KPMG

Pesquisa Global sobre Fraude Bancária

A ameaça multifacetada da fraude: Os bancos estão prontos para enfrentar este desafio?

Maio 2019

Ser especialista transforma negócios.

kpmg.com.br

Índice

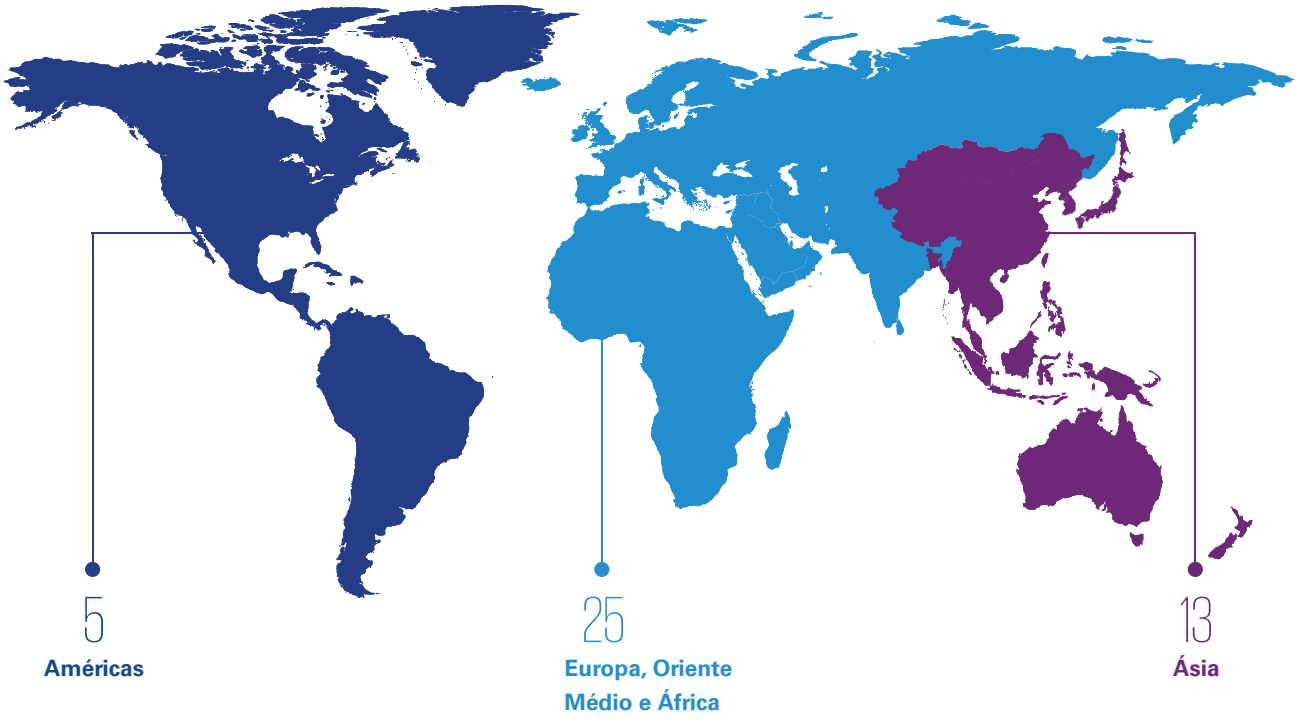
Prefácio

A KPMG tem o prazer de compartilhar o resultado da nossa Pesquisa Global sobre Fraude Bancária. A Pesquisa foi realizada para obter uma perspectiva global de como os bancos estão lidando com ameaças de fraudes internas e externas.

A Pesquisa questionou profissionais das áreas de risco de fraude bancária, investigações e profissionais de segurança sobre tendências em tipologias de fraude, desafios enfrentados pelos bancos na mitigação de ameaças internas e externas no período de 2016 a 2018, segurança na era digital e como os bancos estão estruturando suas equipes e implantando recursos para otimizar seus esforços no gerenciamento de risco de fraude.

A Pesquisa Global de Bancos da KPMG foi realizada entre novembro de 2018 e fevereiro de 2019 em 43 bancos de varejo, 13 dos quais estão localizados na Ásia-Pacífica, 5 na América e 25 na região da Europa, do Oriente Médio e da África (EMEA). Um total de 18 bancos têm faturamento anual superior a US$ 10 bilhões e 31 empregam mais de 10.000 pessoas em todo o mundo.

Gostaríamos de agradecer aos entrevistados por dedicarem tempo para participar da pesquisa. Temos o prazer de compartilhar os resultados, acompanhados de percepções globais e regionais dos profissionais da firma-membro da KPMG.



Fonte: Pesquisa Global sobre Fraude Bancária, KPMG International 2019

> *"Nossa pesquisa identificou que o custo com a fraude está aumentando em um ritmo mais rápido do que os investimentos para o gerenciamento de riscos de fraude. Repensar esta questão é extremamente importante."*

David Hicks
Global Forensic Leader
KPMG International

Principais resultados

— Mais da metade dos entrevistados da pesquisa sofreu aumentos no valor total e no volume total de fraudes externas. O aumento das tipologias de fraude em todo o mundo, de 2015 a 2018, inclui roubo de identidade e de aquisição de contas, ataques cibernéticos, fraude sem cartão e golpes de pagamentos autorizados. Neste relatório, nos referimos a esses pagamentos, autorizados pelo cliente, como golpes.

— A maior parte dos entrevistados afirmou globalmente que o custo total, o custo médio e o volume de fraudes internas de funcionários detectados permaneceram iguais ou diminuíram. Isto pode, no entanto, não apresentar uma imagem real do custo da fraude interna. Muitas fraudes externas se originam de alguém que trabalha dentro do banco.

— Mais da metade dos entrevistados recuperou menos de 25% das perdas por fraude, demonstrando que a prevenção de fraudes é fundamental. Os bancos estão investindo em novas tecnologias, incluindo alertas de fraude em tempo real com base em aprendizagem de máquina *(machine learning)*, reconhecimento de voz, facial e de impressões digitais (biometria) e perfis de como os clientes interagem com seus dispositivos e serviços bancários pela Internet (biometria comportamental) na prevenção de fraudes.

— Em todas as regiões, os bancos pesquisados consideraram os ataques cibernéticos como o desafio mais significativo no risco de fraude. Os fraudadores estão obtendo dados do cliente por meio de hackers, em tentativas de engenharia social, na *dark web* e em redes criminosas após vazamentos de dados, fora do controle dos bancos. Em última análise, no entanto, os clientes consideram que é responsabilidade dos bancos impedir fraudes de engenharia social em sua conta. Exemplos de tais métodos de engenharia social são apresentados no Anexo 1.

— A pesquisa apresenta que, globalmente, os bancos estão vendo uma tendência crescente nas fraudes. Exemplos de tipos de golpes são apresentados no Anexo 2. Os fraudadores estão manipulando e coagindo os clientes a fazerem pagamentos a eles, evitando os controles bancários. O Reino Unido introduziu um *Código Modelo para Reembolso Contingencial de Golpes de Pagamento Autorizado* para reembolsar clientes em determinadas circunstâncias; e para os reguladores e o governo fornecerem uma solução sustentável para as vítimas dos golpes.

— Os clientes são fundamentais no processo de prevenção e detecção de atividades fraudulentas em suas contas, particularmente para reduzir as perdas por golpes, mas deve ser feito um trabalho educacional sobre fraudes e golpes para os clientes.

— O Open Banking é considerado um grande desafio para o gerenciamento do risco de fraude nos bancos, e os bancos ao redor do mundo estão se preparando para abrir suas portas para terceiros acessarem os dados de seus clientes. Perguntas estão sendo feitas sobre a confiança que pode ser colocada em controles de terceiros. O Open Banking também representa uma oportunidade para se obter uma base de dados de clientes enriquecida, que pode ser usada para prevenir e detectar atividades fraudulentas e recuperar perdas por fraude.

< 25% Mais da metade dos entrevistados recuperou menos de um quarto das perdas por fraude.

> 50% Mais da metade dos entrevistados globalmente teve um aumento no valor da fraude

> 60% Mais de 60% dos entrevistados tiveram um aumento no volume de fraudes global

Tipologias

- Transações sem a apresentação do cartão físico
- Engenharia social
- Golpes
- Fraude virtual

Segurança no Mundo Digital

- Aumento de produtos entregues via canais digitais
- Regras, aprendizagem de máquina, inteligência artificial e robótica
- Alto volume de falsos positivos

Investimento *versus* Custos

- Modelos operacionais complexos
- Processos não ágeis
- Educação do Cliente
- "Aqui e agora", em oposição às tendências emergentes

Modelo Operacional da Fraude

- Ausência de Modelo Operacional de Prevenção à Fraude e de Avaliação do Risco de Fraude
- Falhas na mensuração do impacto no gerenciamento das informações e nas decisões de investimento
- Otimização da tecnologia versus quantidade de mão de obra
- Operações financeiras criminosas em massa

> *"No contexto de um cenário bancário global em mutação, no qual a demanda por serviços bancários com atendimento presencial está diminuindo, os volumes de pagamentos digitais estão aumentando e os pagamentos estão sendo processados em segundos, os fraudadores estão criando novas maneiras de roubar os bancos e seus clientes. Os bancos precisam ser ágeis para responder a novas ameaças e adotar novas abordagens e tecnologias para prever e prevenir fraudes."*

Natalie Faulkner,
Global Fraud Lead,
KPMG International

Temas da pesquisa

Tendências da fraude

Fraude externa

A pesquisa demonstrou que, em 2018, 61% dos entrevistados indicaram que o volume total de fraude externa tem aumentado e 59% disseram que o valor tem aumentado.

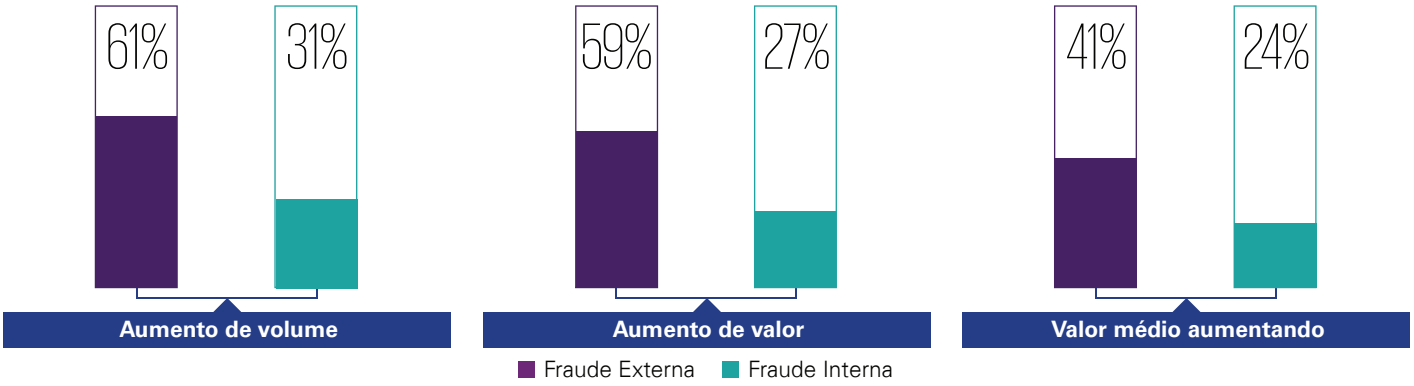
Na maioria dos casos, os entrevistados informaram que, aparentemente, o valor médio de cada fraude permaneceu o mesmo (21%) ou diminuiu (38%). Isso provavelmente deve-se ao alto volume e baixo valor das fraudes com cartões. O aumento das tipologias de fraudes externas em todo o mundo, de 2015 a 2018, inclui roubo de identidade e aquisição de contas, ataques cibernéticos, fraude sem a apresentação do cartão físico e golpes.

Fraude interna (funcionário)

Ao contrário da fraude externa, a maioria dos entrevistados afirmou que, globalmente, o custo total, o custo médio e o volume de fraudes internas permaneceram iguais ou diminuíram em 2017 e 2018. Isso, no entanto, pode não apresentar um quadro completo da ameaça interna a uma instituição financeira, visto que em nossa experiência muitos incidentes de fraude externa se originam de agentes criminosos experientes, que trabalham com fontes internas que possuem um conhecimento detalhado dos sistemas, dos processos e dos controles bancários (e quaisquer falhas ou pontos fracos de controle).

O potencial dano da fraude interna pode ser tão grande quanto, se não maior do que, a fraude externa, dada a capacidade dos funcionários de explorar os pontos fracos nos controles para atingir os ativos mais valiosos de um banco. Os bancos devem continuar a adotar uma abordagem proativa para detectar fraudes internas.

Essas estatísticas são baseadas em fraudes detectadas pelos bancos. Em nossa experiência, a detecção de fraudes está se tornando cada vez mais sofisticada, no entanto haverá sempre um elemento de fraude desconhecido, ainda a ser detectado.



Fonte: Pesquisa Global sobre Fraude Bancária, KPMG International 2019

Recuperações de perda por fraude

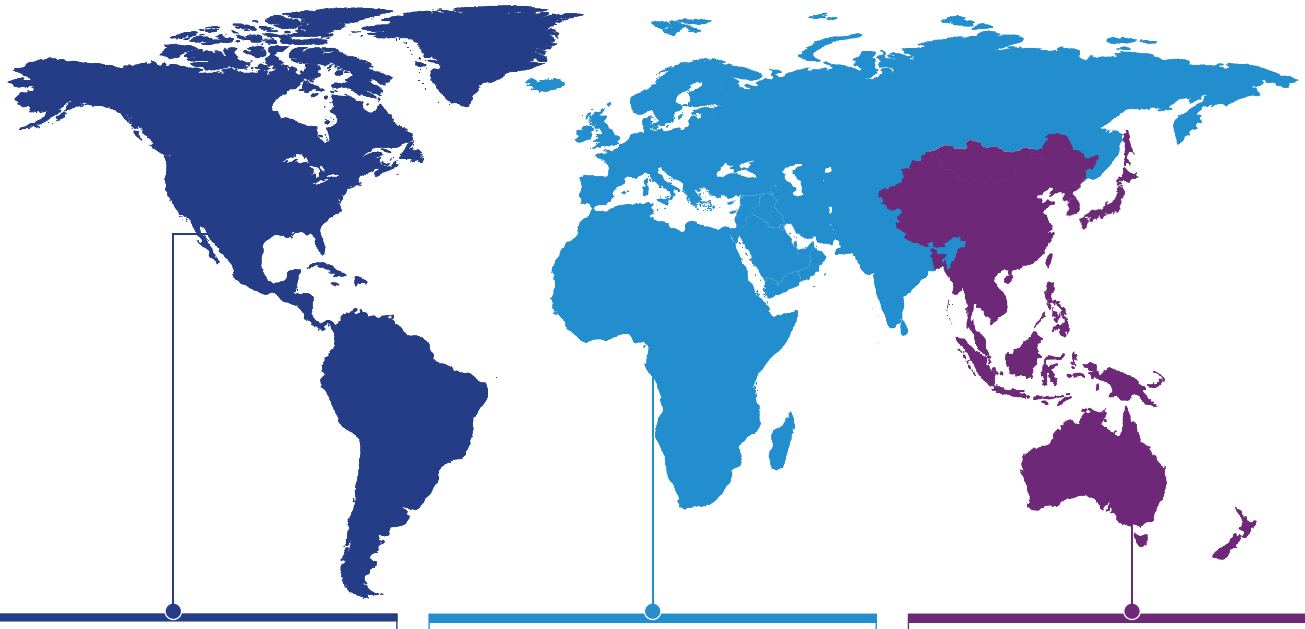
Mais da metade dos entrevistados declarou que a recuperação de fraudes era inferior a 25% do valor desviado. Este baixo índice demonstra a importância dos esforços na previsão e na prevenção de fraudes.

Pesquisa das tendências de tipologias de fraude por região 2017-2018 com base nas respostas em comum

Tipologia de Fraude	Américas	EMEA	Ásia-Pacífica
Golpes	▲ Aumentado	▲ Aumentado	▲ Aumentado
Transações sem a apresentação do cartão físico	▲ Aumentado	▲ Aumentado	▲ Aumentado
Fraude cibernética/*on-line*	▲ Aumentado	▲ Aumentado	▲ Aumentado
Fraude de identidade/falsidade ideológica/ estelionato	▲ Aumentado	▲ Aumentado	▲ Aumentado
Fraude interna	▲ Aumentado	▲ Aumentado	● Permaneceu igual
Roubo de dados	▲ Aumentado	● Permaneceu igual	▲ Aumentado
Fraude em hipoteca	● Permaneceu igual	▲ Aumentado	▲ Aumentado
Fraude empresarial/comercial	● Permaneceu igual	● Permaneceu igual	● Permaneceu igual
Fraude nas demonstrações financeiras	● Permaneceu igual	● Permaneceu igual	● Permaneceu igual
Negociação desonesta	● Permaneceu igual	● Permaneceu igual	● Permaneceu igual

Desafios enfrentados pelos bancos hoje

A pesquisa apresentou uma questão sobre quais são os desafios mais significativos enfrentados hoje pelas instituições financeiras em termos de risco de fraude. De uma lista de sete opções[1]; as 5 principais respostas por região são representadas no gráfico a seguir.



Américas

1. Ataque cibernético e violação de dados
2. Pagamentos instantâneos/pagamentos *on-line*
3. Open Banking
4. Canais digitais
5. Moedas virtuais/moedas criptográficas

EMEA

1. Ataque cibernético e violação de dados
2. Pagamentos instantâneos/pagamentos *on-line*
3. Canais digitais
4. Segunda Diretiva de Serviços de Pagamento (PSD2)/Open Banking
5. Engenharia social

Ásia-Pacífico

1. Ataque cibernético e violação de dados
2. Engenharia social
3. Pagamentos instantâneos/pagamentos *on-line*
4. Canais digitais
5. Open Banking

Fonte: Pesquisa Global sobre Fraude Bancária, KPMG International 2019

Analisamos esses desafios em mais detalhes abaixo.

“O risco de fraude cibernética é o desafio mais significativo enfrentado pelas instituições financeiras em todas as três regiões. Os cinco principais riscos de fraude nas três regiões estão relacionados à transformação digital pela qual o mundo está passando. As instituições financeiras precisam de uma mudança de paradigma em sua abordagem para mitigar os riscos de fraude no futuro. Fundamentalmente, as instituições financeiras precisam entender a transformação digital que está acontecendo rapidamente ao nosso redor, absorver os riscos de fraude decorrentes dessa mudança rápida e projetar uma estrutura de gerenciamento de riscos de fraude que seja capaz de mitigar esses riscos de fraude de forma sustentável, eficaz e eficiente. Eu não acho que as soluções existentes dentro das instituições financeiras, embora seja impreterível se manter, sejam capazes de lidar com os crescentes riscos de fraude, em decorrência de serem muito fragmentados e simplistas. A nova geração de gerenciamento de riscos de fraude deve ser capaz de lidar com a transformação digital em constante evolução, identificar os riscos de fraude desconhecidos, aproveitar os benefícios da tecnologia e reduzir o custo de estar em conformidade.”

Lem Chin Kok
Forensic Lead, Asia Pacific,
KPMG em Cingapura

1. Ataque cibernético e violação de dados

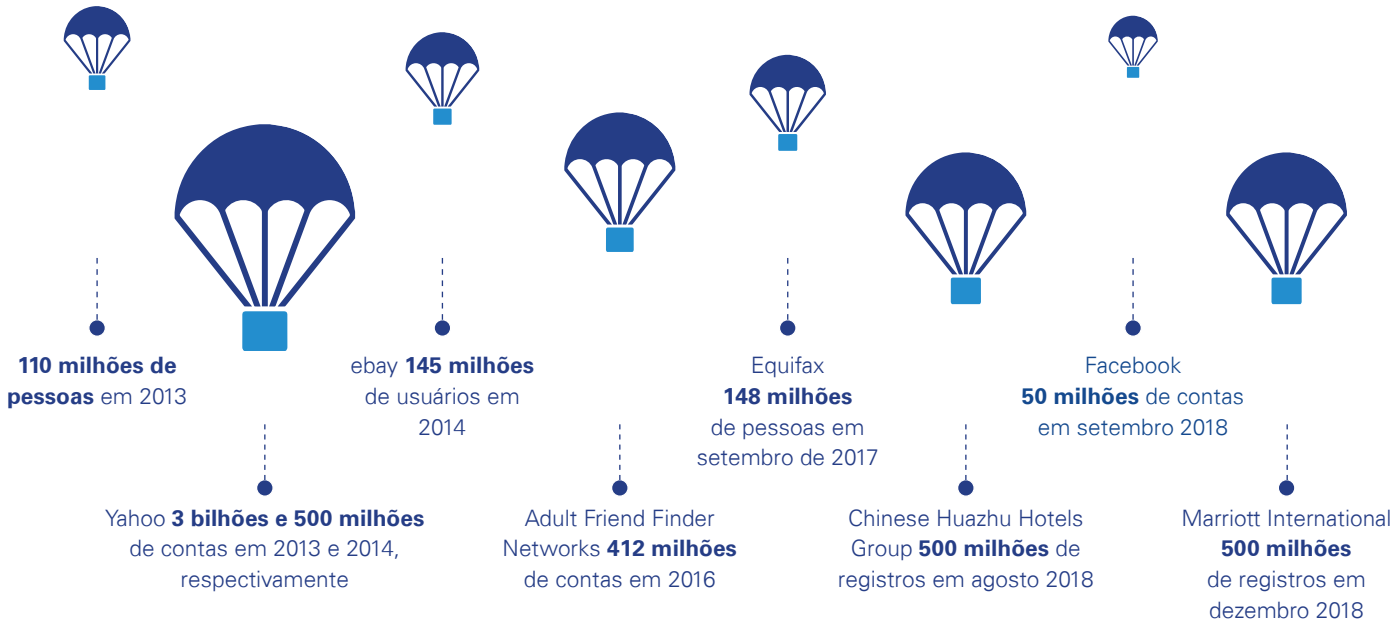
Os entrevistados ao redor do mundo consideram os ataques cibernéticos e a violação de dados como o desafio mais significativo que enfrentam. Nos últimos anos, ocorreram inúmeros vazamentos de dados de alto perfil relatados na imprensa, cujos números são apresentados na representação abaixo.

Em um mundo interconectado, enquanto um vazamento de dados pode estar relacionado a uma empresa, ou a um país, os dados mantidos frequentemente se referem a indivíduos ao redor do mundo. Por meio dessas violações de dados, os criminosos cibernéticos podem se apossar de grandes quantidades de informações, que podem ser usadas para facilitar o roubo de identidade, fraude de engenharia social e para golpes de pagamentos instantâneos, do tipo *push* autorizados, em que dados pessoais são usados para conquistar a confiança de um cliente ou facilitar a aquisição das contas de clientes.

Como exemplo, em 2018, uma grande companhia aérea sofreu uma violação de dados em que hackers obtiveram mais de 244.000 dados de cartões de crédito. Os hackers cobraram entre US$ 9 e US$ 50 pelas informações de cada cartão na Dark Web, resultando em receitas estimadas de US$ 12,2 milhões[2].

"Nomes, endereços de e-mail, senhas, números de seguridade social, datas de nascimento, números de cartão de crédito, dados bancários, números de passaporte, números de telefone, endereços residenciais, carteiras de motorista, registros médicos - todos esses dados foram obtidos por hackers amorfos e sombrios por fraude, para roubo de identidade"[3]

Dados/registros de clientes em domínio público[4]



> *"Como este relatório demonstra, a transformação digital em curso do setor bancário está certamente criando novos riscos de fraude. Mas também está gerando novas soluções e oportunidades incríveis para os encarregados de proteger os clientes e ativos do banco. Dada a relação entre tecnologia e risco de fraude, os bancos podem querer priorizar prevenção de fraudes e gestão de crimes financeiros dentro de suas estratégias digitais."*
>
> ***Judd Caplain***
> *Global Head of Banking and Capital Markets, KPMG International*

2. Engenharia social: Um holofote sobre as fraudes

A engenharia social foi citada como um dos 5 principais desafios para os bancos da EMEA e da Ásia-Pacífico que participaram das pesquisas.

Engenharia social pode resultar em:

Acesso não autorizado a contas bancárias de clientes, pelo qual os fraudadores obtêm informações pessoais dos clientes que são usadas para acessar suas contas bancárias (tomada de posse de conta). Exemplos de alguns dos métodos que os fraudadores empregam para obter informações sobre os clientes estão descritos no Apêndice 1.

Pagamentos autorizados em que um cliente é coagido a transferir seu dinheiro para uma conta controlada pelo fraudador, sob o pretexto de que ele seja um beneficiário legítimo (também conhecido como golpes, fraude eletrônica, pagamentos instantâneos do tipo *push* autorizados. Neste relatório, nos referimos a esses pagamentos autorizados

Os entrevistados relataram um aumento nos golpes em cada região global em 2018. Dos velhos golpes do "Príncipe da Nigéria", novos truques de personificação estão sendo empregados por fraudadores, incluindo golpes de relacionamento, agência governamental/imposto, aplicações financeiras, loteria, compromisso de e-mail comercial, suporte de tecnologia/acesso remoto[7] e golpes com avós, para citar alguns. Todos esses golpes têm o mesmo objetivo de obter acesso aos dados da vítima, que são então usados pelos fraudadores para apropriar-se indevidamente dos recursos da vítima ou persuadi-la a efetuar um pagamento para uma conta controlada pelo fraudador. Exemplos de tais golpes são apresentados no Apêndice 2.

Perdas com fraudes estão crescendo exponencialmente.

Em 2018, o Federal Bureau of Investigation (FBI) dos Estados Unidos informou que os golpes de compromisso de e-mail comercial resultaram em perdas globais de mais de US$ 12 bilhões entre 2013 e 2018[5]

Na Austrália, a Australian Competition and Consumer Commission (ACCC) informou que quase meio bilhão de dólares australianos foram perdidos para golpistas em 2018[6].

É provável que essa seja apenas a ponta do iceberg, que nem todos os consumidores saibam ou relatem que foram enganados.

As vítimas de golpes variam. Embora os idosos sejam um grupo demográfico de risco considerável, os golpes também afetam:

- Clientes que são socialmente isolados e solitários, como os golpes de relacionamento
- Financeiramente vulneráveis, como golpes de empréstimos mediante o pagamento de taxas antecipadas para a obtenção do empréstimo, golpes de cobrança de dívidas e golpes de aplicações financeiras "bons demais para serem verdadeiros"
- Empresas em que um membro da equipe financeira recebe um e-mail alegando ser do diretor executivo ou diretor financeiro (CEO/CFO), exigindo uma transferência de fundos, enquanto estes estão ausentes em licença/férias
- Jovens, com golpes de emprego, férias e loteria.

Os bancos costumam ser culpados por falharem na prevenção e na detecção das fraudes. Do ponto de vista de um banco, a dificuldade em detectar fraudes é que o cliente está acessando a própria conta, portanto os controles de acesso não detectam as fraudes. Muitos bancos agora têm uma equipe dedicada a fraudes para lidar com esse risco crescente.

Quando as fraudes são detectadas pelos bancos antes do processamento do pagamento, os bancos tem se deparado com clientes que estão convencidos da legitimidade da transação e que ainda podem ser inflexíveis em querer que o pagamento seja processado, apesar de o banco informar que o beneficiário da transação é uma fraude.

Na maioria dos países, não existe uma estrutura clara de responsabilidade que dita quem arca com o custo das fraudes, com alguns bancos julgando a perda como sendo do cliente, enquanto outros bancos avaliam golpes caso a caso antes de determinar se o banco compensará o cliente pelo seu prejuízo.

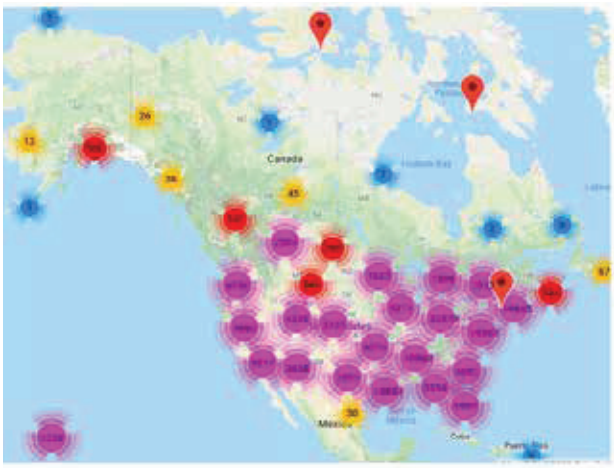
Mesmo quando o banco não está assumindo a responsabilidade pelos golpes, estamos vendo essa forma de fraude ocupar um tempo significativo do funcionário, em uma situação emocionalmente carregada, quando os clientes percebem que perderam somas significativas.

Nos casos em que o banco está arcando com o passivo, as perdas médias dos golpes são significativamente mais altas do que fraudes de cartão.

O Reino Unido introduziu um *Código Modelo para Reembolso Contingencial de Golpes de* Pagamento Instantâneo Tipo *Push* Autorizado (Código), para reembolsar as vítimas de golpes em qualquer caso em que o banco ou o prestador de serviços de pagamento é considerado culpado e o cliente atendeu aos padrões esperados dele sob o Código[7]. O Código é voluntário e foi desenvolvido em um esforço para proteger os clientes, e para que reguladores e o governo proporcionem uma solução sustentável. Os bancos que assinaram o Código ainda não foram anunciados, embora um grande banco de varejo tenha anunciado que irá reembolsar seus clientes por todos os golpes, incluindo a fraude de pagamento tipo *push*[8]. Será interessante ver se mais países introduzem estruturas semelhantes para os bancos.

O gráfico a seguir exibe os volumes de golpes relatados por vítimas e potenciais vítimas nos EUA e no Canadá de 1° de julho de 2015 a 22 de abril de 2019.

152.595 Golpes Encontrados



Fonte[9] acessada em 22 de abril de 2019

3. Evolução dos canais digitais e processamento de pagamentos instantâneos e/ou pagamentos *on-line*: A mudança para o banco digital com menos "tempo de contato presencial" com o cliente

A evolução dos canais digitais foi citada como um dos três principais desafios pelos entrevistados da pesquisa nas Américas e na região EMEA.

A proporção de produtos e serviços fornecidos pelos bancos por meio de canais digitais está aumentando. O *World Payments Report 2018* prevê que as transações não monetárias (em espécie) crescerão em 12,7% até 2021[10].

Dos entrevistados da pesquisa, 78% disseram que mais de um quarto de seus produtos e serviços é fornecido por meio de canais digitais. Em muitos mercados, estamos vendo o surgimento de novos e desafiantes bancos digitais, que entregam seus produtos exclusivamente por meio de canais digitais.

Com menos clientes mantendo e sacando dinheiro, devido à facilidade dos serviços bancários digitais e pagamentos sem dinheiro em espécie, a demanda dos clientes por serviços bancários presenciais está diminuindo. Isso está levando a uma tendência global de fechamento de agências bancárias.

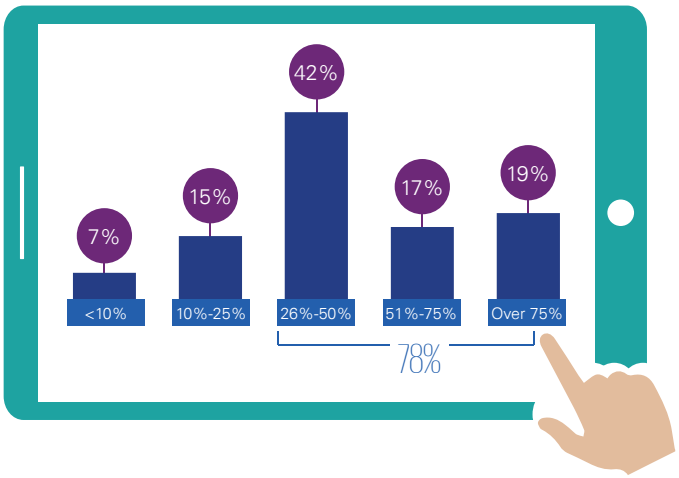
O Reino Unido fechou dois terços das agências bancárias nos últimos 30 anos[11], quase 6.000 agências fecharam na Europa[12] e nos EUA quase 9.000 agências foram fechadas nesta década[13].

Além disso, o processamento de pagamentos mais rápido pode representar um desafio, com menos tempo disponível para os bancos examinarem as transações à procura de fraude. Pagamentos mais rápidos também reduzem as taxas de recuperação de perdas por fraude devido à velocidade dos pagamentos, se os fundos forem transferidos por meio de diversas contas em segundos e no exterior.

Com os bancos sempre sensíveis ao equilíbrio entre mitigação do risco de fraude e experiência do cliente, conforme visto na pesquisa, os bancos estão respondendo por meio de ferramentas de prevenção e detecção de fraudes em tempo real, impondo limites e elaborando meios de autenticação para transações de alto risco, em um esforço para mitigar risco de aumento de fraudes em um ambiente de pagamentos em tempo real.

A autenticação de nomes também é fundamental, particularmente para pagamentos tipo *pull*, em que fraudadores podem se apresentar como uma empresa de serviços públicos ou de telecomunicações, por exemplo, para solicitar pagamento. O Reino Unido respondeu a esse risco com a confirmação de beneficiário quando os clientes solicitam transferências de fundos.

Que proporção de seus produtos/serviços são entregues via canais digitais?



Fonte: Pesquisa Global sobre Fraude Bancária, KPMG International 2019

− Menos agências reduzem a interação presencial entre bancos e seus clientes, o que está sendo explorado por criminosos organizados e fraudadores para cometer fraudes além das fronteiras, cometendo *hacking* e *phishing* para obter informações de identidade do cliente e, assim, facilitar a aquisição de contas de clientes.

\+ Mais transações digitais fornecem um rico conjunto de dados de comportamento digital do cliente, facilitando a identificação de pagamentos potencialmente fraudulentos.

> *"Atualmente, há muita dispersão e fragmentação em sistemas de prevenção de fraudes dentro de uma única entidade. As entidades financeiras devem evoluir para modelos de gestão de fraudes mais centralizados e transversais, com o objetivo de identificar sinergias e melhorar a eficiência."*

Enric Olcina
Forensic Lead, Europa, Oriente Médio e África, KPMG na Espanha

Os bancos estão investindo em tecnologia para melhor detectar fraudes - então, por que as perdas por fraude estão aumentando? Consideramos os desafios enfrentados pelos bancos na mitigação de fraudes e como os bancos estão estruturando suas funções de fraude para responder a essa crescente ameaça que se apresenta.

4. Open Banking

O Open Banking foi citado como um dos 5 principais desafios enfrentados pelos bancos em todas as regiões. O Open Banking representa uma mudança radical na forma como as instituições financeiras operarão em todo o mundo, transferindo a propriedade das informações da conta dos bancos e das instituições financeiras para seus clientes.

Os clientes poderão compartilhar suas informações e dados de transações com terceiros [como outros bancos, aplicativos de orçamentos *(apps), fintechs*, empresas de telefonia e plataformas de investimento], por meio da Interface de Programação de Aplicativos — Application Programming Interfaces (APIs).

Os reguladores estão cada vez mais encorajando e, em alguns países, obrigando o setor bancário a oferecer aos clientes acesso a serviços bancários abertos, por meio do desenvolvimento de APIs.

O Open Banking provavelmente impactará o gerenciamento de riscos de fraude de várias maneiras para as instituições financeiras:

- Como em todas as reformas que resultam em transações bancárias mais rápidas e mais convenientes para os consumidores, é provável que uma proporção maior de pagamentos seja feita por meio de canais digitais, resultando em maiores volumes de transações em que os bancos analisam a atividade da conta à procura de fraude.
- Com o Open Banking, os bancos contarão com a segurança de terceiros para proteger as informações bancárias dos clientes acessadas por meio de APIs. Se esses terceiros não fornecerem proteção adequada contra fraudes, os clientes provavelmente considerarão o banco, e não os aplicativos, culpados.
- O acesso aberto a informações bancárias em instituições financeiras fornecerá, aos fraudadores que obtiverem acesso, a capacidade de coletar dados de clientes mais confidenciais, apresentando uma visão mais holística das contas de um cliente para atingir contas de saldo positivo mais alto nos bancos.
- Por outro lado, para os bancos, essa maior transparência das contas de seus clientes nos bancos provavelmente permitirá uma verificação de identidade mais robusta, a identificação antecipada de contas falsas/fraudulentas e um rastreamento mais eficiente de fundos fraudulentos.

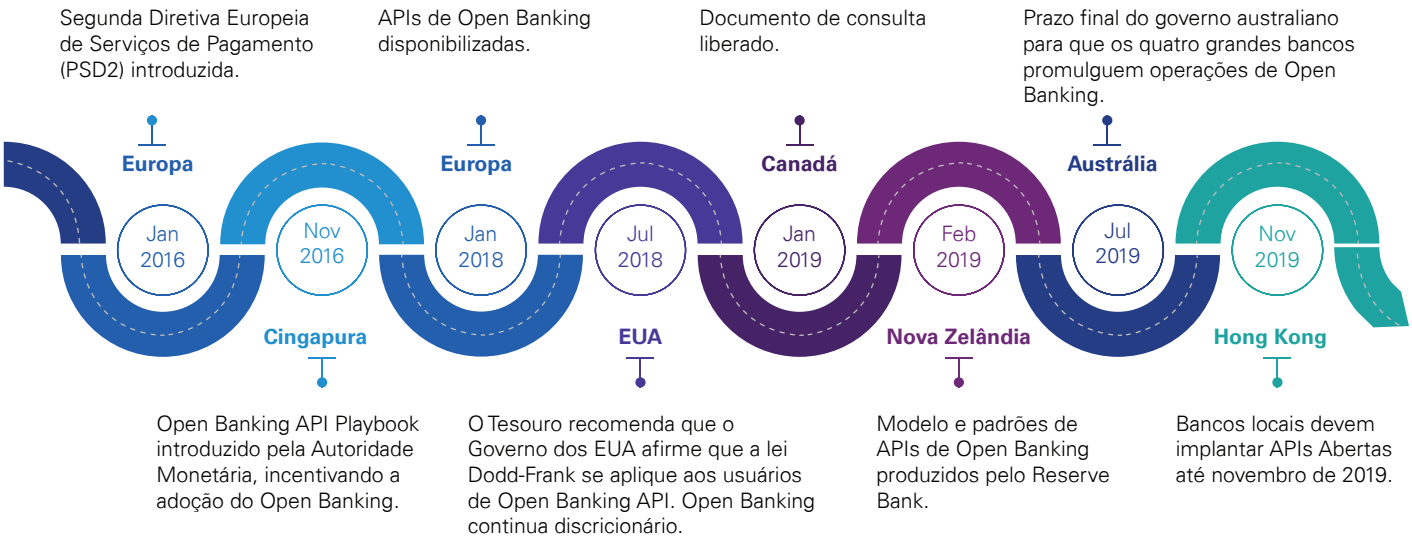
Como os bancos devem se preparar?

Segurança de dados – Os registros bancários incluem informações sensíveis e confidenciais de clientes e exigem os mais rigorosos padrões de segurança de dados. Os bancos devem garantir que as APIs incluam controles de segurança de dados robustos e que os desenvolvedores de terceiros sejam examinados antes de receber acesso, bem como antes de serem credenciados como prestadores de serviços.

Identidade digital – O Open Banking depende muito de uma identidade digital integrada em sua fundação. A consolidação do perfil *on-line* holístico para uma pessoa, organização ou dispositivo eletrônico permitirá uma experiência de autenticação segura e fluída.

Gerenciamento de acesso – Os bancos precisarão da capacidade de vincular um cliente, com segurança e confidencialidade, aos seus dados. Isso exigirá uma estrutura que rege direitos de acesso (e revogação), limitações de uso e segurança. Assim como o uso de uma conta de mídia social, para fazer *login* em uma conta bancária, os clientes exigem um conjunto padronizado ou personalizável de protocolos de gerenciamento de acesso, definidos para o compartilhamento e uso de dados com provedores de serviços de terceiros.

Um resumo da história do Open Banking em todo o mundo

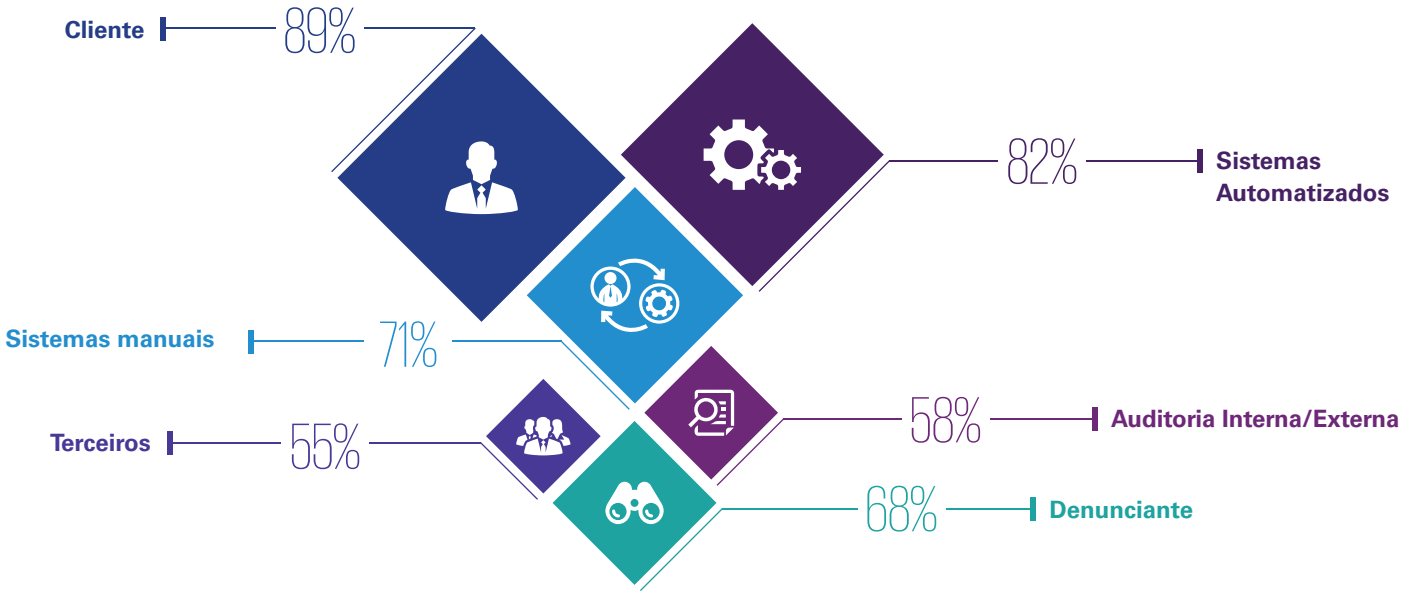


Neste ambiente desafiador, pode-se fazer mais para educar os clientes

Os clientes desempenham um papel fundamental na prevenção e na detecção de fraudes, particularmente no que diz respeito a golpes em que os clientes estão facilitando o pagamento. Na pesquisa, a maioria dos entrevistados apontou os clientes como uma fonte de detecção de atividade fraudulenta identificada em 2018.

Dada essa descoberta, aliada à baixa taxa de recuperação de fraudes identificada na pesquisa, com mais da metade dos entrevistados declarando que recuperações representam menos de 25% das perdas por fraude, os bancos podem fazer mais para educar seus clientes a fim de prevenir e detectar fraudes.

Como os bancos identificam atividades fraudulentas?



Fonte: Pesquisa Global sobre Fraude Bancária, KPMG International 2019

Os fraudadores estão se tornando cada vez mais sofisticados. Para armar os clientes com as habilidades necessárias para evitar ser vítima de fraude, os bancos devem educar os clientes para:

- Consultar regularmente a movimentação de sua conta;
- Reverter imagens de busca no Google usadas em golpes de relacionamentos;
- Aprender a identificar e-mails, mensagens de texto/SMS e telefonemas de *phishing*;
- Alterar as senhas com frequência;
- Ignorar *pop-ups*;
- Reconhecer *e-mails* de *spam* por meio de erros de ortografia, falta de informações seguras sobre o *site, links* duvidosos para cliques e endereços de *e-mail* que diferem da organização que em tese seria a autora do *e-mail*;
- Se não tiver certeza, pergunte a um amigo ou membro da família;
- Lembrar que uma organização genuína nunca pedirá senhas ou ficará preocupada se você solicitar o término de uma ligação e o retorno em um número de seus registros;
- Estar ciente do *spoofing* de identificação de chamadas, em que os fraudadores imitam o número de telefone da instituição que eles estão fingindo ser. A falsificação *(spoofing)* de identificação de chamadas tem sido usada, por exemplo, para parecer um número de telefone de amigos ou familiares da vítima, pelo qual os fraudadores fingem estar no local de um acidente e seu parente/amigo será deixado para morrer se não transferir dinheiro imediatamente para o chamador[14].
- Lembre-se que, se a oferta for boa demais para ser verdade, geralmente é;

Além disso, a educação do cliente deve alavancar canais digitais e não digitais para cuidar de clientes idosos e vulneráveis, que geralmente são menos experientes em tecnologia.

O modelo operacional de fraude

Quanto custa o gerenciamento de riscos de fraudes para você e quão eficaz é?

A pesquisa fez perguntas para entender como os bancos estruturam suas operações de gerenciamento de riscos de fraude para otimizar alocação de recursos e para informar a tomada de decisões de investimento em sua governança, pessoas, processos e tecnologia.

Apesar de ser um centro de custos, o custo total do gerenciamento de riscos de fraude para os bancos não é monitorado em 52% dos bancos pesquisados. Isso faz com que seja um *outlier* dentro das operações bancárias e reduz a visibilidade para a Diretoria e os Comitês de Risco que tomam decisões importantes sobre orçamento, recursos e investimentos.

Em termos de responsabilização pela eficácia de funções antifraude, houve uma diversidade de respostas no que diz respeito à responsabilização do proprietário do risco de fraude por efetivamente prevenir, detectar e responder a suspeitas de fraude; e recuperação de perdas por fraude. As respostas variaram de nenhuma avaliação formal a *scorecards*/principais indicadores de desempenho, manutenção das perdas previstas em planejamento/apetite por risco, satisfação do negócio/cliente, compras misteriosas e garantia de segunda linha.

Houve uma diversidade nas respostas a como as instituições financeiras estruturam globalmente seus modelos operacionais de gerenciamento de riscos de fraude.

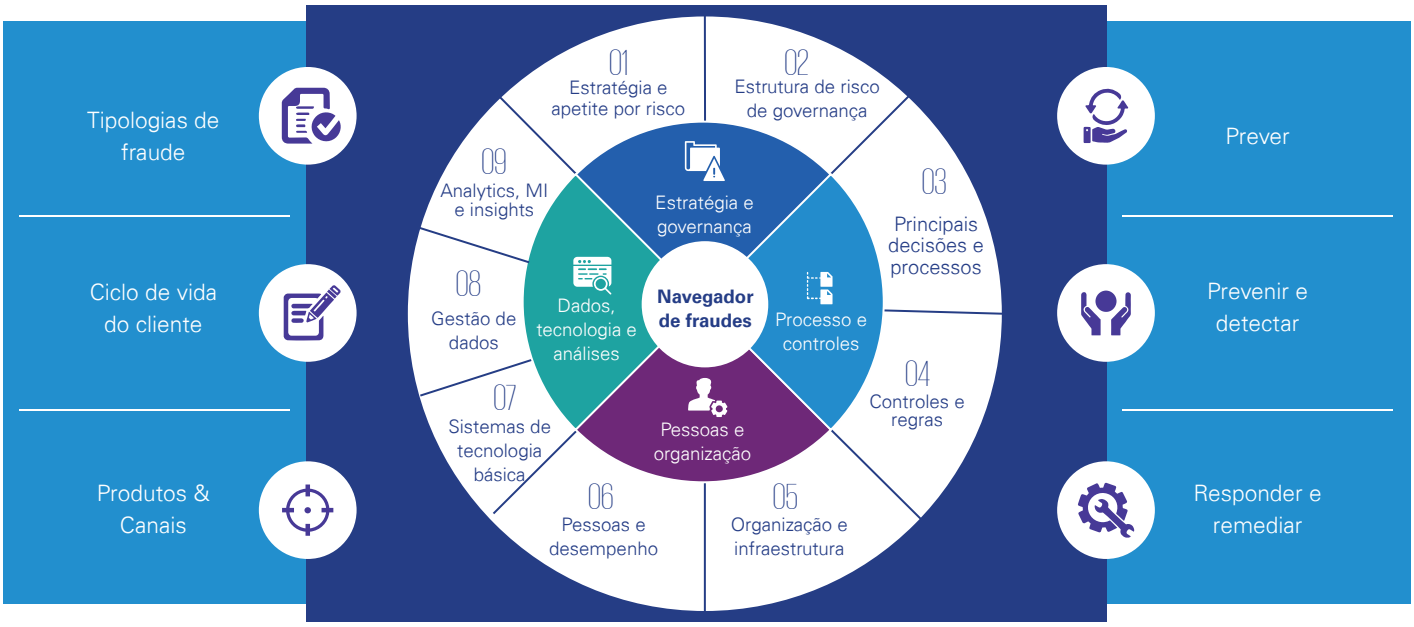
Fonte: Pesquisa Global sobre Fraude Bancária, KPMG International 2019

> *"À medida que os fraudadores e os riscos de fraude se tornam mais sofisticados decorrentes da mudança para canais e ferramentas digitais, os Reguladores esperam cada vez mais que as instituições financeiras obtenham mais consistência e integração da Primeira e da Segunda linhas de defesa em sua abordagem de prevenção, detecção e resposta a riscos de fraudes."*

Thomas Stanton
Fraud Lead, Américas, KPMG nos EUA

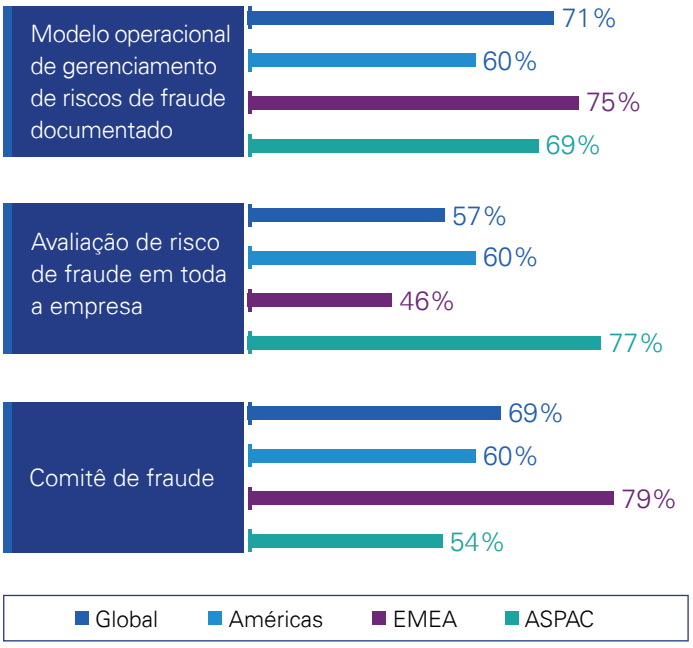
Navegador de Fraudes da KPMG

Um modelo operacional de gerenciamento de riscos de fraude bem estruturado e uma avaliação de risco em toda a empresa são importantes para garantir que as defesas dos bancos sejam robustas para mitigar consistentemente o risco de fraude interna e externa dentro do apetite por risco de fraude do banco.



Fonte: KPMG Fraud navigator 2019

A pesquisa constatou que nem todos os entrevistados têm um modelo operacional de gerenciamento de riscos de fraude documentado, conduzem uma avaliação de risco de fraude em toda a empresa e têm um comitê de fraude da seguinte forma:



Governança, Pessoas, Processo....

A pesquisa encontrou diferenças em como as instituições financeiras estruturam suas operações de gerenciamento de riscos de fraude, com o proprietário do risco de fraude designado encontrado:

- **69%** na primeira linha de defesa, administrada pelas unidades de negócio/funcionários focados nos clientes (Primeira Linha);
- **31%** na segunda linha de defesa, na função de segurança do grupo, proporcionando supervisão de risco e conformidade às unidades de negócios (Segunda Linha).

As linhas de relatório para o proprietário do risco de fraude variaram, sendo as denúncias feitas ao Comitê de Fraude, ao diretor de riscos, ao *head* de *compliance*, ao diretor jurídico e à Auditoria Interna.

Curiosamente, parece que não existe um modelo "certo" seguido pelos bancos globalmente para estruturar consistentemente suas operações de gerenciamento de riscos de fraude.

A pesquisa encontrou diferenças em quem define o apetite por risco de fraude do banco, com:

- ***52%** Diretoria/Comitê de Risco
- ***29%** Primeira linha
- ***5%** Segunda linha

...e Tecnologia

As instituições financeiras enfrentam um desafio significativo para superar as técnicas em constante mudança dos fraudadores. Os bancos estão cada vez mais buscando aprimorar os sistemas por meio do monitoramento de transações, possibilitado pela aprendizagem de máquina/inteligência artificial e gerenciamento de acesso biométrico. A maioria dos entrevistados da pesquisa investiu nos seguintes métodos para prever, prevenir e detectar tentativas de fraude:

- Autenticação de dois fatores ou multifatorial para verificar a identidade de um cliente, exigindo que os usuários forneçam algo que conhecem, por exemplo, uma senha, com outros fatores que eles têm, por exemplo, código de verificação de mensagem de texto/SMS ou impressão digital;
- 70% dos bancos pesquisados têm soluções de tecnologia capazes de pontuar riscos e tomar decisões em tempo real;
- 67% usam biometria física (reconhecimento de voz, impressão digital e facial). Observamos que agora existe um mercado de crimes cibernéticos para impressões digitais e casos de fraudadores que registram e replicam vozes de clientes usando tecnologia;[15]
- 63% usam uma combinação de regras e aprendizagem de máquina incorporadas em sua tecnologia para facilitar a detecção de fraudes.

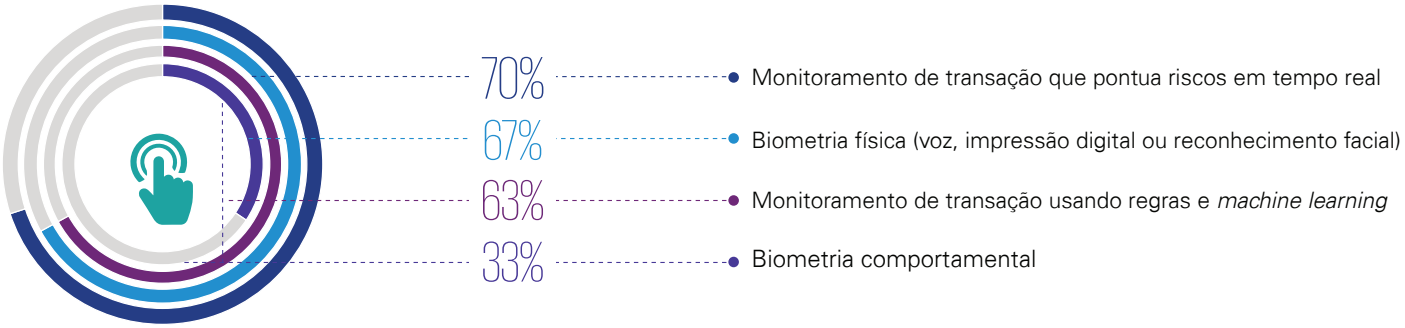
Os entrevistados relataram investimentos em biometria comportamental, tecnologia de revisão de mídia adversa, análise de rede e autenticação do Google.

Apesar dos avanços e dos investimentos em tecnologia, 51% dos bancos pesquisados relataram um número significativo de falsos positivos resultantes de suas soluções de tecnologia, prejudicando a eficiência na detecção de fraudes.

Sistemas ineficazes afetam as informações de gerenciamento de fraudes — os riscos dos bancos estão ocultos à vista de todos? Relatórios deficientes também podem afetar negativamente a capacidade de a Diretoria e o Comitê de Risco tomarem decisões apropriadas sobre investimentos e alocação de recursos, com o investimento em fraudes sendo considerado insuficiente para crimes financeiros na pesquisa.

Além disso, devido ao tamanho e à complexidade das operações e dos processos bancários, pode levar algum tempo para efetuar a mudança. Em contraste, os fraudadores podem ser ágeis em suas tentativas de fraude. Como as tipologias de fraude, como golpes e fraude de identidade/engenharia social para facilitar a tomada de conta, tornam-se cada vez mais predominantes e os criminosos organizados compartilham conhecimento dentro de suas redes nas jurisdições para superar os métodos de detecção de fraude bancária, os bancos reconhecem a necessidade de aprimorar continuamente seus esforços de gerenciamento de riscos de fraude para gerenciar esses riscos.

Proporção de entrevistados que investiram na seguinte tecnologia



Fonte: Pesquisa Global sobre Fraude Bancária, KPMG International 2019

Para continuar a aprimorar a detecção de fraudes, os entrevistados da pesquisa identificaram a necessidade de investir em novas tecnologias nos próximos três anos, incluindo:

- Tecnologia de monitoramento de transações com *machine learning*/inteligência artificial (IA)/robótica;
- Inovações em *software* Fintech/RegTech que automatiza a entrega de serviços financeiros, incluindo a automação de Know Your Customer (KYC);
- Biometria e um maior uso de dados de código aberto e mídia social.

Em conclusão, ainda há oportunidades de melhoria para os bancos otimizarem seu modelo operacional antifraude em governança, pessoas, processos e tecnologia, particularmente em torno de:

- Equilíbrio entre o número de funcionários e os aprimoramentos da tecnologia;
- Otimização da alocação de recursos por meio do planejamento de recursos, apesar da incerteza na hora de investigar;
- Aprimoramento de sistemas de detecção de fraudes, particularmente para reduzir falsos positivos nos sistemas, por meio de um *loop* de *feedback* para aprimorar algoritmos e conjuntos de regras.

Os bancos devem planejar além da tecnologia para alcançar resultados e desempenho ideal em seu modelo operacional antifraude em toda governança, pessoas, processos e tecnologia.

E quanto à fusão das funções de *compliance* anticrimes financeiros e antifraude?

As multas significativas que são cobradas globalmente por não reportar atividades suspeitas de lavagem de dinheiro ou deficiências associadas em termos de controle de crimes financeiro estão afetando as decisões de investimento dos bancos de elevar crime financeiro antes de fraude.

Os resultados da pesquisa revelam que mais de 50% dos entrevistados planejam investir mais em *compliance* anticrimes financeiros [Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo (AML CTF), Antissuborno e Corrupção (ABC) e triagem de Sanções] do que no gerenciamento de riscos de fraude.

Os resultados da pesquisa revelaram que 43% dos entrevistados tinham relatórios integrados, 40% tinham estruturas de governança integradas, 38% tinham sistemas integrados e 35% tinham equipes integradas entre *compliance* de anticrimes financeiros e antifraude.

Para 43% dos entrevistados, não havia integração entre *compliance* de anticrimes financeiros e antifraude.

A tabela abaixo apresenta considerações para um modelo individual versus modelo integrado para fraudes e crimes financeiros.

Razões percebidas para combinar Fraude com Crime Financeiro

Equipes Integradas de Fraude e Crimes Financeiros - Perspectiva de Pessoas e Processos

- As atividades associadas a Crime Financeiro, como Know Your Customer (KYC), e os relatórios de assuntos suspeitos também são relevantes para o risco de fraude. Como uma equipe com uma estratégia, é provável que haja mais integração para alavancar inteligência em relação ao mesmo ataque/incidente. Por exemplo, o produto do crime (fraude) que está sendo repassado por meio de contas falsas, o qual deve ser reportado ao regulador de Crimes Financeiros.
- A diversidade de funções e pensamentos da equipe é vista como um benefício em equipes integradas.
- Evita a duplicação de esforços ou falta de comunicações para incidentes que afetem tanto fraude quanto crime financeiro.
- Alavancar os benefícios do investimento significativo em crime financeiro para beneficiar também o gerenciamento de riscos de fraude e corrupção.

Equipes Integradas de Fraudes e Crimes Financeiros - Perspectiva tecnológica

- Alavancar bandeira vermelha/inteligência de alerta e perfil dinâmico de clientes entre fraude e crime financeiro.
- Economia de custos no uso da mesma plataforma de tecnologia, com diferentes módulos e interfaces de usuário.

Razões percebidas para individualizar/não combinar Fraude

Equipes Individualizadas de Fraude e Crimes Financeiros

- Provavelmente, o principal motivador das equipes individualizadas são os diferentes requisitos de relatórios regulamentares e, especificamente, as penalidades significativas por não notificação de suspeitas de crimes financeiros aos reguladores e multas por suborno/corrupção e prisão em alguns países, particularmente pela Securities and Exchange Commission (SEC) e pelo Departamento de Justiça (DoJ) dos EUA em nível mundial. Tais penalidades não são cobradas por não comunicação de fraude.
- Cultura legada/organizacional - "sempre fizemos assim".

Sistemas Individualizados de Fraude e Crimes Financeiros

- Capacidade de escolher um sistema de fraude "best in breed" e sistema de crimes financeiros, potencialmente com um terceiro sistema para identificar inteligência cruzada.
- Potencialmente, a falta de consciência em relação a soluções adequadas que podem gerenciar ambos os riscos.

Conclusão

No contexto de um cenário bancário global em mutação, no qual as redes de agências estão encolhendo, os volumes de pagamentos digitais estão aumentando e os pagamentos estão sendo processados em segundos, os fraudadores estão criando novas maneiras de roubar bancos e seus clientes.

Então, como os bancos devem responder?

Os resultados da nossa pesquisa mostram que os fraudadores estão mudando o foco das aquisições de contas para golpes em que os clientes são explorados como um elo fraco. Mais precisa ser feito pelos bancos para educar e proteger seus clientes.

Nossa pesquisa reforça que o dano potencial da fraude interna pode ser tão grande, se não maior, do que a fraude externa, dada a capacidade dos funcionários de explorar pontos fracos nos controles para atingir os ativos mais valiosos de um banco. Os bancos devem continuar a adotar uma abordagem proativa para detectar fraudes internas.

No contexto de mais países implementando o Open Banking, os bancos devem aprimorar sua capacidade de analisar *big data* em um ambiente de Open Banking e navegar pelas APIs.

Os métodos usados por fraudadores internos e externos continuam a evoluir. Há uma crescente necessidade de os bancos garantirem a eficiência e a eficácia operacional dos controles de fraudes digitais, alavancando análises avançadas de dados e perícia humana para prever, prevenir e detectar fraudes. Sistemas ineficazes afetam as informações de gerenciamento de fraudes — os riscos dos bancos estão ocultos à vista de todos? Relatórios deficientes também podem afetar negativamente a capacidade da Diretoria e do Comitê de Risco de tomar decisões apropriadas sobre investimentos e alocação de recursos, com o investimento em fraudes sendo considerado insuficiente para crimes financeiros na pesquisa.

Tecnologia apenas não é suficiente, com mais da metade dos nossos entrevistados globais relatando falsos positivos que prejudicam a eficiência na detecção de fraudes. Os bancos devem planejar além da tecnologia, para alcançar resultados e desempenho ideal em seu modelo operacional antifraude em toda governança, pessoas, processos e tecnologia.

Os fraudadores estão se tornando mais sofisticados e podem rapidamente mudar e adaptar suas abordagens. Os bancos precisam ser ágeis para responder a novas ameaças e adotar novas abordagens e tecnologias para prever e prevenir fraudes.

Apêndice 1

Exemplos de métodos de engenharia social

Phishing/Spoofing: Um ataque de *phishing* é quando um golpista envia um *e-mail* fingindo ser alguém que não é para obter informações pessoais da vítima. *Phishing* geralmente envolve um usuário clicando em um *link* e digitando sua senha, após isso o golpista terá informações suficientes para obter acesso à conta ou à caixa de e-mail da vítima. Em média, 4% dos alvos de qualquer campanha de phishing clicarão no link.

Spear Phishing: refere-se a tentativas de *phishing* em que o golpista usa informações de código-fonte aberto para criar *e-mails* altamente personalizados para incentivar ainda mais a vítima a clicar em um *link* em seu *e-mail*. Por exemplo, um golpista pode identificar por meio da mídia social que a vítima está esperando uma encomenda, e criará um *e-mail* de *phishing* que parece ser do serviço de entrega, com uma mensagem referente a essa encomenda com um *link* falso para rastrear a entrega.

Pretexting: é uma forma de engenharia social na qual o atacante fabrica um cenário, um pretexto convincente, para o motivo pelo qual eles exigem informações da vítima. Normalmente, os golpistas personificam pessoas em uma posição de autoridade, como autoridades fiscais ou um banco, e solicitam informações de seus alvos para confirmar sua identidade.

***Baiting*:** é um ataque de engenharia social projetado para manipular a vítima por meio de sua curiosidade. O golpista oferecerá à vítima algo de bom (como uma atualização de *software*, um prêmio ou deixar um USB em um local público para a vítima conectar ao computador), que, uma vez aberto pela vítima, fará com que o computador da vítima instale *software* malicioso.

***Quid Pro Quo*:** Esta é uma variante do *baiting*, pela qual o golpista prometerá um serviço ou benefício após a execução de uma ação específica. Por exemplo, um *hacker* pode se passar por um especialista em segurança de TI, oferecendo uma atualização de *software*, permitindo que a vítima desative seu *software* antivírus primeiro, instalando, assim, o *software* malicioso sem restrições no computador.

Apêndice 2

Tipologias de fraude

Perda média por tipo de fraude (valores em US$)	
Aplicações financeiras	$8,648
Catfish/ relacionamentos *on-line*	$6,003
Transações	$3,993
Criptomoeda*	$3,147
Reformas de residências	$2,895
Câmbio/golpe nigeriano ou da Nigéria	$2,133
E-mail de compromisso de negócios	$1,717
Emergências familiares ou com amigos	$1,219
Produto falsificado	$1,210
Viagem/férias	$887
Empréstimo com pagamento de taxa antecipada	$716
Caridade	$708
Fraude de identidade/ falsidade ideológica/ estelionato	$683
Aluguel	$662
Emprego	$598
Sorteio/loteria/prêmio	$547
Fatura falsa	$441
Perdão de dívida	$388
Compras *on-line*	$365
Cheque ou ordem de pagamento falsificados	$341
Suporte técnico	$255
Cartão de crédito	$231
Subsídio do governo (auxílio governamental)	$218
Assistência saúde/ assistência médica/ plano de saúde	$170
Bolsa de estudos	$155
Serviços públicos	$106
Cobrança de dívidas	$98
Listas telefônicas (páginas amarelas)	$91
Phishing	$44
Arrecadação de impostos	$31
Outros	$746

* Denota uma categoria rastreada pela primeira vez em 2018

Fonte: BBB Scam Tracker, 2015 a dezembro de 2018

As perdas médias nas Américas por tipologia de fraude.

Fraudes em aplicações financeiras: As fraudes relacionadas a investimentos apresentam à vítima uma oportunidade única, muitas vezes garantindo retornos elevados, caso invista seu dinheiro. As vítimas geralmente são contatadas por telefone ou e-mail por fraudadores que alegam oferecer aconselhamento genuíno sobre investimentos.

Fraudes de relacionamentos ou catfish: Os golpes de relacionamento tiram proveito de pessoas que procuram por um amor, criando perfis falsos em sites de namoro ou mídias sociais, os quais fingem ser um potencial parceiro romântico. Após um namoro on-line, muitas vezes demorado, o fraudador pedirá dinheiro, presentes ou informações pessoais. Os golpes costumam atuar nos gatilhos emocionais das vítimas, por exemplo, pedindo dinheiro para pagar as "contas médicas da família", ou para voos para que possam visitar a vítima. Os fraudadores também podem pedir fotos íntimas que usarão para chantagear a vítima.

Golpe nigeriano ou golpe do príncipe da Nigéria: O golpe do "Príncipe da Nigéria", um dos mais antigos golpes em execução, no qual a vítima é contatada por alguém que alega ser do exterior e que afirma ser muito rico e/ou da realeza, solicitando assistência para retirar dinheiro de seu país pela oportunidade de participação nos milhões de dólares, ainda é prevalente e eficaz. Solicitações são feitas para que a vítima pague impostos, subornos a funcionários do governo e taxas legais com a promessa de que todas as despesas serão reembolsadas quando os fundos estiverem fora do país. Já em posse do pagamento, ou dados bancários, o "Príncipe" desaparecerá, muitas vezes com o conteúdo da conta bancária da vítima.

Business E-mail Compromise (BEC): Uma forma comum de fraude por e-mail, o BEC tem como alvo indivíduos com acesso a instalações bancárias da empresa e usa engenharia social para induzi-los a fazer pagamentos aos fraudadores. Frequentemente, o fraudador fingirá ser o CEO da empresa, solicitando um pagamento urgente que contorne os controles usuais. O Internet Crime Complaints Center (IC3) do FBI publicou em junho de 2018 o BEC como um golpe de US$ 12 bilhões.

Emergências familiares ou com amigos: Frequentemente direcionado para idosos e com pouca audição, o fraudador fingirá ser o neto da vítima. O "neto" alegará estar com problemas, precisando de dinheiro (por exemplo, fingindo estar na cadeia, com problemas legais ou com dívidas). Muitas vezes, as vítimas são informadas de que são a única pessoa em quem o neto confia e que não devem contar a mais ninguém. Os golpistas usarão as informações das mídias sociais para tornar sua história mais crível e obscurecer suas vozes fingindo chorar.

Golpes de loteria: Golpistas de loteria contatam as vítimas informando que eles ganharam na loteria ou um sorteio que eles nunca haviam realmente entrado. As vítimas serão solicitadas a pagar uma taxa antecipada para liberar ou entregar seu presente ou dinheiro. Eles também podem ser solicitados a ligar para um número de telefone de altos encargos para reivindicar o prêmio. Frequentemente, os fraudadores usarão os nomes das competições reais para que, se a vítima pesquisar a fraude, ela pareça legítima.

Golpes de suporte técnico/acesso remoto: Os golpes de suporte técnico/ acesso remoto convencem a vítima de que há um problema no computador ou na Internet e que o novo software é necessário para corrigir o problema. A vítima receberá uma ligação, e-mail ou um pop-up de computador informando que há problemas com sua conexão de Internet, ou com o computador, e orientará a vítima a entrar em contato com o fraudador para corrigi-lo. Os golpistas podem citar problemas comuns, como velocidade da Internet, como evidência do problema. Em seguida, solicitarão que a vítima forneça acesso remoto a eles para "descobrir qual é o problema". Uma vez que o fraudador tenha acesso ao computador da vítima, ele coleta seus dados, acessa suas contas bancárias e, frequentemente, faz pagamentos para ele mesmo.

Golpes de agência governamental: Em fraudes de agências do governo, os fraudadores entram em contato com as vítimas por telefone, mensagem de texto ou e-mail fingindo ser de um órgão judiciário ou da administração fiscal. Em alguns casos, o fraudador pedirá um pagamento urgente para liquidar uma dívida, como multa de estacionamento vencida ou pagamento de impostos. O fraudador pode ameaçar, dizendo que o não pagamento resultará no aumento do pagamento ou em prisão.

Apêndice 3

Referências

Meta 2013: 110 milhões. Baseado no número citado no relatório de The Huffington Post, "Target Hacked: Retailer Confirms 'Unauthorised Access' Of Credit Card Data" (19 de dezembro de 2013). Disponível em https:// www.huffpost.com/entry/target-hacked-customer-credit-card- data-accessed_n_4471672

Yahoo 2013: 3 bilhões. Baseado no número citado no relatório de The New York Times, "All 3 Billion Yahoo Accounts Were Affected by 2013 Attach" (Nicole Perlroth, 3 de outubro de 2017). Disponível em: https://www. nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Yahoo 2014: 500 milhões. Baseado no número citado no relatório de The Washington Post, "Yahoo confirms data breach affecting at least 500 million accounts" (Hayley Tsukayama, Craig Timberg & Brian Fung, 22 de setembro de 2016). Disponível em: https://www. washingtonpost.com/news/ the-switch/wp/2016/09/22/report-yahoo- to-confirm-data-breach-affecting-hundreds-of-millions-of-accounts/

Ebay 2014: 145 milhões. Baseado no número citado no relatório de The Washington Post, "eBay asks 145 million users to change passwords after data breach" (Andrea Peterson, 21 de maio de 2014). Disponível em: https:// www.washingtonpost.com/news/the-switch/ wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords- after-data-breach/

Adult Friend Finder 2016: 412 milhões. Baseado no número citado no relatório de The Verge, "Over 300 million AdultFriendFinder accounts have been exposed in massive breach" (Andrew Liptak, 13 de novembro de 2016). Disponível em: https://www.theverge. com/2016/11/13/13615750/412-million-adultfriendfinder-accounts- exposed-breach

Equifax - setembro de 2017: 148 milhões de consumidores americanos. Baseado no número produzido pelo Comitê de Supervisão e Reforma do Governo da Câmara dos Deputados dos EUA, The Equifax Data Breach Report (dezembro de 2018) p2. Disponível em: https://oversight.house. gov/ wp-content/uploads/2018/12/Equifax-Report.pdf

Chinese Huazhu Hotels Group - agosto de 2018 : 500 milhões de registros. Baseado no número citado no relatório de China Daily, "Huazhu Hotels Group investigates alleged info leak" (29 de agosto Adata (incluindo nome e números de celulares), 130 milhões de registros de check-in (incluindo nome e endereço) e 240 milhões de registros de estadia em hotel (incluindo números de cartão de crédito e datas de entrada e saída).

Facebook - setembro de 2018: 50 milhões de contas. Baseado no número citado no relatório de The Guardian, "Facebook says nearly 50m users compromised in huge security breach" (Julia Carrie Wong, 29 de setembro de 2018). Disponível em: https://www.theguardian.com/technology/2018/ sep/28/facebook-50-million-user-accounts-security-berach

Marriott International de 2018: 500 milhões de registros. Baseado no número citado no relatório de The New York Times, "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing" (David E. Sanger et al, 11 de dezembro de 2018). Disponível em: https:// www.nytimes. com/2018/12/11/us/politics/trump-china-trade.html

O Daily Mail, "hackers russos fizeram £9.4m com a violação de dados da British Airways com os dados de cartão de crédito dos clientes colocados à venda por apenas £ 6.94, dizem especialistas" (Sami Quadri, 14 de novembro de 2018).

Os dados de cartão de crédito disponíveis para venda eram de clientes da Europa, do México, do Brasil e da China, incluindo outros.

Disponível em: https://www.dailymail.co.uk/news/article-6387001/ Russian-hackers-9-4m-British-Airways-data-breach.html

Wired, "The Wired Guide to Data Breaches" (Lily Hay Newman, 12 de julho de 2018). Disponível em: https://www.wired.com/story/wired-guide- to-data-breaches/

Anúncio de serviço público do FBI, "Business E-Mail Compromise: The 12 Billion Dollar Scam" (12 de julho de 2018). Relatório afirma que 78.617 incidentes de golpes de e-mails de negócios ocorreram entre outubro de 2013 e maio de 2018, resultando em perdas globais de US$ 12.536.948.299. Os golpes de e-mail de negócios são definidos como "quando um participante compromete contas de e-mail corporativo legítimas por meio de engenharia social ou técnicas de invasão de computador para realizar transferências não autorizadas de fundos". Disponível em: https://www.ic3. gov/media/2018/180712.aspx

Comissão Australiana de Concorrência e Defesa do Consumidor, Targeting Scams Report (maio de 2019). US$ 489 bilhões em perdas relatadas à ACCC de mais de 378.000 relatórios de fraude. Disponível em https://www. accc.gov.au/publications/targeting-scams-report-on-scam-activity/ targeting-scams-report-of-the-accc-on-scam-activity-2018

Grupo Diretor de Golpes de Pagamento Tipo Push Autorizado, Comunicado à imprensa de 28 de fevereiro de 2019 e cópia anexa do Código. O Código declara que o cliente não pode ser reembolsado se o cliente "ignorar advertências efetivas", "não realizou ações apropriadas" ou quando se comportou de maneira "comprovadamente negligente". O Código entra em vigor em 28 de maio de 2019, os signatários ainda não foram anunciados. Disponível em: https://appcrmsteeringgroup.uk/app-scams-steering-g

1 Pagamentos mais rápidos, Violações cibernéticas e de dados, Diretiva de Serviços de Pagamento Open Banking, Moedas virtuais, Evolução de canais digitais, Engenharia social, Uso criminoso de inteligência artificial.

2 The Daily Mail, "hackers russos fizeram £ 9,4 m com a violação de dados da British Airways com os dados de cartão de crédito dos clientes colocados à venda por apenas £ 6,94, dizem especialistas" (Sami Quadri, 14 de novembro de 2018). Os dados de cartão de crédito disponíveis para venda eram de clientes da Europa, do México, do Brasil e da China, incluindo outros. Disponível em: https://www.dailymail.co.uk/news/article-6387001/ Russian-hackers-9-4m-British-Airways-data-breach.html

3 Wired, "The Wired Guide to Data Breaches" (Lily Hay Newman, 12 de julho de 2018). Disponível em: https://www.wired.com/story/wired-guide- to-data-breaches/

4 Meta 2013: 110 milhões. Baseado no número citado no relatório de The Huffington Post, "Target Hacked: Retailer Confirms 'Unauthorised Access' Of Credit Card Data" (19 de dezembro de 2013). Disponível em https://www.huffpost.com/entry/target-hacked-customer-credit-card- data-accessed_n_4471672

Yahoo 2013: 3 bilhões. Baseado no número citado no relatório de The New York Times, "All 3 Billion Yahoo Accounts Were Affected by 2013 Attach" (Nicole Perlroth, 3 de outubro de 2017). Disponível em: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Yahoo 2014: 500 milhões. Baseado no número citado no relatório de The Washington Post, "Yahoo confirms data breach affecting at least 500 million accounts" (Hayley Tsukayama, Craig Timberg & Brian Fung, 22 de setembro de 2016). Disponível em: https://www. washingtonpost.com/news/the-switch/wp/2016/09/22/report-yahoo- to-confirm-data-breach-affecting-hundreds-of-millions-of-accounts/

Ebay 2014: 145 milhões. Baseado no número citado no relatório de The Washington Post, "eBay asks 145 million users to change passwords after data breach" (Andrea Peterson, 21 de maio de 2014). Disponível em: https://www.washingtonpost.com/news/the-switch/ wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords- after-data-breach/

Adult Friend Finder 2016: 412 milhões. Baseado no número citado no relatório de The Verge, "Over 300 million AdultFriendFinder accounts have been exposed in massive breach" (Andrew Liptak, 13 de novembro de 2016). Disponível em: https://www.theverge. com/2016/11/13/13615750/412-million-adultfriendfinder-accounts- exposed-breach

Equifax - setembro de 2017: 148 milhões de consumidores americanos. Baseado no número produzido pelo Comitê de Supervisão e Reforma do Governo da Câmara dos Deputados dos EUA, The Equifax Data Breach Report (dezembro de 2018) p2. Disponível em: https://oversight.house. gov/wp-content/uploads/2018/12/Equifax-Report.pdf

Chinese Huazhu Hotels Group - agosto de 2018 : 500 milhões de registros. Baseado nos números citados no relatório do China Daily, "Huazhu Hotels Group investigates alleged info leak" (29 de agosto de 2018). Disponível em: https://www.chinadaily.com.cn/a/201808/29/WS5b86473da310add14f38871b.html. Acesso não autorizado a 123 milhões de dados de registros do Huazhu Hotels Group (incluindo nome e números de celulares), 130 milhões de registros de check-in (incluindo nome e endereço) e 240 milhões de registros de estadia em hotel (incluindo números de cartão de crédito e datas de entrada e saída).

Facebook - setembro de 2018: 50 milhões de contas. Baseado no número citado no relatório de The Guardian, "Facebook says nearly 50m users compromised in huge security breach" (Julia Carrie Wong, 29 de setembro de 2018). Disponível em: https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach

Marriott International de 2018: 500 milhões de registros. Baseado no número citado no relatório de The New York Times, "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing" (David E. Sanger et al, 11 de dezembro de 2018). Disponível em: https:// www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

5 Anúncio de serviço público do FBI, "Business E-Mail Compromise: The 12 Billion Dollar Scam" (12 de julho de 2018). Relatório afirma que 78.617 incidentes de golpes de e-mails de negócios ocorreram entre outubro de 2013 e maio de 2018, resultando em perdas globais de US$ 12.536.948.299. Os golpes de e-mail de negócios são definidos como "quando um participante compromete contas de e-mail corporativo legítimas por meio de engenharia social ou técnicas de invasão de computador para realizar transferências não autorizadas de fundos". Disponível em: https://www.ic3.gov/media/2018/180712.aspx.

6 Comissão Australiana de Concorrência e Defesa do Consumidor, Targeting Scams Report (maio de 2019). US$ 489 bilhões em perdas relatadas à ACCC de mais de 378.000 relatórios de fraude. Disponível em https://www. accc.gov.au/publications/targeting-scams-report-on-scam-activity/ targeting-scams-report-of-the-accc-on-scam-activity-2018.

7 Grupo Diretor de Golpes de Pagamento Tipo Push Autorizado, Comunicado à imprensa de 28 de fevereiro de 2019 e cópia anexa do Código. O Código declara que o cliente não pode ser reembolsado se o cliente "ignorar advertências efetivas", "não realizou ações apropriadas" ou quando se comportou de maneira "comprovadamente negligente". O Código entra em vigor em 28 de maio de 2019, os signatários ainda não foram anunciados. Disponível em: https://appcrmsteeringgroup.uk/app-scams-steering- group-agrees-voluntary-code/.

8 The Independent, "TSB torna-se o primeiro banco a oferecer 'garantia de reembolso' a todas as vítimas de fraude" (Ben Chapman, 16 de abril de 2019). Disponível em: https://www.independent.co.uk/news/business/news/tsb-bank-fraud-guarantee-refund-scams-a8870781.html

9 BBB Scam Tracker, reportando vítimas e potenciais vítimas dos EUA e do Canadá de 1º de julho de 2015 a 22 de abril de 2019. Disponível em: https://www.bbb.org/scamtracker/us/

10 Relatório de Pagamentos Mundiais de 2018, p6. Disponível em https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/ World-Payments-Report-2018.pdf

11 The Financial Times, "UK has lost two-thirds of bank branches in 30 years" (Emma Agyemang, 16 de novembro de 2018). Disponível em: https://www.msn.com/en-gb/money/news/uk-has-lost-two-thirds-of- bank-branches-in-30-years/ar-BBPL1Z7

12 The European Banking Federation, 2018 Facts & Figures (11 de setembro de 2018). Disponível em: https://www.ebf.eu/ebf-media- centre/banking-in-europe-ebf-publishes-2018-facts-figures/)

13 The Wall Street Journal, "Thousands of Bank Branches are Closing, Just Not at These Banks" (Allison Prang, 15 de junho de 2018). Disponível em: https://www.wsj.com/articles/the-bank-branch-is- dyingjust-not-at-these-banks-1529055000

14 CNBC.com, "You think it's your friend calling, but it's actually this growing phone scam" (Annie Nova, 12 de junho de 2018). Disponível em: https://www.cnbc.com/2018/06/12/you-think-its-your-friend-calling- but-its-actually-this-growing-phone-scam.html

15 https://www.zdnet.com/article/cybercrime-market-selling-full- digital-fingerprints-of-over-60000-users/

Fale com o nosso time

Emerson Melo
Sócio-líder de Forensic da KPMG no Brasil
Tel.: (11) 3940-4526
emersonmelo@kpmg.com.br

Rafael Weksler
Sócio-líder de Risk Advisory Solutions
da KPMG no Rio de Janeiro
Tel.: (21) 2207-9232
rweksler@kpmg.com.br

Alexandre Massao
Sócio de Forensic &
Litigation da KPMG no Brasil
Tel.: (11) 3940-6379
amhabe@kpmg.com.br

Carolina Paulino
Sócia de Forensic & Litigation
da KPMG no Brasil
Tel.: (11) 3940-4096
cpaulino@kpmg.com.br

Fernanda Flores
Sócia de Forensic & Litigation
da KPMG no Brasil
Tel.: (11) 3940-4891
fernandaflores@kpmg.com.br

Marcelo Gomes
Sócio de Forensic & Litigation
da KPMG no Brasil
Tel.: (11) 3940-4829
marceloagomes@kpmg.com.br

Raphael Soré
Sócio de Forensic & Litigation
da KPMG no Brasil
Tel.: (11) 3940-5958
rsore@kpmg.com.br

Marcelo Gomes
Sócio de Forensic & Litigation
da KPMG no Brasil
Tel.: (11) 3940-4829
marceloagomes@kpmg.com.br

Alexandre Martins
Sócio de Risk Advisory Solutions
da KPMG no Brasil
Tel.: (41) 3304-2737
amartins@kpmg.com.br

Patrícia Silva (MG)
Sócia-diretora de Risk Advisory Solutions
da KPMG no Brasil
Tel.: (31) 2128-5740
pssilva@kpmg.com.br

Alessandro Gratão
Sócio-diretor da área de Forensic Investigation
Discovery da KPMG no Brasil
Tel.: (11) 3940-5740
alessandrogratao@kpmg.com.br

Dino Almeida
Sócio-diretor de Forensic & Litigation
da KPMG no Brasil
Tel.: (11) 3940-4545
dinoalmeida@kpmg.com.br

Thais Silva
Sócia-diretora de Forensic & Litigation
da KPMG no Brasil
Tel.: (21) 2207-9237
thaisasilva@kpmg.com.br

#KPMGTransforma

Baixe o nosso APP

kpmg.com.br

/kpmgbrasil