Melhores Práticas de Segurança para Pagamentos Manuais e Eletrônicos

As transações bancárias de hoje estão mais digitalizadas do que nunca. Apesar da tendência de aumento dos pagamentos eletrônicos e da disponibilização de meios mais eficientes para gerenciar a área de Pagamentos a Fornecedores das empresas, algumas vezes ainda é necessário transferir recursos financeiros de maneira manual. Veremos a seguir alguns dos riscos de fraude relacionados com ambos os métodos de pagamento, juntamente com algumas das melhores práticas para estar protegido contra essas ameaças.

Pagamentos Manuais

Quais são os riscos?

Por definição considera-se que os pagamentos realizados manualmente trazem maiores riscos que as transferências eletrônicas. Estes apresentam um risco de fraude inerente, devido à intervenção manual necessária para realizar a transação. Os pagamentos manuais incluem os seguintes riscos associados:

- São fáceis de falsificar, especialmente com os modernos aplicativos atualmente disponíveis, que permitem que qualquer pessoa, com um computador, possa imprimir cheques, logotipos de empresas e outras coisas mais que tornam as falsificações mais acessíveis;
- As assinaturas dos representantes das empresas podem ser facilmente obtidas, interceptando-se cheques ou documentação da empresa no correio. Sendo tais assinaturas facilmente falsificadas;
- As transações manuais possuem pontos de vulnerabilidade que os tornam suscetíveis a alterações. As transações em papel podem ser facilmente interceptadas no caminho ao banco, onde os detalhes do beneficiário podem ser capturados e depois alterados, para redirecionar os recursos a contas fraudulentas pertencentes a terceiros;
- A demora na conciliação de contas torna mais tardia a detecção de qualquer fraude e também aumenta o risco de fraude interna. A solicitação de uma transação manual em papel pode ser completamente falsificada por uma fonte interna e ser inserida em um grupo de transações em papel que foram solicitadas durante o dia, o que acaba redirecionando recursos a uma conta fraudulenta externa;
- Os pagamentos manuais, com frequência, podem ser realizados sem passar por processos de controle;
- Geralmente não podem ser concluídos de modo remoto, o que leva as empresas a trabalharem com exceções em algumas situações, como cheques e documentos pré-assinados, o que gera riscos desnecessários a organização.

Como combatê-los?

Se for necessário realizar pagamentos manuais, há uma série de medidas que você pode tomar para proteger-se contra as fraudes.

- Se você realiza pagamentos regulares a um determinado fornecedor, pode configurar uma instrução de pagamento padrão que já esteja com os dados apropriadamente

validados. Uma vez que esse processo estiver configurado, todos os pagamentos devem ser feitos somente a essa conta;

- Não aceite alterações sem a verificação adequada. Por exemplo, uma solicitação para alterar dados de uma conta bancária de um fornecedor deve ser verificada com um processo de "Call-back" (retorno de ligação), utilizando um número de telefone previamente fornecido por esse fornecedor;
- As solicitações de transferência manual devem ser executadas com níveis adicionais de aprovação;
- Devem-se utilizar sempre formulários pré-estabelecidos e autorizados, que não sejam diferentes de utilizações anteriores.

Pagamentos eletrônicos

Porque são seguros?

Os pagamentos eletrônicos são considerados mais seguros, por uma série de razões, que incluem:

- São criptografados e podem ser protegidos com uma senha segura de "único uso" gerada por dispositivos de segurança (tokens) e podem exigir diversos níveis de autorização e aprovação;
- São rapidamente realizados e não possuem riscos de serem interceptados;
- As assinaturas não podem ser falsificadas. Os perfis e autorizações são suportados por senha segura e aprovações em múltiplos níveis;
- Realiza-se uma conciliação imediata e automatizada. As contas podem ser verificadas e conciliadas em tempo real, o que permite a detecção de eventuais erros;
- Os limites para autorizações podem ser estabelecidos de acordo com os riscos associados a cada transação;
- Permitem o acesso remoto de maneira segura no caso dos usuários que realizam e aprovam as transações fora do escritório.

Existem riscos?

Apesar de possuírem maior segurança, os pagamentos eletrônicos não estão livres de riscos. Seja de modo intencional ou não, as senhas, por exemplo, podem estar comprometidas. Isto pode ocorrer se as senhas são compartilhadas ou são guardadas em lugares inseguros. Também existe o risco de conspirações, que envolva duas áreas ou funcionários trabalhando em conjunto para comprometer a integridade do pagamento. Portanto, algumas das melhores práticas para reduzir os riscos dos pagamentos eletrônicos incluem:

- Garanta que o token e a senha de acesso sejam guardados sempre de forma separada;
- Não permita que as senhas sejam compartilhadas;
- Garanta que os funcionários estejam com os níveis de autorização adequados ao seu cargo;
- Faça com que todas as suas transações sejam aprovadas através de um duplo controle; por exemplo, defina como padrão a funcionalidade de feito-conferido;
- Defina critérios de conciliação de contas, de tal modo que riscos sejam rapidamente identificados;
- Garanta que as transações de alto valor exijam sempre múltiplos aprovadores.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions

1461594 08/16