FinWise Bank alerta sobre violação de dados internos

Data: 2025-09-16 09:45:00

Autor: Inteligência Against Invaders

Uma fintech dos EUA notificou os clientes de que suas informações pessoais podem ter sido

comprometidas depois que um ex-funcionário as acessou.

O incidente no FinWise Bank ocorreu em 312024 de maio, mas não foi descoberto até mais de um ano depois, em 182025 de junho, de acordo com um documento do Gabinete do Procurador-Geral do Maine.

“A FinWise sofreu um incidente de segurança de dados envolvendo um ex-funcionário que acessou os dados da FinWise após o término de seu emprego”, diz a carta de notificação de violação.

“Alguns dos dados afetados incluem os dados da American First Finance (AFF).”

A FinWise trabalha com o credor de crédito AFF para oferecer empréstimos parcelados aos consumidores.

Leia mais sobre ameaças internas: 61% das empresas dos EUA atingidas por violações de dados internos

De acordo com a notificação, 689.000 clientes FinWise/AFF foram afetados pelo incidente interno. Na carta de notificação, a FinWise redigiu a maioria das categorias de informações pessoais relevantes para o caso, revelando apenas que os nomes completos dos clientes foram comprometidos.

“Ao saber do incidente, a FinWise imediatamente lançou uma investigação em consulta com profissionais externos de segurança cibernética que investigam e analisam regularmente esses tipos de situações para ajudar a determinar se algum dado confidencial foi acessado pelo ex-funcionário da FinWise após o término de seu emprego”, acrescentou.

A FinWise, com sede em Utah, ofereceu aos clientes afetados 12 meses de serviços gratuitos de monitoramento de crédito e proteção contra roubo de identidade, e pediu que eles colocassem um alerta de fraude e/ou congelamento de segurança nos arquivos de crédito, bem como obtivessem um relatório de crédito gratuito.

“Além disso, você deve sempre permanecer vigilante na revisão regular de seus extratos de conta financeira e relatórios de crédito em busca de atividades fraudulentas ou irregulares”, acrescentou.

A maioria das empresas não tem detecção de ameaças internas

O CISO da Exabeam, Kevin Kirkwood, afirmou que 90% das organizações não têm recursos para detectar e responder efetivamente a ameaças internas.

“As organizações devem fazer um trabalho melhor de priorizar e segmentar o acesso a informações confidenciais para evitar que uma pessoa possa acessar toda e qualquer informação”, acrescentou.

“Nesse caso, o agente da ameaça responsável foi demitido pela FinWise antes da ocorrência da violação, mas ainda tinha o conhecimento necessário para roubar centenas de milhares de registros de clientes.”

Kirkwood argumentou que os CISOs deveriam combinar mais investimentos em defesa cibernética com programas de educação aprimorados para os funcionários – mantendo as ameaças de IA em mente.

“As organizações devem fornecer diretrizes claras sobre como reduzir o acesso desnecessário ou não autorizado a informações confidenciais”, explicou.