciais e financeiras fraudulentas e exploração de grandes conjuntos de dados. Além disso, novas tecnologias desenvolvidas por atores legítimos e ilegítimos automatizaram processos que, de outra forma, seriam trabalhosos e custosos. Exemplos incluem o uso de bots para fazer milhares de cliques em um site a fim de manipular classificações de mecanismos de busca (ou seja, fraude de cliques) e dispositivos de fazenda SIM baratos e prontamente disponíveis que contêm vários cartões SIM para fazer chamadas fraudulentas ou enviar mensagens de texto em grandes volumes para vítimas em potencial

Um fator-chave na evolução das metodologias de fraude é a exigência de que os infratores se adaptem continuamente às medidas de segurança compensatórias introduzidas pelo Estado ou pela indústria.[282] Um exemplo é o aumento da fraude sem cartão presente, que surgiu em resposta à introdução do chip e do PIN para aumentar a segurança do cartão.[283] Exemplos mais recentes incluem o surgimento do roubo de impressões digitais de dispositivos comprometidos para neutralizar o uso crescente de dados biométricos para autenticação de identidade e acesso a contas.[284] As tecnologias de inteligência artificial têm o potencial de aumentar este ambiente adverso, aumentando as capacidades dos criminosos para perpetrar fraudes, ao mesmo tempo que oferece às organizações o potencial de melhorar as suas ciberdefesas.[285]

---

276 Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023; Europol, European Cybercrime Centre e European Union Agency for Criminal Justice Cooperation (Eurojust), "First report of the observatory function on encryption" (Haia, 2019); Europol e Eurojust Public Information, "Common challenges in combating cybercrime" (2019); e Annamaria Szakonyi, Brian Leonard e Maurice Dawson, "Dark web: a breeding ground for ID theft and financial crimes", em Handbook of Research on Theory and Practice of Financial Crimes, Abdul Rafay, ed. (Hershey, Pensilvânia, Estados Unidos, IGI Global, 2021).
277 Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023.
278 Szakonyi, Leonard e Dawson, "Dark web: a breeding ground for ID theft and financial crimes".
279 Tor é um navegador usado para acessar a dark web.
280 Europol, "Massive blow to criminal dark web activities after globally coordinated operation", 20 de julho de 2017.
281 Button e Cross, Cyber Frauds, Scams and Their Victims.
282 Albanese, "Fraud".
283 Michael Levi, "Organising and controlling payment card fraud: fraudsters and their operational environment", Security Journal, vol. 16, n.º 2 (abril de 2003).
284 Europol, "Online fraud schemes".
285 Borja Álvarez Martínez e outros, "Mapping the state of the art: artificial intelligence for decision-making in financial crime", em Cybersecurity for Decision Makers, Narashima Rao Yajihala e Kenneth David Strang, eds. (Boca Raton, Flórida, Estados Unidos, CRC Press, 2023). https://www.routledge.com/Cybersecurity-for-Decision-Makers/Vajjhala-Strang/p/book/9781032334974?srsltid=AfmBOoqL0-ovS3IO4TG_gXX5etTA9rOcLN0rjwAxlbsccdVeH4w-ICPo

Os desenvolvimentos em inteligência artificial, em particular a inteligência artificial generativa, que é capaz de gerar conteúdo que imita características humanas, provavelmente desempenharão um papel fundamental na formação de fraudes no futuro. Prevê-se que as capacidades dos fraudadores serão aprimoradas de duas maneiras: (a) amplificando o alcance e o volume de ofensas, facilitando a produção de maiores quantidades de conteúdo fraudulento em maior velocidade; e (b) refinando os métodos existentes de engenharia social, produzindo conteúdo mais sofisticado, convincente e personalizado.[286]

O uso de inteligência artificial foi observado nos seguintes aspectos de fraude:

- Preparo e direcionamento. As tecnologias de inteligência artificial aumentam a capacidade dos infratores de processar e revisar grandes volumes de dados para direcionar vulnerabilidades, processar rapidamente dados roubados para extrair mais valor.[287] A inteligência artificial generativa será capaz de projetar e produzir conteúdo mais refinado e personalizado em velocidade, como texto, imagens e documentos, para facilitar a fraude.[288] FraudGPT, uma ferramenta de inteligência artificial generativa projetada para facilitar o crime cibernético, é capaz de automatizar uma variedade de tarefas, incluindo a criação de materiais fraudulentos, como e-mails.[289]

- Engenharia social. Clones de voz e tecnologias deep-fake fornecem aos infratores capacidade aprimorada de personificar indivíduos ou entidades confiáveis pelas vítimas para promover produtos ou serviços fraudulentos.

- Evitando a detecção. O uso crescente de tecnologia de inteligência artificial na perpetração de fraudes tem o potencial de aumentar o anonimato e ofuscar ainda mais a trilha de volta aos criminosos responsáveis.[290]

Foi observado que os fraudadores são clientes ávidos do crime cibernético como serviço, fazendo uso de ferramentas e/ou dados oferecidos.[291] Espera-se que a maior disponibilidade legítima de tecnologia de inteligência artificial e o aumento da oferta de ferramentas cibernéticas habilitadas por inteligência artificial em mercados criminosos clandestinos sirvam para melhorar as capacidades de possíveis infratores de fraude que são menos qualificados tecnicamente.[292] A consequência é a redução das barreiras de entrada para o envolvimento em fraudes organizadas.

Na presente seção, algumas das técnicas e recursos que desempenham um papel fundamental subjacente na facilitação das muitas variantes da fraude organizada foram destacados. A gama diversificada de canais através dos quais os fraudadores se comunicam com as vítimas, empregam engano, e a gama de técnicas usadas para frustrar os esforços da aplicação da lei, evitar o risco de detecção e punição, também foram destacadas. Esses métodos evoluem continuamente, frequentemente em conjunto com mudanças globais legítimas em comunicações, finanças, comércio e tecnologia. É importante que os Estados-Membros, em parceria com indústrias-chave, como os setores financeiro e tecnológico, identifiquem e rastreiem os métodos subjacentes adotados por fraudadores para fornecer respostas estratégicas mais eficazes para prevenir esses crimes.

---

276 Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023; Europol, European Cybercrime Centre e European Union Agency for Criminal Justice Cooperation (Eurojust), "First report of the observatory function on encryption" (Haia, 2019); Europol e Eurojust Public Information, "Common challenges in combating cybercrime" (2019); e Annamaria Szakonyi, Brian Leonard e Maurice Dawson, "Dark web: a breeding ground for ID theft and financial crimes", em Handbook of Research on Theory and Practice of Financial Crimes, Abdul Rafay, ed. (Hershey, Pensilvânia, Estados Unidos, IGI Global, 2021).
277 Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023.
278 Szakonyi, Leonard e Dawson, "Dark web: a breeding ground for ID theft and financial crimes".
279 Tor é um navegador usado para acessar a dark web.
280 Europol, "Massive blow to criminal dark web activities after globally coordinated operation", 20 de julho de 2017.
281 Button e Cross, Cyber Frauds, Scams and Their Victims.
282 Albanese, "Fraud".
283 Michael Levi, "Organising and controlling payment card fraud: fraudsters and their operational environment", Security Journal, vol. 16, n.º 2 (abril de 2003).
284 Europol, "Online fraud schemes".

CAPÍTULO V

Combate à fraude organizada

A fraude organizada é perpetrada em grandes volumes e penetra em muitos setores comerciais e financeiros. Para os perpetradores, as recompensas são altas e as barreiras e riscos são baixos. Uma resposta abrangente inclui estratégias de prevenção ao crime e leis adequadas para fechar as abundantes oportunidades criminosas para perpetrar esses crimes, em conjunto com uma aplicação robusta da lei para mirar e dissuadir os infratores. Controles mais eficazes são necessários para abordar as vulnerabilidades técnicas em infraestrutura e sistemas e para fornecer educação e promover a conscientização nos setores público e empresarial para ajudar a defender contra fraudes. Respostas estratégicas devem considerar os seguintes princípios: [293]

- Impedir que o crime organizado se (re)infiltre nas comunidades, na economia e nas instituições políticas
- Perseguir grupos criminosos organizados eseus ganhos ilícitos, aumentando assim sua capacidade operacional de custos e riscos
- Proteger pessoas vulneráveis e vítimas de (mais) danos
- Promover parcerias e cooperação a todos os níveis, incluindo além das fronteiras internacionais – uma abordagem de toda a sociedade

Estratégias contra o crime organizado precisam levar em conta as complexidades do problema da fraude organizada, especialmente porque é transnacional, explora tecnologias e sistemas globais e se adapta continuamente a mudanças em sistemas comerciais e financeiros. A mudança depende de políticas que adotam uma abordagem multifacetada que coordena respostas entre departamentos e agências governamentais, setores-chave na indústria privada e na sociedade civil. Há também uma necessidade de maior colaboração internacional para entender e abordar a fraude organizada que atravessa fronteiras.

Essas estratégias abrangentes de toda a sociedade contra o crime organizado são particularmente importantes em contextos onde os grupos criminosos organizados são cada vez mais policriminosos,[294] envolvidos em várias formas de crime organizado, incluindo fraude organizada. Estratégias isoladas ou respostas focadas em apenas uma área, como garantir resultados de justiça criminal, não abordariam suficientemente o caráter multidimensional dos grupos criminosos organizados envolvidos na prática de múltiplas infrações. Além disso, a falta de coordenação entre as respostas a diferentes tipos de crime pode criar brechas, duplicar esforços e usar inadequadamente recursos restritos. Estratégias regionais e

293 UNODC, "Kit de ferramentas estratégicas contra o crime organizado para o desenvolvimento de estratégias de alto impacto" (Viena, 2021).
294 Veja, por exemplo, UNODC, Escritório Regional para o Sudeste Asiático e Pacífico, Cassinos, fraude cibernética e tráfico de pessoas para criminalidade forçada no Sudeste Asiático; e UNODC, Departamento de Pesquisa e Análise de Tendências e Escritório Regional para a África Ocidental e Central, "Impacto do crime organizado transnacional na estabilidade e no desenvolvimento no Sahel" (Viena, 2024). https://www.unodc.org/documents/data-and-analysis/tocta_sahel/TOCTA_Sahel_Transversal_2024.pdf

nacionais contra o crime organizado estruturadas em torno dos quatro pilares mencionados acima (prevenir, perseguir, proteger e promover) podem servir como uma estrutura abrangente aser complementada por respostas personalizadas e específicas para cada crime, como planos de ação, centros de coordenação eforças-tarefa contra a fraude organizada.

LISTA DE VERIFICAÇÃO PARA REVISÃO DE ESTRATÉGIAS E ELABORAÇÃO DE PLANOS DE AÇÃO CONTRA FRAUDES

PREVENIR a fraude organizada

- Análise estratégica para identificar e avaliar as causas econômicas, culturais, sociais e institucionais da marginalização e vulnerabilidade que criam os caminhos para o envolvimento em fraudes.
- Respostas para desviar ou dissuadir grupos vulneráveis ao recrutamento ou a outras formas de envolvimento em fraudes. Isso inclui abordar aqueles que atuam em setores e profissões-chave suscetíveis à corrupção, além de adotar medidas para incentivar denúncias e proteger vítimas, testemunhas, informantes e denunciantes.
- Medidas para contestar as narrativas dos grupos do crime organizado que recrutam indivíduos para cometer fraudes.

PERSEGUIR grupos criminosos organizados

- Legislação em vigor para a criminalização da fraude, incluindo, quando apropriado, a classificação da fraude como crime grave, em conformidade com o artigo 2(b) da Convenção sobre o Crime Organizado. As penas devem ser dissuasivas, proporcionais, claras e certas, evitando qualquer violação de direitos humanos ou constitucionais.
- Agências de aplicação da lei e o Judiciário equipados com as competências técnicas necessárias para investigar eficazmente a fraude organizada, incluindo investigação financeira, investigação de crimes cibernéticos, perícia digital e técnicas especiais de investigação relevantes, além de identificar, rastrear, bloquear, apreender e confiscar produtos do crime e outros ativos.
- Sistemas de banco de dados para agregar e analisar dados nacionais de aplicação da lei, a fim de facilitar a identificação de grupos criminosos organizados e orientar as respostas estratégicas e táticas à fraude organizada.

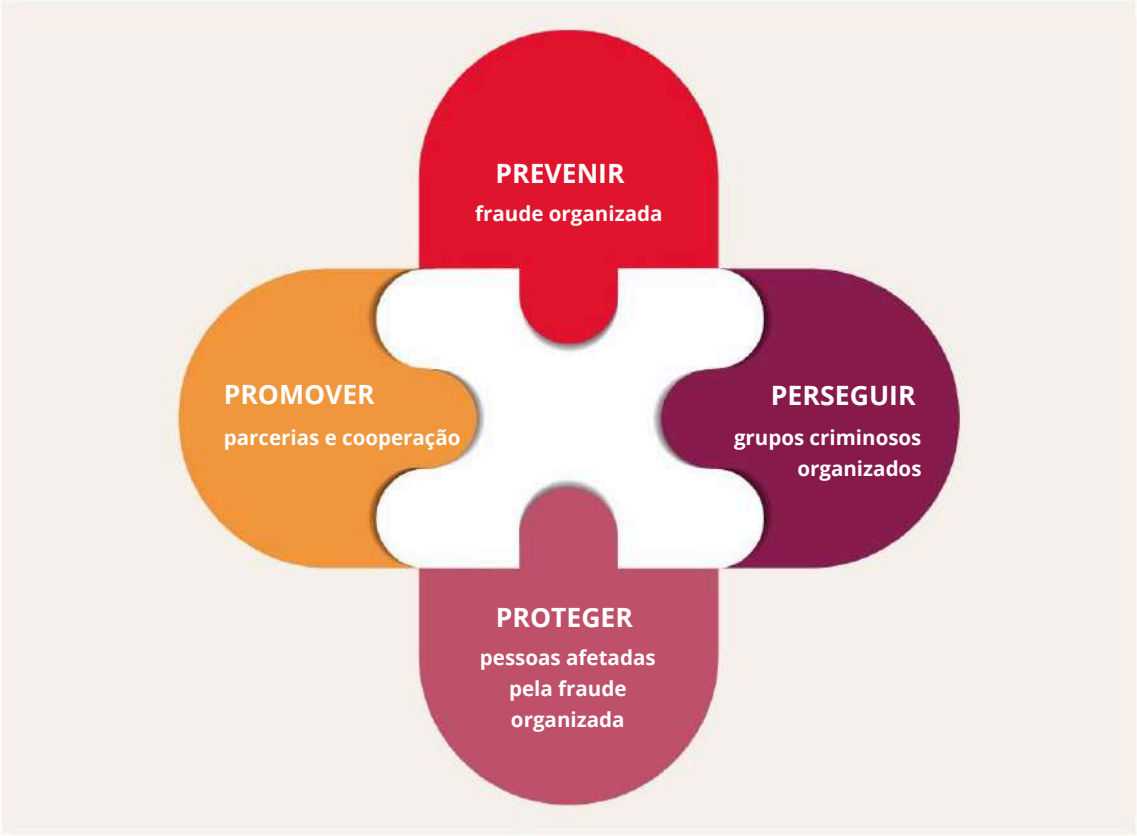
PROTEGER pessoas afetadas pela fraude organizada

- Campanhas de conscientização para o público e a comunidade empresarial, visando promover comportamentos seguros e proteger contra o risco de se tornarem vítimas de fraude.
- Medidas para identificar e apoiar vítimas que são vulneráveis e estão em risco de serem repetidamente fraudadas ou de sofrer danos graves.

PROMOVER parcerias e cooperação

- Abordagem de toda a sociedade para prevenir e combater a fraude, incluindo a participação do setor privado, da sociedade civil, do meio acadêmico e de atores do setor educacional, conforme apropriado.
- Canais de denúncia claros para que o público e a comunidade empresarial possam relatar fraudes às autoridades competentes e acessar o suporte necessário.
- Medidas legislativas e outras diretrizes para orientar o compartilhamento de informações entre o Estado e o setor privado, incluindo empresas de setores-chave, como finanças e tecnologia.
- Medidas para promover o engajamento estratégico com empresas e órgãos do setor privado, identificar fraquezas e vulnerabilidades sistêmicas e coordenar respostas estratégicas eficazes para prevenir fraudes.
- Estruturas para fomentar a cooperação internacional em matéria penal, incluindo assistência jurídica mútua e equipes conjuntas de investigação.

FIGURA. QUATRO PILARES ESTRATÉGICOS PARA COMBATER A FRAUDE ORGANIZADA



Prevenção de fraude organizada

Campanhas de prevenção e intervenções podem ser direcionadas para dissuadir indivíduos de caminhos para crimes de fraude organizada. A pesquisa é limitada, mas, em certas subculturas, os perpetradores de fraude e crime cibernético têm legitimidade social. Indivíduos nessas comunidades e redes podem adotar várias narrativas para racionalizar seu comportamento ofensivo; exemplos incluem uma visão de que as vítimas estão recebendo o que merecem (por exemplo, são gananciosas) ou atitudes que minimizam os crimes e danos causados pela fraude.[295] Além disso, a fraude pode oferecer aos infratores um meio de alcançar sucesso material que de outra forma seria inatingível, particularmente em regiões onde a pobreza é alta e as perspectivas legítimas são baixas. Em alguns casos, os fraudadores ganham destaque local e fazem demonstrações públicas de riqueza, o que os torna figuras aspiracionais para os jovens. Alguns jovens se envolvem em crimes cibernéticos sem saber que estão cometendo um crime ou causando danos.[296] Esses crimes podem equivaler a fraude de baixo nível, mas trazem o risco de que os infratores sejam atraídos pela perspectiva de lucros criminosos e evoluam para fraude organizada. Os padrões e caminhos para a fraude organizada precisam ser compreendidos dentro dos contextos sociais, econômicos e políticos locais, e as intervenções precisam ser direcionadas para abordar as causas raiz das infrações de fraude.[297]

295 Veja, por exemplo, Shover, Coffey e Sanders, "Dialing for dollars"; e Whitty, "419: it's just a game".
296 Mary Aiken, Julia Davidson e Philipp Amann, "Caminhos juvenis para o cibercrime" (2016).
297 Veja, por exemplo, Lorenzo Pasculli, "Coronavírus e fraude no Reino Unido: da responsabilização da sociedade civil à desresponsabilização do Estado", Coventry Law Journal, vol. 25, n.º 2 (dezembro de 2020).

Grupos criminosos organizados envolvidos em fraudes incorporam associações soltas com indivíduos que são vitais para facilitar ocrime, mas adotam um papel periférico no esquema fraudulento. Isso inclui indivíduos em ocupações profissionais que facilitam a fraude (por exemplo, profissionais de direito e finanças) e membros do público que fornecem o uso de suas contas por uma taxa (por exemplo, mulas de dinheiro). Para esses co- infratores, os níveis de cumplicidade e culpabilidade podem ser ambíguos, com alguns contentes em pegar o dinheiro sem fazer muitas perguntas sobre os crimes subjacentes. Campanhas de informação pública direcionadas a esses grupos de risco para destacar a gravidade do crime e o risco de que eles recebam sanções da justiça criminal podem servir para aumentar a conscientização e desviar e dissuadir indivíduos de se envolverem nesses crimes.

ESTUDO DE CASO: DESVIANDO OS JOVENS DO CIBERCRIME

Em resposta ao aumento no volume de jovens que entram no sistema de justiça criminal por crimes de *hacking*, o Reino dos Países Baixos estabeleceu o programa de reabilitação HACK_Right para infratores primários com idade entre 12 e 30 anos. O programa serve para aumentar a conscientização sobre a lei, as consequências do envolvimento em *hacking* e o impacto nas vítimas. O objetivo é desviar as pessoas do crime cibernético e de outros crimes potencialmente mais sérios (como fraude organizada) e redirecionar essas habilidades para atividades legítimas.

Fonte: JAM Schiks, Susanne van 't Hoff-de Goede eE. Rutger Leukfeldt, "Uma intervenção alternativa para hackers juvenis? Uma avaliação qualitativa da intervenção Hack_Right", *Journal of Crime and Justice* (2023).

Perseguição de grupos criminosos organizados

Legislação

A adoção de estruturas legais claras e robustas é importante para avaliar e combater a fraude, de modo a garantir que os profissionais possam identificar com confiança a presença do crime organizado e atribuir os recursos e intervenções proporcionais. Além disso, a cooperação internacional depende de ter um entendimento claro e comum entre as diferentes jurisdições legais do que constitui fraude organizada, guiada pelas disposições da Convenção sobre o Crime Organizado.

Alguns Estados-Membros abordaram delitos relacionados com fraudes em legislação especializada, enquanto outros incorporaram tais delitos em códigos criminais existentes. A fraude também pode ser abordada numa multiplicidade de leis, criando múltiplas definições. Há uma necessidade de quadros legais para fornecer suficiente:

- Clareza, para facilitar a compreensão do profissional para garantir a aplicação eficaz da lei e uma delimitação clara de comportamentos legais e ilegais
- Cobertura, que deve ser abrangente e flexível o suficiente para capturar a diversidade de métodos usados para perpetrar fraudes, incluindo métodos emergentes e futuros, como aqueles que exploram novas tecnologias.[298]

[298] Veja, por exemplo, Ben Summers, "The Fraud Act 2006: has it had any impact?", *Amicus Curiae,* n.º 75 (2008).

Alguns países adotaram definições legais altamente especificadas e prescritivas de fraude que enumeram os vários produtos, serviços ou técnicas que constituem atividade fraudulenta na lei, por exemplo, o uso de informações pessoais de uma vítima, personificação de uma autoridade ou criação de uma falsa esperança de ganhar algo. Outros empregam definições legais amplas que podem ser aplicadas a uma variedade de cenários ou contextos criminais (veja o cap. I acima). A fraude é altamente diversa nos métodos empregados pelos perpetradores e no impacto sobre as vítimas ou mais amplamente. Assim, as estruturas de condenação dos países variam, incluindo a presença de fatores agravantes e atenuantes, que podem se referir à experiência da vítima, às características dos fraudadores e à perpetração de certas categorias de fraude.[299]

A combinação de fatores agravantes incluídos na legislação pode determinar os tipos de fraude e a pena máxima, que podem variar entre os Estados. Uma perspectiva centrada na vítima foi adotada em algumas estruturas legais, enquanto outras são focadas nas características dos infratores e seus métodos. Ao determinar o impacto da infração, alguns países olham para as perdas financeiras como uma proporção da renda anual da vítima, ou a quantia de dinheiro roubada, se dispositivos de computador foram usados ou se um reincidente ou grupo criminoso organizado está envolvido (veja os exemplos abaixo).

EXEMPLO LEGISLATIVO: MÉXICO

CÓDIGO PENAL FEDERAL

Artigo 386. Qualquer pessoa que adquirir algo ilicitamente ou alcançar um ganho indevido enganando outra pessoa ou se aproveitando do erro dessa pessoa será culpada pelo crime de fraude.

O crime de fraude será punido com as seguintes penas:

I. Reclusão de três dias a seis meses ou multa de 30 a 180 unidades de multa, se o valor do bem adquirido por meio do ato de fraude não for superior a 10 vezes o salário mínimo;
II. Reclusão de seis meses a três anos e multa de 10 a 100 vezes o salário mínimo, se o valor do bem adquirido por meio do ato de fraude for superior a 10 vezes, mas não superior a 500 vezes o salário mínimo;
III. Reclusão de 3 a 12 anos e multa de até 120 vezes o salário mínimo, se o valor do bem adquirido por meio do ato de fraude for superior a 500 vezes o salário mínimo.

299 Esses fatores são compilados para resumir as estruturas legais dos diferentes países. Nem todos os fatores estavam presentes nas estruturas legislativas de cada país. Exemplos de fatores agravantes incluem: experiência da vítima (grande impacto financeiro ou outro impacto pessoal (por exemplo, instilar medo ou uma sensação de perigo na vítima); grande perda financeira para indivíduos ou entre vítimas; grande escala em termos de volume de vítimas e/ou quantia de dinheiro perdida; mirar em vítimas que são de alguma forma vulneráveis; mirar no Estado, instituições públicas ou caridade; características do fraudador (envolvimento de um grupo criminoso organizado ou gangue; infratores reincidentes); ecategorias de fraude (fraude eletrônica ou de computador; envolvendo aemissão de ações, títulos, *warrants* ou valores mobiliários; envolvendo arepresentação de um funcionário público, abuso de uma posição oficial ou abuso de relações pessoais).

EXEMPLO LEGISLATIVO: UZBEQUISTÃO

CÓDIGO PENAL

Artigo 168. Fraude

Fraude, ou seja, a aquisição da propriedade de alguém ou o direito a ela por engano ou abuso de confiança,

será punida com uma multa de até 100 vezes o salário mínimo mensal, ou trabalho corretivo por até um ano, ou prisão por até seis meses.

A fraude cometida:
(a) Em grande escala;
(b) Repetidamente ou por um reincidente perigoso;
(c) Por concerto prévio de um grupo de indivíduos;
(d) Com a ajuda de dispositivos computadorizados;
será punida com uma multa de 100 a 300 vezes o salário mínimo mensal, ou trabalho corretivo por até dois anos, ou prisão por até cinco anos.

A fraude cometida:
(a) Em grande escala;
(b) Por um reincidente perigoso especial;
(c) Por um grupo organizado ou em seus interesses;
será punida com uma multa de 300 a 600 vezes o salário mínimo mensal, ou trabalho corretivo por até três anos, ou prisão de 5 a 10 anos.

No caso de compensação pelo dano pecuniário, a pena de prisão não será aplicada.

As faixas de sentença também são altamente variáveis. Em alguns países (por exemplo, Uruguai), quatro anos de prisão é a sentença máxima, enquanto em outros países (por exemplo, Estados Unidos) há provisão para sentenças de até 30 anos de prisão. Em alguns outros países, não há faixas de sentença estipuladas, com sentenças provavelmente dependentes da discrição do promotor ou da aplicação de um critério geral para determinar a gravidade do crime.

EXEMPLO LEGISLATIVO: ESTADOS UNIDOS DA AMÉRICA

TÍTULO 18

Artigo 1344. Fraude Bancária

Quem, com conhecimento, executa ou tenta executar um esquema ou artifício:

(a) Para fraudar uma instituição financeira; ou
(b) Para obter qualquer um dos valores monetários, fundos, créditos, ativos, títulos ou outras propriedades pertencentes a, ou sob a custódia ou controle de, uma instituição financeira, por meios de falsos ou fraudulentos pretextos, representações ou promessas;

será multado em não mais de $1.000.000 ou preso por não mais de 30 anos, ou ambos.

Aplicação da Lei

A aplicação da lei tem um papel importante a desempenhar como parte de uma estratégia mais ampla focada na prevenção da fraude e na proteção do público. A justiça criminal pode agir como um impedimento para desmotivar infratores ou potenciais infratores, proporciona punição, protege a sociedade de infratores prejudiciais e reforça os valores sociais sobre comportamentos aceitáveis.[300] A capacidade de fornecer uma aplicação robusta da lei é afetada pelos fatores abaixo descritos.

Avaliação e direcionamento da fraude organizada

No contexto das demandas variadas e concorrentes do crime organizado, os recursos policiais comumente se direcionam para crimes diferentes da fraude.[301] Ao enfrentar a fraude organizada, as sentenças criminais podem ser insuficientes, as informações podem estar faltando e, talvez mais fundamentalmente, podem existir incertezas sobre como integrar a fraude nas políticas contra crimes graves e organizados. A incapacidade de identificar essas interseções pode deixar os fraudadores organizados impunes à aplicação da lei. Estruturas claras e robustas de políticas e legislações ajudam a identificar mais claramente os casos de fraude que constituem casos graves e organizados de crime e fortalecem as avaliações na aplicação da lei para direcionar recursos proativos de investigação criminal.

Investigação criminal

Há preocupações em muitas regiões de que a polícia possa não estar preparada ou equipada para lidar com o crescimento da ciberfraude. Isso se relaciona parcialmente às políticas, sistemas e cultura da aplicação da lei que têm lutado para se adaptar a esse novo cenário criminal.[302] Algumas agências de aplicação da lei estabeleceram unidades especializadas com capacidades em investigação de fraude e cibercrime, comumente focadas em realizar as investigações mais complexas para direcionar os infratores de maior risco.[303] Os recursos principais incluem a capacidade de realizar investigações digitais eficazes, profissionais com experiência em investigação financeira e forense digital, e tecnologia para facilitar os procedimentos investigativos.

Interrupção

A fraude organizada pode ser perpetrada em grandes volumes e a uma velocidade frequentemente incompatível com o ritmo lento das investigações complexas de fraude. A interrupção pode tirar proveito de uma ampla gama de técnicas e capacidades disponíveis para a aplicação da lei e organizações parceiras, oferecendo táticas mais diversas para impedir a capacidade dos criminosos de cometer crimes e, assim, reduzir o risco de mais danos ao público.[304] As táticas podem ser direcionadas para os atos, atores ou ambientes criminógenos, com exemplos-chave incluindo a retirada de sites; a apreensão de proventos criminosos; o direcionamento de indivíduos-chave em uma rede, como aqueles que facilitam a lavagem de dinheiro ou fornecem informações pessoais roubadas; e intervenções para interromper a co-perpetracão, como táticas para minar a confiança em mercados criminosos.[305]

---

300 Button e outros, "Fraud and Punishment".
301 Doig e Levi, "A case of arrested development?".
302 Adam M. Bossler e Tom J. Holt, "Patrol officers' perceived role in responding to cybercrime", Policing: An International Journal of Police Strategies and Management, vol. 35, No. 1 (março de 2012); e Barry Loveday, "Still plodding along? The police response to the changing profile of crime in England and Wales", International Journal of Police Science and Management, vol. 19, No. 2 (abril de 2017).
303 Mark Button e Martin J. Tunley, "Explaining fraud deviancy attenuation in the United Kingdom", Crime Law and Social Change, vol. 63, Nos. 1 e 2 (março de 2015); e Dale Willits e Jeffrey Nowacki, "The use of specialized cybercrime policing units: an organizational analysis", Criminal Justice Studies, vol. 29, No. 2 (abril de 2016).
304 Michael Skidmore, "Lifting the lid on 'disruption' as an approach to controlling serious and organised crime", Perspectives on Policing Paper, No. 9 (Londres, The Police Foundation, 2023).
305 Para ilustrar, agências de aplicação da lei de vários países miraram um site criminoso que fornecia software para criminosos fazerem chamadas automáticas que simulavam serviços legítimos. Isso interrompeu o fornecimento de software que se estimava ter sido usado para fazer 10 milhões de chamadas fraudulentas para membros do público e causou perdas de €115 milhões (Europol, "Online fraud schemes"). Veja também Alice Hutchings e Thomas Holt, "The online stolen data market: disruption and intervention approaches", Global Crime, vol. 18, No. 1 (2016).

Cooperação Internacional

É comum que os infratores, vítimas, tecnologias e outros facilitadores da fraude organizada sejam transnacionais, o que pode causar confusão sobre a jurisdição e dificultar investigações criminais localizadas. Isso se deve, entre outras coisas, aos desafios de se obter rapidamente assistência jurídica mútua de outros países, especialmente para adquirir e compartilhar dados e evidências do setor privado para facilitar a investigação e a acusação, além dos complexos processos de extradição.[306] A cooperação internacional também é importante para a apreensão e confisco de proventos criminais, devolução de bens roubados e garantia de compensação para as vítimas.[307]

Força de trabalho diversa

As pessoas têm experiências diferentes com o sistema de justiça criminal, devido a fatores como racismo, sexismo, capacitismo, homofobia e discriminação com base no status socioeconômico. A capacidade de lidar adequadamente com essas experiências é limitada pela contínua sub-representação de mulheres e pessoas de diversas origens nas entidades de aplicação da lei, no sistema de justiça criminal e em posições de tomada de decisão, com pesquisas[308] indicando que as oficiais femininas estão em melhor posição para atender às necessidades de mulheres e meninas em suas comunidades. Apesar disso, a UNODC constatou que a porcentagem de policiais mulheres em todos os países estudados variava entre 3% e 37%.[309]

ESTUDO DE CASO: ACORDO REGIONAL PARA COMBATER A FRAUDE ORGANIZADA

A China e a Associação das Nações do Sudeste Asiático, em conjunto com o Escritório das Nações Unidas sobre Drogas e Crime (UNODC), desenvolveram uma estratégia transnacional para melhorar as respostas nacionais, bilaterais e regionais ao tráfico de pessoas e às operações de cassinos e golpes. Um objetivo chave é aumentar a capacidade das agências de aplicação da lei e dos profissionais da justiça criminal de responder de maneira abrangente e coordenada. Uma rede de pontos focais regionais foi estabelecida para ajudar no compartilhamento de informações e na coordenação de investigações criminais, além de facilitar a prestação de respostas rápidas a solicitações de assistência dos países da região. Além disso, a rede serve para fortalecer a capacidade dos membros em investigações de cibercrime, perícias digitais, manuseio de evidências digitais, ativos virtuais e investigações financeiras. Ela também realiza trabalhos para revisar e fortalecer a implementação de marcos legislativos e de políticas para combater crimes relacionados às operações de cassinos e golpes, além de aprimorar a cooperação com o setor privado, órgãos regionais e a sociedade civil.

Fonte: UNODC, Escritório Regional para o Sudeste Asiático e Pacífico, "Roteiro de cooperação regional dos Estados- membros da ASEAN e da República Popular da China para abordar o crime organizado transnacional e o tráfico de pessoas associado a cassinos e operações fraudulentas no Sudeste Asiático" (Bangkok, 2023).

306 Eva Nagyfejeo, "EU's emerging strategic cyber culture(s)", Policing: A Journal of Policy and Practice, vol. 15, n.º 1 (março de 2021).
307 Por exemplo, a Joint Cybercrime Action Taskforce da Europol coordena atividades operacionais para combater fraudes transnacionais com pagamentos, e o Eurojust facilita a prestação de assistência jurídica e cooperação entre os países membros (Eurojust, "Actions across Europe against online fraud with cryptocurrencies", comunicado de imprensa, 7 de novembro de 2023). Veja também South-East Asia Justice Network, disponível em www.unodc.org/roseap/en/SEAJust/index.html.
308 UNODC, INTERPOL e United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women), Women in Law Enforcement in the ASEAN Region (Bangkok, 2020).
309 UNODC, Issue Paper: Organized Crime and Gender.

Policiamento baseado em inteligência

A fraude organizada geralmente ultrapassa fronteiras jurisdicionais ao recrutar co-infratores geograficamente dispersos, visando vítimas em várias jurisdições e utilizando fornecedores de tecnologia localizados no exterior. A fraude organizada que é geograficamente dispersa pode não se alinhar com as prioridades da polícia territorial, que estão focadas em uma agenda local, em vez de uma agenda transfronteiriça, e que são limitadas a jurisdições, dados e sistemas discretos e localizados. A visibilidade depende de uma perspectiva nacional ou internacional sobre o crime. Além disso, nem toda fraude é sentida de maneira aguda por cada vítima individual: o impacto é difuso, e só quando visto de forma agregada é que esse crime se torna sério, por exemplo, devido ao fato de os fraudadores estarem cometendo grandes volumes de fraudes, adquirindo grandes lucros criminosos ou minando a confiança e a integridade dos sistemas legítimos.[310] A capacidade de avaliar o dano neste contexto depende da disponibilidade de informações para conectar os delitos e identificar crimes persistentes e os riscos associados.

Identificar fraude organizada depende da compilação de conjuntos de dados e da análise de conexões entre pontos de dados para extrair informações sobre grupos criminosos organizados. Uma única vítima que denuncia uma fraude pode ter um conhecimento limitado dos infratores e seus métodos; padrões de crime e os riscos correspondentes do crime organizado são identificados por meio de processos de análise de dados para conectar crimes separados e produzir a inteligência necessária para uma resposta proativa da polícia. Um modelo de policiamento que se concentra unicamente na realização de investigações criminais reativas sobre crimes denunciados comumente falha em ir além da superfície e abordar o esquema fraudulento subjacente, pois a fraude organizada raramente é revelada em um único relatório de fraude.

Proteção das pessoas afetadas pelo crime organizado

Os fraudadores empregam técnicas de engenharia social para explorar os fatores psicológicos e comportamentais humanos que tornam as pessoas vulneráveis ao engano e à manipulação.[311] Consequentemente, a prevenção eficaz do crime depende não apenas do desenvolvimento de sistemas mais seguros, mas também de equipar a comunidade pública e empresarial com o conhecimento, a conscientização e as capacidades para se defender contra fraudes. A fraude é altamente diversa e está em constante evolução, e a eficácia das campanhas de educação e conscientização reside em mensagens públicas que sejam sucintas e claras o suficiente para influenciar os comportamentos e a vigilância do público.[312] A eficácia também reside na acessibilidade de tais campanhas, incluindo a consideração dos diferentes idiomas falados por grupos populacionais específicos e medidas de acessibilidade para pessoas com deficiência. A vulnerabilidade é frequentemente específica do contexto e as informações públicas podem precisar ser projetadas e direcionadas a pessoas que estão envolvidas em mercados ou atividades específicas onde há riscos.[313] Além disso, a vulnerabilidade não é estática: ela oscila de acordo com as circunstâncias da vítima e os métodos específicos empregados pelos fraudadores. Portanto, pode haver necessidade de mensagens de prevenção para chegar a um indivíduo ou empresa em risco no momento certo.[314]

---

310 Levi, "Organized fraud and organizing frauds".
311 Brandon Atkins e Wilson Huang, "A study of social engineering in online frauds", Open Journal of Social Sciences, vol. 1, n.º 3 (agosto de 2013).
312 Veja, por exemplo, Comissão Europeia, Anti-Fraud Knowledge Centre, Biblioteca, Boas práticas, "#Fraudoff", disponível no European Union Funds Anti-Fraud Knowledge and Resource Centre (https://antifraud-knowledge-centre.ec.europa.eu/); e Cassandra Cross e Michael Kelly, "The problem of 'white noise': examining current prevention approaches to online fraud", Journal of Financial Crime, vol. 23, n.º 4 (outubro de 2016).
313 Por exemplo, a Securities and Exchange Commission dos Estados Unidos oferece educação direcionada a investidores em potencial para melhorar seu conhecimento sobre o mercado e ajudá-los a se defender contra fraudes (veja em https://www.investor.gov/about-us).
314 O Cyber Security Information Sharing Partnership no Reino Unido tem como objetivo ajudar as empresas a compartilhar informações em tempo real sobre ameaças cibernéticas dinâmicas, garantindo que as organizações membros estejam cientes dos riscos emergentes e possam implementar contramedidas (Reino Unido, "Government launches information sharing partnership on cyber security", comunicado de imprensa, 27 de março de 2013).

Os fraudadores podem atacar a mesma vítima em várias ocasiões, como em alguns casos de fraude romântica e de investimento, por meio de manipulação ou engano por parte do perpetrador ou com base em uma vulnerabilidade pessoal.[315] Essas vítimas podem não reconhecer que estão sendo fraudadas e podem não denunciar a fraude à polícia. Fontes financeiras e de inteligência podem ajudar a identificar vítimas em risco e impulsionar respostas proativas de proteção por parte das entidades de aplicação da lei e outras organizações nos setores público e privado.[316]

Promoção de parcerias e cooperação

Coleta nacional de dados

As informações sobre fraude vêm de uma variedade de fontes e em várias formas. Elas incluem relatórios sobre crimes e inteligência recebidos de membros do público, corporações privadas e pequenas empresas que foram alvos ou fraudadas, relatórios e inteligência coletados por reguladores do setor público ou do setor privado e relatórios coletados por organizações de defesa do consumidor ou outras fontes. As agências de aplicação da lei não têm o monopólio dos dados de fraude, e essas fontes variadas significam que é difícil compilar um quadro abrangente do crime para demonstrar a escala e a natureza do problema.[317] A fragmentação dos dados significa que há desafios para as agências estaduais na identificação e no rastreamento de padrões e tendências importantes, na avaliação de riscos, na atribuição de funções e recursos e no desenvolvimento de estratégias robustas. Há também uma falta de dados desagregados por gênero sobre a questão, o que afeta a capacidade das autoridades nacionais de entender as tendências de gênero e as características de intersecção que moldam as experiências das pessoas com fraude organizada. No entanto, há uma série de medidas que podem ser tomadas para produzir um quadro mais consolidado. Essas medidas são descritas abaixo.

Relato centralizado de fraude

O panorama fragmentado de denúncias pode impactar as vítimas e suas experiências ao buscar a ajuda e o apoio de que necessitam. Elas podem se deparar com um cenário confuso de entidades do setor público e privado, além de organizações da sociedade civil, que oferecem uma ampla gama de suporte, tornando a busca pelo serviço adequado um processo prolongado de tentativa e erro, com vítimas sendo encaminhadas de uma organização para outra.[318] Esse problema pode ser agravado por respostas ineficazes da polícia, especialmente em equipes regionalizadas que possuem capacidade limitada para conduzir investigações complexas e transfronteiriças. A oferta de canais de denúncia que sejam simplificados e interconectados contribui para garantir que as vítimas recebam o apoio necessário, ao mesmo tempo em que consolida o panorama nacional sobre fraudes e suas vítimas.

315 Veja, por exemplo, Elisabeth Carter, "Confirm not command: examining fraudsters' use of language to compel victim compliance in their own exploitation", The British Journal of Criminology, vol. 63, n.º 6 (novembro de 2023).
316 Um exemplo da Austrália envolveu a polícia, em parceria com o departamento governamental de comércio, monitorando transferências internacionais de dinheiro para países de alto risco a fim de identificar e abordar indivíduos suspeitos de serem vítimas de fraude (Cross e Blackshaw, "Improving the police response to online fraud").
317 Levi e Burrows, "Measuring the impact of fraud in the UK".
318 Button e outros, "Not a victimless crime".

ESTUDO DE CASO: RELATÓRIOS CENTRALIZADOS

Na Austrália, o *National Anti-Scam Centre* é um exemplo de uma iniciativa liderada pelo governo para facilitar a denúncia de fraudes por parte das vítimas. O centro tem um foco na proteção do consumidor e adota o princípio de *"nenhuma porta errada"*, pelo qual, independentemente das circunstâncias e necessidades individuais, todas as vítimas de fraude recebem suporte. Em outros países, tem havido um foco na consolidação de sistemas de registro de crimes por meio da introdução de centros nacionais de denúncias para vítimas de fraude e crimes cibernéticos. Por exemplo, nos Estados Unidos da América, o *Internet Crime Complaint Center*, operado pelo FBI, recebe todos os relatórios públicos de crimes na Internet, incluindo fraudes.

Fontes: Austrália, National Anti-Scam Centre, "National Anti-Scam Centre in action", atualização trimestral (julho–Setembro de 2023); e www.fbi.gov/video-repository/ic3_112117.mp4/view.

A disponibilidade de um órgão único, responsável e autorizado para receber denúncias de crimes facilita o processo de denúncia para as vítimas, o que é particularmente importante no caso das fraudes, considerando os altos níveis de subnotificação.[319]

Integração de conjuntos de dados

Para combater a fraude, parcerias estratégicas com o setor privado e outros atores são indispensáveis, inclusive para o desenvolvimento de marcos legais que viabilizem o compartilhamento de dados e inteligência sobre crimes. Um grande volume de fraudes tem como alvo instituições como bancos, prestadores de serviços financeiros, empresas de comércio eletrônico e outras companhias. Muitas vezes, isso ocorre por meio do uso indevido de contas legítimas de clientes (por exemplo, tomada de conta ou fraude ao consumidor), levando diversas vítimas a denunciar tais fraudes diretamente ao seu provedor de serviços, em vez de à polícia.
Além disso, empresas do setor privado realizam análises de dados complexas para identificar riscos e se proteger contra fraudes ou até mesmo iniciam suas próprias investigações internas para identificar os responsáveis. Para isso, são necessários canais que garantam o compartilhamento eficiente desses dados com as autoridades policiais ou outros órgãos públicos.[320]

A integração de conjuntos de dados de diferentes setores ajuda a compilar um panorama estratégico mais completo do problema. Essas informações compartilhadas também podem ser utilizadas para alavancar respostas táticas contra crimes e riscos relacionados, que, de outra forma, permaneceriam ocultos. Tais respostas incluem ações policiais baseadas em inteligência e intervenções para redução de danos, alertando sobre riscos e protegendo indivíduos ou empresas de se tornarem vítimas de fraude.

Parcerias entre os setores público e privado

As fraudes organizadas raramente ocorrem em espaços públicos sob controle do Estado, mas sim em ambientes comerciais controlados por intermediários do setor privado, que fornecem serviços de comunicação via Internet, comércio eletrônico, serviços financeiros, aplicativos web e telecomunicações. Empresas privadas projetam as tecnologias e sistemas que os fraudadores incorporam e exploram em seus esquemas ilícitos. No entanto, elas também desempenham um papel central como vítimas, fornecedoras de segurança online, fontes de informações para compreender esses crimes e centros de expertise e capacidade antifraude.

319 Por exemplo, apenas 17% das fraudes vivenciadas pelo público no Reino Unido no período de 12 meses entre abril de 2016 e março de 2017 foram reportadas à polícia (Reino Unido, Home Office, The Scale and Nature of Fraud: A Review of the Evidence (2018)).
320 No Reino Unido, a polícia desenvolveu uma parceria estreita com a Cifas e a United Kingdom Finance, que coletam dados sobre fraudes que têm como alvo suas organizações membros, incluindo partes interessadas-chave no setor de serviços financeiros. Veja, por exemplo, Reino Unido, Office for National Statistics, Crime in England and Wales: year ending June 2023, 19 de outubro de 2023.

Assim, têm um papel particularmente importante no desenvolvimento e implementação de estratégias para eliminar vulnerabilidades exploradas por criminosos, visando mitigar riscos futuros de fraude organizada.

O escopo para enfrentar a fraude organizada depende da promoção da cooperação com empresas do setor privado, que individual e coletivamente governam os domínios digitais que oferecem um terreno fértil para atividades fraudulentas.

A capacidade de intermediários do setor privado para agir contra fraudadores organizados varia de acordo com suas funções e com o grau de proximidade de sua relação comercial com aqueles que utilizam seus serviços para fins criminosos. Sob os princípios estratégicos de promoção da cooperação e parcerias em uma abordagem de "toda a sociedade" para o enfrentamento do crime organizado, os intermediários do setor privado podem desempenhar uma série de papéis essenciais,[321] tais como:

- Identificação de atores e atividades criminosas suspeitas, notificando as autoridades ou as vítimas potenciais (incluindo denúncias internas de fraude);
- Prevenção de comunicações fraudulentas, impedindo que estas cheguem às vítimas por meio da remoção ou bloqueio de sites maliciosos, anúncios ou perfis falsos;
- Fornecimento de dados desagregados por gênero, aprimorando o quadro estratégico de inteligência e facilitando investigações criminais;
- Prevenção da perda de fundos, bloqueando ou revertendo transferências financeiras destinadas a infratores;
- Educação dos usuários sobre fraudes, aumentando a conscientização de maneira acessível e adaptada a diferentes grupos-alvo;
- Desenvolvimento de sistemas e políticas que minimizem e mitiguem os riscos de fraude.

Nos casos em que a fraude representa uma ameaça para um setor ou empresa, as estratégias podem ser orientadas por necessidades e objetivos internos.[322] Em algumas situações, os sistemas de diferentes setores ou empresas podem servir como vetores para fraudes que impactam atores externos, como membros do público ou outros setores. Por exemplo, o uso de telecomunicações para enviar mensagens fraudulentas é um tipo de fraude que afeta vítimas individuais e prestadores de serviços financeiros que processam pagamentos ou solicitações de transferência.

Adotar uma perspectiva estratégica em diversos setores facilita a identificação de vulnerabilidades sistêmicas na infraestrutura tecnológica, comercial ou financeira. Uma abordagem consiste em considerar estrategicamente as principais etapas na perpetração de determinados tipos de fraude e identificar as convergências com tecnologias, produtos e serviços, incluindo, por exemplo, o canal de entrada para o primeiro contato com as vítimas (como anúncios em redes sociais), a interação com as vítimas (como mensagens falsificadas) e os processos de conversão dos lucros ilícitos (como sistemas de pagamento).

A coordenação precisa ser realizada de uma forma que leve em conta a gama de indústrias e organizações que compõem essa infraestrutura, incluindo corporações globais e pequenas empresas, empresas situadas dentro do país e aquelas que operam fora da jurisdição legal, bem como empresas com diferentes recursos e capacidades para auxiliar no trabalho de combate à fraude.[323] Existem vários meios de incorporar o setor privado a uma abordagem coordenada, incluindo o fomento de parcerias

321 UNODC, “Organized crime strategy toolkit”.
322 For example, the Southern African Fraud Prevention Service facilitates the sharing of information among member companies to identify and address internal risks of fraud (see www.safps.org.za/Home/About).
323 See, for example, Michael Levi and Matthew Leighton Williams, “Multi-agency partnerships in cybercrime reduction: mapping the UK information assurance network cooperation space”, Information Management and Computer Security, vol. 21, No. 5 (November 2013).

estratégicas entre o Estado, o setor privado e organizações da sociedade civil,[324] bem como o estabelecimento e a adoção de padrões ou princípios voluntários para orientar políticas e práticas mais consistentes através de empresas e o estabelecimento de regulamentações estatutárias para impor obrigações a partes interessadas-chave no setor privado.[325]

É importante esmiuçar os principais estágios da fraude para ajudar a identificar os pontos estratégicos para direcionar a atividade de prevenção ao crime. Há vários exemplos em que parcerias público-privadas foram cultivadas para implementar estratégias para prevenir a vulnerabilidade sistêmica. Os estudos de caso definidos abaixo representam iniciativas para lidar com cada um dos estágios da fraude descritos acima.

ESTUDO DE CASO: RESPOSTA INTERSETORIAL ASITES MALICIOSOS

O National Cyber Security Centre no Reino Unido da Grã-Bretanha e Irlanda do Norte tem acordos com provedores de serviços de Internet no Reino Unido para compartilhar informações em tempo real sobre sites que foram identificados como fraudulentos. Os provedores podem então bloquear o acesso aos sites fraudulentos e impedir que os fraudadores associados se comuniquem com possíveis vítimas no Reino Unido.

Fonte: Reino Unido, National Cyber Security Centre, "NCSC se une à indústria para oferecer proteção sem precedentes ao público contra golpes", 11 de maio de 2022.

ESTUDO DE CASO: RESPOSTA INTERSETORIAL À COMUNICAÇÃO EM MASSA VIA MENSAGEM DE TEXTO

Em uma tentativa de conter o alto volume de *smishing* que explora as telecomunicações para personificar organizações legítimas, a Autoridade Australiana de Comunicações e Mídia introduziu um registro de remetentes de mensagens de texto. O sistema incentiva a participação de partes interessadas importantes da indústria para estabelecer um diretório de remetentes confiáveis, a fim de restringir a capacidade dos criminosos de enviar mensagens de texto em massa que personificam (ou falsificam) essas organizações. Isso serviria para filtrar mensagens maliciosas que pretendem representar essas organizações e, assim, impedi-las de atingir possíveis vítimas.

Fonte: Parlamento da Austrália, "Telecommunications Amendment (SMS Sender ID Register) Bill 2024", disponível em www.aph.gov.au/.

324 See, for example, United Kingdom, Home Office "Joint fraud taskforce", 17 October 2017.
325 Por exemplo, o Regulamento de Serviços Digitais da União Europeia introduzirá novas obrigações para marketplaces online rastrearem os vendedores em suas plataformas, a fim de ajudar a perseguir fraudadores de maneira mais eficaz. Veja: 325 Por exemplo, a Lei dos Serviços Digitais da União Europeia introduzirá novas obrigações para os mercados online rastrearem os fornecedores em sua plataforma para ajudar a perseguir fraudadores de forma mais eficaz. Veja https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348..

ESTUDO DE CASO: HUB INTERSETORIAL PARA PREVENIR A PERDA DE DINHEIRO PARA FRAUDE

Em Singapura, o Anti-Scam Command é uma unidade policial centralizada que estabeleceu parcerias estreitas com uma variedade de provedores de serviços financeiros, alguns dos quais estão co-localizados com a unidade policial. As partes interessadas incluem bancos locais e estrangeiros, grupos de segurança de cartões, empresas de fintech e casas de criptomoeda. Essa abordagem integrada permite o compartilhamento rápido de informações e a análise de inteligência financeira para identificar e bloquear transferências financeiras suspeitas de serem fraudulentas. Pagamentos online e transferências bancárias permitem que os fraudadores movam rapidamente e convertem os fundos roubados, e o objetivo dessa colaboração é congelar contas de forma ágil, recuperar fundos e, assim, reduzir as perdas para as vítimas.

Fonte: Força Policial de Singapura, "Abertura do escritório de comando anti-fraude", 6de setembro de 2022.

Respostas eficazes à fraude também precisam levar em conta o cenário regulatório para controlar a provisão de produtos e serviços. A acessibilidade desses produtos e serviços fornece o disfarce para ocultar esquemas fraudulentos e enganar as vítimas. A regulamentação tem um papel fundamental na implementação de mecanismos eficazes de confiança para prevenir a atuação de atores maliciosos dentro de setores legítimos. Isso inclui reguladores do setor público e privado adotando princípios robustos de "conheça seu cliente" ao abrir contas bancárias, solicitar o uso de outros serviços habilitadores, como serviços de pagamento, telecomunicações e outros serviços empresariais (por exemplo, aluguel de escritórios) e registrar empresas ou profissionais (por exemplo, profissionais de serviços financeiros).

Os crimes abrangidos pela fraude organizada atravessam fronteiras nacionais, setores e grupos demográficos. Isso cria complexidades no desenvolvimento de políticas e na entrega de respostas eficazes. Existem etapas fundamentais que cada Estado pode adotar, primeiramente para entender como a fraude organizada se manifesta e impacta dentro de suas fronteiras e, em segundo lugar, para projetar e implementar respostas estratégicas eficazes nos quatro pilares para combater o crime organizado (prevenir, perseguir, proteger e promover). A formulação de políticas também deve levar em consideração o contexto transnacional da fraude organizada para garantir a entrega de respostas internacionais coordenadas. Além disso, a fraude organizada exige uma resposta de toda a sociedade que incorpore parcerias estratégicas com partes interessadas não governamentais, particularmente no setor privado, para produzir uma compreensão mais aprofundada do problema e criar estratégias contra ele.

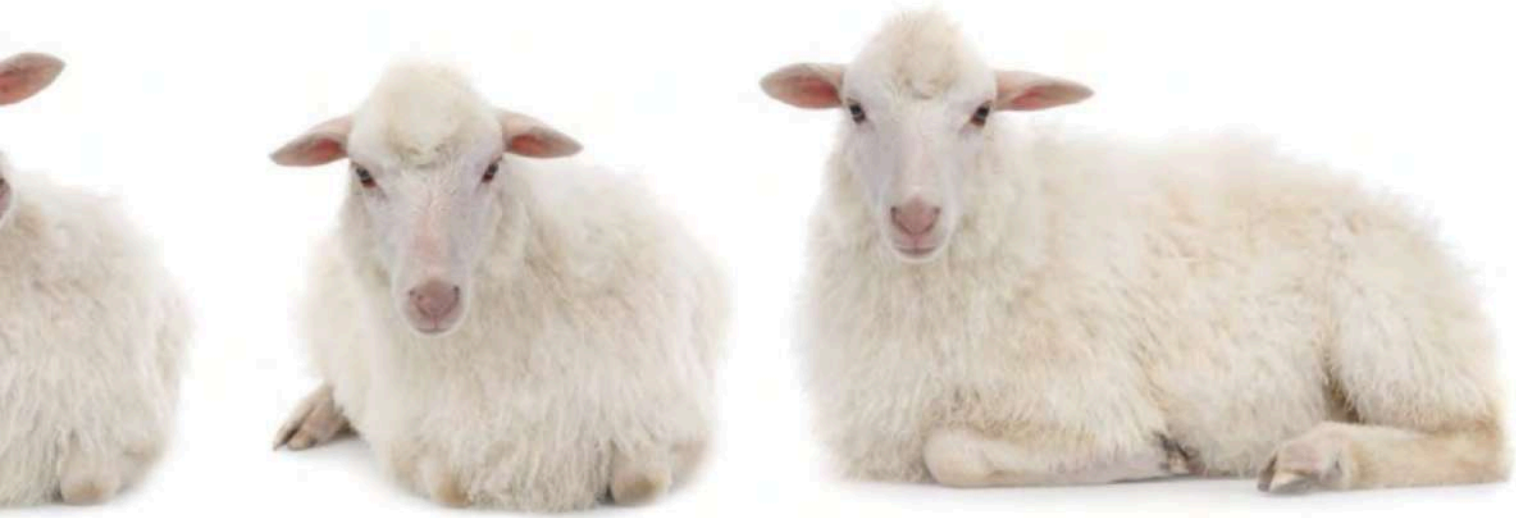
Conclusão

A fraude organizada representa uma ameaça multifacetada e generalizada que transcende fronteiras, indústrias e demografia. Abordar essa questão complexa exige uma abordagem abrangente, começando com o desenvolvimento de uma linguagem comum e uma compreensão das diferentes categorias de fraude organizada.

O presente documento tem como objetivo contribuir para a área acadêmica, fornecendo uma visão geral da fraude organizada que visa membros individuais do público ou instituições privadas com o propósito de obter um benefício financeiro ou outro material. As categorias de fraude desenvolvidas aqui adotam uma perspectiva centrada na vítima e, portanto, têm um foco primário na narrativa ou engano apresentado às vítimas. Embora seja abrangente, o documento não é exaustivo, e ainda existem uma infinidade de questões relevantes para a fraude organizada. Mais pesquisas de acadêmicos, profissionais e da sociedade civil são necessárias para desenvolver nosso conhecimento e compreensão de uma área do crime altamente diversificada e complexa.

As categorias de fraude organizada apresentadas no documento têm o objetivo de fornecer aos stakeholders uma melhor compreensão da questão, com vistas a fomentar estratégias eficazes de múltiplos stakeholders para prevenir a fraude organizada, perseguir grupos criminosos organizados, proteger as pessoas afetadas pela fraude organizada e promover parcerias e cooperação, além de salvaguardar as vítimas e aumentar a resiliência social contra essa ameaça persistente. A colaboração entre setores, a inovação contínua e o compromisso inabalável com a justiça e os direitos humanos são essenciais para mitigar o impacto da fraude organizada e promover um ambiente global mais seguro e protegido.

No entanto, muito ainda precisa ser feito. O documento sobre fraude organizada é uma parte de um projeto mais amplo que desenvolverá ferramentas e pesquisas adicionais para prevenir e combater a fraude organizada, incluindo medidas para fortalecer a legislação, aumentar a conscientização pública e defesas, e promover uma cooperação eficaz com os setores privado e outros, para citar apenas alguns. Ao continuar avançando na compreensão e nas capacidades de resposta, podem ser feitos progressos significativos na proteção de indivíduos e instituições contra a ameaça generalizada da fraude organizada.



UNODC
Escritório das Nações Unidas
sobre Drogas e Crime

Centro Internacional de Viena, Caixa Postal 500, 1400 Viena, Áustria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 263-3389, www.unodc.org

2412213