

O documento de identidade virou um ativo de terceiro

Mais de 153 milhões de digitalizações de habilitação dos Estados Unidos e do Canadá foram colocadas à venda em um serviço de dark web. A empresa violada não era um banco, uma operadora nem um órgão público. Era o fornecedor contratado para conferir o documento.

Resumo executivo

Em 1º de setembro de 2026, o jornalista Brian Krebs revelou que um serviço de dark web chamado Nexus anunciava acesso a mais de 153 milhões de digitalizações de habilitação dos Estados Unidos e do Canadá, 10 milhões de carteiras de identidade, 3 milhões de documentos de viagem e 579 mil carteirinhas de saúde. A base foi associada à IDScan, empresa da Louisiana que processa verificação de documento para locadoras de veículo, varejo e dispensários de cannabis. A companhia publicou aviso em 4 de setembro confirmando acesso não autorizado à sua plataforma em nuvem, e em 10 de setembro confirmou publicamente o comprometimento de dados de clientes. O FBI apura o caso e ações coletivas já foram protocoladas.

Por que este caso merece uma análise

Vazamento de dado pessoal virou rotina, e rotina anestesia. Vale isolar o que distingue este caso de uma nota de rodapé.

Não foi uma lista de e-mail e senha. Foi a imagem do documento: nome completo, número da habilitação, data de nascimento, endereço, foto, validade e assinatura, tudo no mesmo arquivo, no formato legível que o próprio processo de verificação exige. Senha se troca. Documento de identidade, não.

E não foi uma empresa que guardava esse dado por descuido. Era uma empresa cuja função é exatamente essa. A digitalização estava lá porque o cliente dela contratou para que estivesse. A maior parte das pessoas no lote nunca ouviu falar da IDScan: elas alugaram um carro, compraram um produto de venda restrita, entraram em um estabelecimento regulado. O resto da cadeia aconteceu sem que soubessem que existia.

A anatomia do lote

Categoria	Volume anunciado	Por que importa
Habilitações (EUA e Canadá)	mais de 153 milhões	Documento com foto, endereço e número único. Base de abertura de conta em quase todo serviço financeiro digital.
Carteiras de identidade civil	10 milhões	Alcança quem não dirige, inclusive idosos e adolescentes, faixas com menos monitoramento de crédito.
Documentos de viagem	3 milhões	Passaporte sustenta fraude transfronteiriça e abertura de conta em jurisdição diferente da do titular.

Categoria	Volume anunciado	Por que importa
Carteirinhas de saúde	579 mil	Dado de saúde vinculado a documento. É a combinação que sustenta fraude de atendimento e de reembolso.

O valor do conjunto não é a soma das partes. Uma habilitação isolada vale pouco. Uma habilitação com a carteirinha de saúde da mesma pessoa vale muito mais, porque permite responder às perguntas de verificação que existem justamente para separar o titular do impostor.

O mesmo desenho existe no Brasil, com outro nome

É tentador ler um caso americano como problema americano. A infraestrutura de verificação de identidade brasileira tem a mesma forma: poucos fornecedores especializados atendendo muitos contratantes, com retenção de imagem por exigência regulatória ou por decisão de produto. Quem abre conta digital envia foto da CNH ou do RG e uma selfie. Quem contrata seguro, faz cadastro em marketplace ou aluga imóvel envia documento.

Some a isso duas particularidades locais. A primeira é o CPF, identificador único, vitalício e usado como chave primária em praticamente todo sistema do país. A segunda é o Pix, que tornou a transferência instantânea e, na prática, irreversível. Fraude de identidade em um ambiente assim tem janela de recuperação próxima de zero.

O que a LGPD cobra de quem contratou

A confusão mais comum em diálogo de comitê é achar que contratar um fornecedor transfere o risco junto com a atividade. Não transfere.

- **Art. 6º, VII — segurança.** O princípio obriga a adotar medidas técnicas e administrativas aptas a proteger o dado. O dever acompanha o dado, não o servidor onde ele está hospedado.
- **Art. 39 — instruções do controlador.** O operador trata conforme as instruções recebidas. Se o contrato não define prazo de retenção da imagem, não há instrução, e o fornecedor guarda pelo tempo que lhe convier.
- **Art. 42 — responsabilidade.** Controlador e operador respondem solidariamente pelo dano ao titular. A ação judicial chega a quem o titular conhece, que é a marca do balcão.
- **Art. 48 — comunicação.** Incidente com risco relevante vai à ANPD e ao titular. O prazo não para de correr porque a informação do fornecedor ainda não chegou.

A Resolução CD/ANPD nº 15/2024 fixou o prazo de três dias úteis para a comunicação à autoridade. Três dias úteis é pouco para descobrir, por meio de um fornecedor que talvez ainda esteja negando, quantos titulares seus estavam no lote.

Cinco perguntas para o próximo comitê

#	Pergunta	O que uma resposta ruim revela
1	Quais fornecedores retêm imagem de documento dos nossos clientes hoje?	Se a lista demora ou sai incompleta, não existe inventário de operadores, e o Art. 37 já está descumprido.

#	Pergunta	O que uma resposta ruim revela
2	Por quanto tempo cada um retém, e onde isso está escrito?	“Pelo prazo necessário” em contrato significa retenção indefinida na prática.
3	Eles subcontratam? Para quem?	Suboperador não declarado é a camada em que a cadeia deixa de ser auditável.
4	Em quanto tempo somos avisados de um incidente deles?	Sem prazo contratual, a descoberta chega pela imprensa, como neste caso.
5	Precisamos guardar a imagem, ou basta o resultado da verificação?	É a única pergunta que reduz o risco em vez de administrá-lo.

A quinta merece destaque, porque quase nunca é feita. Em uma parcela relevante dos casos, o contratante não precisa da imagem do documento. Precisa da afirmação de que a verificação ocorreu, com data, método e resultado. Guardar a imagem é conveniente para o dia em que alguém questionar o processo, e é exatamente esse conforto que transforma um requisito de conformidade em um passivo que cresce todo mês.

Leitura LATAMSEC

Há uma assimetria nesse mercado que nenhum contrato resolve sozinho. O fornecedor de verificação cobra por checagem, em centavos ou poucos reais. O passivo que ele acumula é proporcional ao volume de imagens retidas, que cresce sem limite. A receita é linear; o risco, cumulativo. Quando o incidente acontece, a diferença entre os dois não cabe no balanço dele e escorre para os contratantes.

A resposta madura não é trocar de fornecedor depois do vazamento. É mudar o que se pede a ele. Retenção mínima escrita em cláusula, com prazo em dias. Comprovação de descarte, com evidência auditável. Notificação em prazo contratual compatível com os três dias úteis da ANPD. E, quando o caso de uso permitir, atestado de verificação no lugar da imagem.

Essa conversa custa caro quando é puxada na renovação e custa pouco quando entra na próxima contratação. A diferença entre os dois momentos costuma ser um caso como este aparecendo no noticiário com o nome da sua empresa no lugar do fornecedor.

Fontes

- KrebsOnSecurity · *FBI Probes Service Selling 153M+ Drivers Licenses* (01/09/2026).
- TIME · *FBI Probes Report of Breach Exposing 153 Million Driver's License Scans* (03/09/2026).
- Cybernews · *153M driver's licenses for sale after alleged leak from IDScan*.
- ANPD · central de notícias e Resolução CD/ANPD nº 15/2024, sobre comunicação de incidente.