paytrack
travel & expense

10 melhores práticas para prevenção de **fraudes com cartões corporativos**

paytrack.com.br

Protegendo seu cartão corporativo contra fraudes

À medida que crimes cibernéticos e fraudes online se tornam mais comuns, proteger seus cartões corporativos tornou-se essencial. Um estudo recente mostrou que 53% das perdas por fraude ocorrem em transações digitais com cartão corporativo, e que, em média, comerciantes dos EUA impedem 1.721 tentativas de transações fraudulentas por mês.

A fraude pode ocorrer de várias maneiras — de transações não autorizadas a golpes de phishing — mas a gestão proativa de riscos pode ajudar. Aqui está o que você precisa saber para gerenciar esses riscos com eficácia.

Prevenção de fraudes com cartões corporativos

Como a fraude pode acontecer

Roubo de dados do cartão: criminosos roubam dados por meio de hacks ou engenharia social para fazer compras não autorizadas. Em 2023, fraudes com cartão foram o tipo mais relatado de roubo de identidade, com 416.582 relatos à FTC.

Golpes de phishing: fraudadores criam sites falsos ou enviam e-mails ou sms enganosos para capturar informações do cartão. O relatório anual sobre phishing da Bolster também constatou que agosto de 2023 teve o maior número de sites maliciosos do ano — 2,2 milhões — à medida que os invasores passaram a usar cada vez mais páginas falsas para enganar os usuários.

Clonagem de cartão: por meio de dispositivos como skimmers, instalados em caixas eletrônicos ou maquininhas adulteradas.

Uso fora do horário comercial ou em locais inusitados: o que pode indicar uso pessoal ou externo à política de viagens da empresa.

Uso indevido por funcionários: podem ultrapassar limites, fazer compras pessoais ou usar o cartão para fins não profissionais.

Fraude por conluio interno: quando dois ou mais funcionários agem juntos para burlar políticas internas, como gerar notas fiscais falsas ou aprovar gastos indevidos.

Golpe da Falsa Central: O criminoso entra em contato se passando por funcionário do banco ou da administradora do cartão, alegando que identificou transações suspeitas na sua conta. Ele orienta a vítima a ligar para a central oficial para confirmar a informação — mas mantém a linha telefônica aberta (trava de linha), de forma que, quando a vítima "desliga" e liga novamente, ainda está falando com o golpista.

Assinaturas recorrentes: armazenar dados do cartão com comerciantes pode expor a empresa à fraude se essas contas forem invadidas.

NFC / Contactless Fraud: Em locais cheios, criminosos usam maquininhas de pagamento sem contato para tentar cobranças rápidas em cartões com NFC habilitado.

Fonte: Bolster.ai

Prevenção de fraudes com cartões corporativos

10 passos para ajudar a prevenir fraudes

01.

Administre políticas apropriadas de cartão

Restringir o uso de cartões físicos apenas a viagens de negócios.

Limitar dispositivos conectados a carteiras digitais.

Cancelar cartões imediatamente em caso de perda/roubo.

Alertar e informar os funcionários sobre os riscos.

02

Use o cartão VCN para viagens corporativas

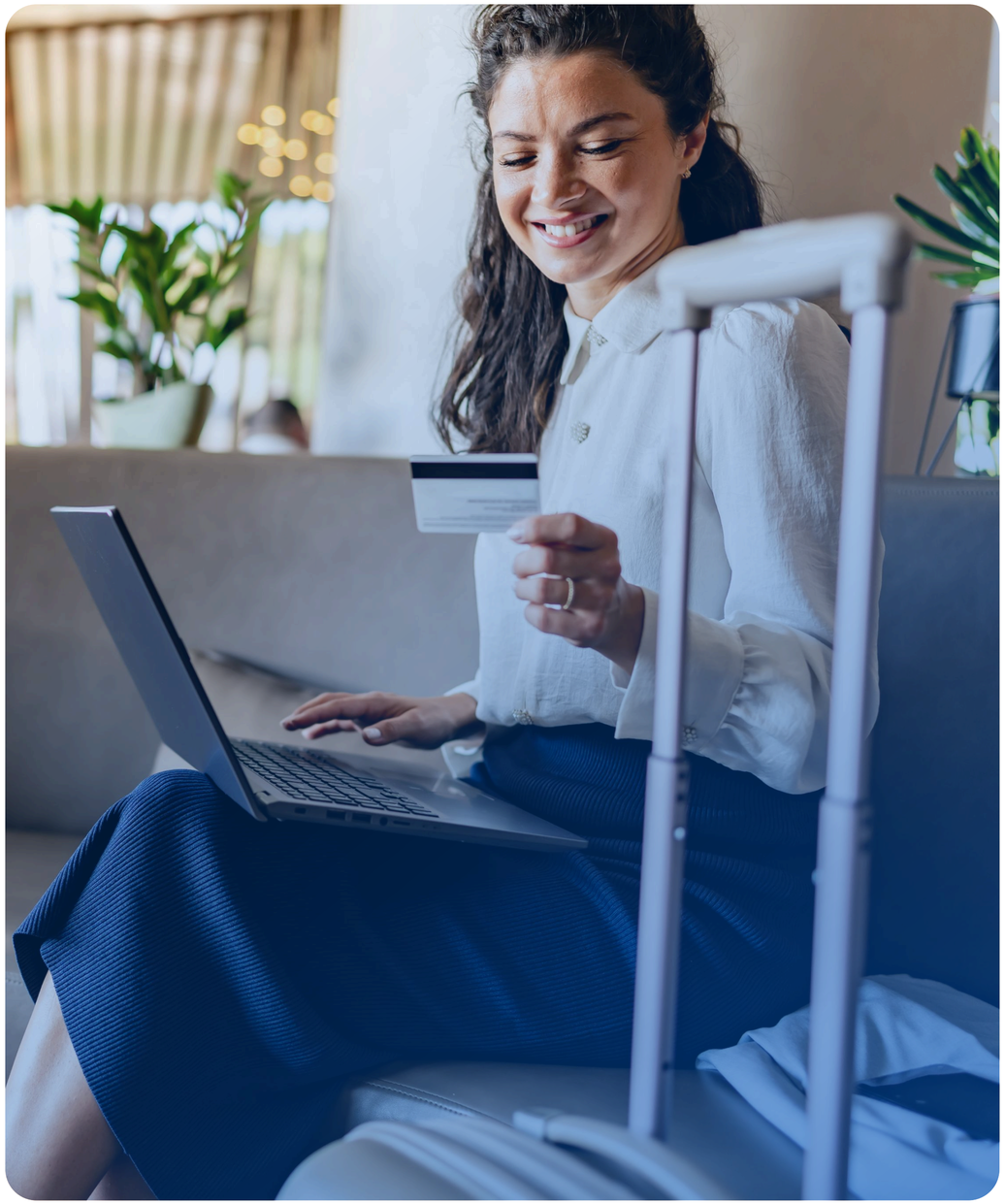
O Virtual Card Number (VCN) é a evolução dos cartões virtuais, trazendo ainda mais segurança e controle para os pagamentos de viagens corporativas. Ele gera números exclusivos e temporários, vinculados a compras específicas — como passagens aéreas, reservas de hotel ou aluguel de veículos — válidos apenas para uma única transação ou para um período pré-determinado.

Assim, mesmo que os dados sejam comprometidos, o cartão se torna inválido, evitando perdas por fraude. Além disso, o VCN permite criar um número diferente para cada fornecedor, facilitando o rastreamento e a conciliação das despesas. Essa tecnologia é especialmente valiosa em ambientes de alta rotatividade de transações, como o turismo corporativo, onde garantir segurança e agilidade no pagamento é essencial para manter a operação sem contratempos.

03. Defina limites de gastos

Para cartões de compra virtual: limite os valores diários e por transação para reduzir perdas em caso de fraude. E para limitar sua exposição ao risco se o cartão for comprometido, bloqueie o uso a categorias específicas de comerciantes ou moedas, e defina datas de expiração curtas. Isso restringe os tipos de estabelecimentos e os valores que os fraudadores podem tentar cobrar.

Para cartões físicos: estabeleça uma política apropriada e defina o limite de crédito e o limite por transação como igual ou inferior ao limite total de gastos do cartão — ou igual ao valor exato da compra empresarial.



04.

Limite usuários autorizados

Auditorias internas devem revisar o uso por departamento e por tipo de despesa, para detectar concessões excessivas ou fora da política. O ideal é que o cartão esteja vinculado diretamente a um projeto ou centro de custo, com responsáveis identificáveis.

- Restrinja o acesso apenas a quem realmente precisa.
- Faça revisões periódicas.

05.

Eduque os funcionários

- Ensine a identificar tentativas de phishing.
- Oriente sobre como agir em caso de perda ou roubo.

Treinamentos periódicos podem usar **exemplos reais de fraude** dentro da própria empresa (quando possível), simulando tentativas de golpe para reforçar a vigilância.

06

Habilite autenticação em duas etapas (2FA)

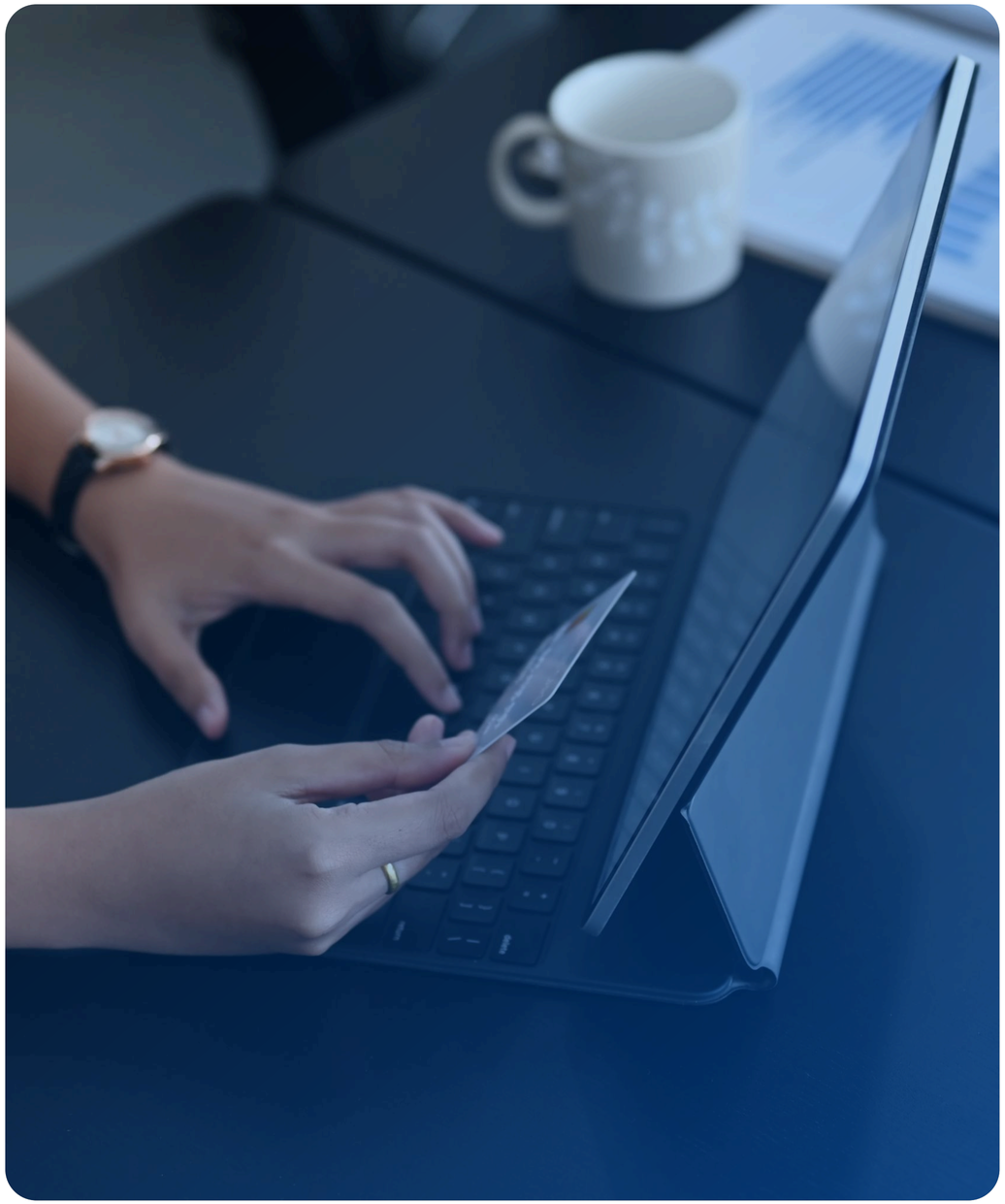
Adiciona uma camada extra de segurança contra acessos não autorizados. Prefira emissores de cartão que integrem o 2FA com sistemas biométricos (como reconhecimento facial ou digital) para aprovação de transações via app.

07.

Monitore transações regularmente

Utilize IA para detecção de padrões anômalos, como:

- Compras em feriados
- Reembolsos duplicados
- Uso acima da média histórica do usuário
- Configure alertas em tempo real
- Faça auditorias mensais



08.

Criptografe dados de pagamento

Trabalhe com fornecedores e parceiros que criptografam os dados ou que tenham um plano de segurança de dados/pagamentos implementado, o que reduzirá a exposição à fraude em caso de violação.

Ajude a garantir que suas informações de pagamento sejam enviadas de forma segura e diretamente ao fornecedor, de modo que só possam ser processadas por ele. Reforce a exigência de PCI DSS (Payment Card Industry Data Security Standard) entre fornecedores que armazenam ou processam dados sensíveis do cartão.

09. Mantenha-se atualizado sobre tendências de fraude

Acompanhe notícias e alertas do setor para se antecipar a novas ameaças.
Uma dica é acompanhar relatórios como o da Bolster.ai.

- Relatórios da ACFE, **Association of Certified Fraud Examiners.**
- Alertas da Febraban, **Federação Brasileira de Bancos.**
- Publicações de **consultorias em compliance** como Deloitte e KPMG.

10

Trabalhe com emissores confiáveis de cartões

A Paytrack oferece monitoramento inteligente com alertas em tempo real, regras customizáveis e inteligência antifraude integrada à plataforma. Além da tecnologia antifraude, avalie:

- Tempo médio de resposta a disputas de transações.
- Disponibilidade de dashboards para análise granular de gastos.
- Capacidade de integrar com o ERP da empresa.

Boas práticas contínuas de prevenção de fraudes

Tome sempre as seguintes ações – você pode ser responsabilizado por transações não autorizadas, conforme permitido por lei:

- Aja diante de alertas ou avisos de fraude.
- Relate as fraudes assim que identificá-las.
- Considere desativar cartões não utilizados ou inativos por mais de 12 meses.

Compromisso da Paytrack com a sua proteção

Além dos controles antifraude integrados à plataforma, a Paytrack monitora transações em tempo real e aplica inteligência de dados para detectar comportamentos suspeitos e proteger os recursos da sua empresa.

Esse é o **nosso compromisso com mais de 7.000 (CNPJ) clientes** que contam com a gente - e podemos fazer o mesmo por você.

Espaço do Especialista

O cartão corporativo é um voto de confiança da empresa. Cada transação realizada deve ser realizada com responsabilidade, além de fortalecer nossa reputação e evitar prejuízos que podem comprometer todo o time. Fraudes não são apenas erros, são riscos sérios que devemos prevenir com atenção, bom senso e compromisso inegociável com a segurança.

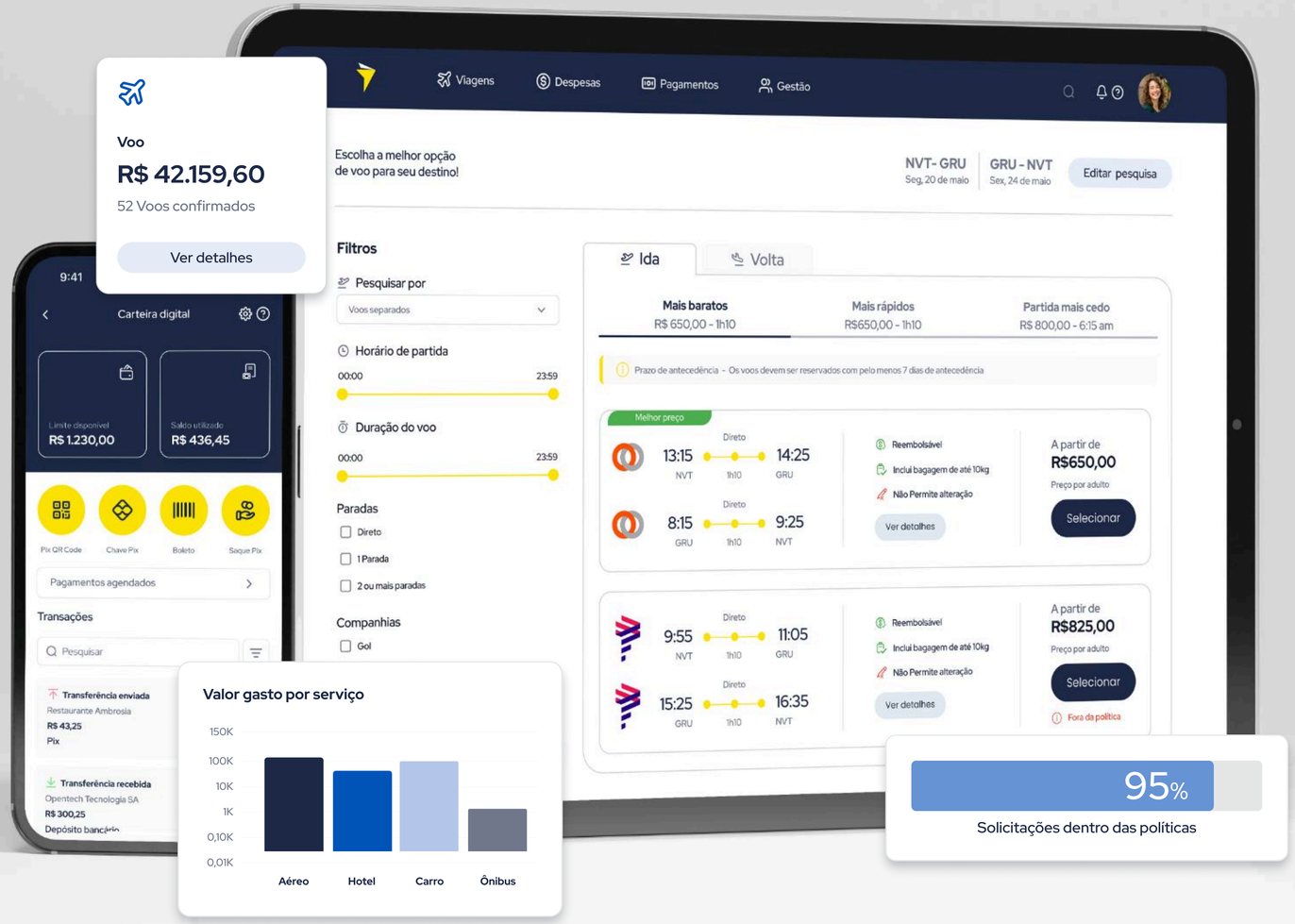
- Renan Ferraro, Gerente de Cyber Security

paytrack
travel & expense

A Paytrack é uma plataforma completa para gestão de despesas e viagens corporativas. Com ela, você elimina tarefas manuais, centraliza pagamentos, ganha visibilidade em tempo real e reduz riscos de fraude com cartões corporativos.

Diga adeus às planilhas, recibos físicos e retrabalho.
Diga olá à automação, controle e economia.

Acesse **paytrack.com.br** para saber mais.



Contatos:

E-mail: contato@paytrack.com.br
Telefone: 0800 888 0560
Endereço: Rodovia Paul Fritz Kuehnrich, 955 - 1º andar - Blumenau, SC