MATERIAL DE REFERÊNCIA PARA O AGENTE

ISTO É WU SM POLÍTICA E PROCEDIMENTOS ANTIFRAUDE PARA AGENTE

WESTERN UNION WU SM

moving money for better

Sumário

NOME DA EMPRESA _____

ENDEREÇO _____

CIDADE, PAÍS, CÓDIGO POSTAL _____

DATA _____

1. Introdução

Esta P&P (Policy and Procedure, política e procedimento) descreve os padrões do programa que a Western Union ("WU") exige que seja implementado por seus Agentes[1] e descreve as etapas que o Agente deve seguir para adotar esses padrões. Os padrões e requisitos estabelecidos nesta P&P fazem parte dos Requisitos de Serviços da Western Union. A Western Union está disponível para ajudar os Agentes se tiverem quaisquer dúvidas sobre os requisitos do programa contidos nesta P&P.

Esta P&P foi adotada pelo Agente da Western Union nomeado na parte superior da página. O objetivo desta P&P é estabelecer um programa antifraude projetado para proteger os consumidores da Western Union. A fraude ao consumidor é cometida por pessoas que cometem golpes, convencendo indivíduos desavisados a enviar dinheiro a elas. Vários tipos de golpes são descritos nesta P&P. Todos os FLAs (Front-Line Associates, atendentes) devem ler esta P&P e entender os tipos de golpe listados nela. (Um FLA é uma pessoa que executa transações da Western Union na loja do Agente.) Todos os FLAs devem concluir o treinamento em fraude antes de fornecer produtos e prestar serviços da Western Union. Esta P&P descreve as etapas que um FLA deve seguir se o Agente ou um consumidor parecer ser vítima de uma fraude.

Devido aos avanços da tecnologia, os métodos para fraudar consumidores bem-intencionados estão se tornando cada vez mais sofisticados e difíceis de identificar. Por isso, os Agentes da Western Union podem ser usados acidentalmente para ajudar criminosos a fraudar pessoas. Os processos exigidos nesta P&P foram projetados para identificar e impedir que os criminosos usem os produtos e serviços da Western Union para fraudar consumidores. A conscientização do FLA e do Agente sobre o comportamento e os tipos de transações dos consumidores no ponto de venda pode ajudar a impedir fraudes contra os consumidores da Western Union.

Esta P&P também implementa processos projetados para impedir que os Agentes também se tornem vítimas de fraude. As fraudes contra Agentes são uma ação cometida por um terceiro que resulta em prejuízo financeiro para um Agente ou para a Western Union. Os Agentes FLAs desempenham um papel importante para impedir que os Agentes sejam vítimas de fraude. Todos os FLAs que processam transações da Western Union devem ler esta P&P e realizar o treinamento completo em como identificar, impedir e relatar fraudes contra Agentes.

A prevenção contra fraudes é uma parceria entre o Agente e a Western Union. Por esses motivos, esta P&P exige o treinamento e a conscientização dos FLAs, bem como uma comunicação saudável entre o Agente e a Western Union por meio do Contato Dedicado da Western Union. *A Western Union é exigida por seus órgãos reguladores a monitorar as atividades de fraude em todas as lojas do Agente e a suspender ou rescindir os Agentes (ou suas lojas) que sejam usados para facilitar transações de fraude. Se o FLA for cúmplice em uma fraude, a Western Union encerrará o contrato do Agente de fornecer os produtos e prestar os serviços da Western Union.. Nos casos em que um FLA temporário for cúmplice em atividades de fraude, a Western Union encerrará o contrato do Agente de fornecer os produtos e prestar os serviços da Western Union em qualquer loja em que o FLA temporário cometeu a atividade em cumplicidade e encerrará o ID do FLA temporário.* Portanto, é fundamental que todos os FLAs entendam os princípios desta P&P e sigam os procedimentos descritos aqui.

O diretor designado do Agente identificado na caixa abaixo é responsável por garantir que esta P&P e todo o treinamento adequado sejam implementados.

DIRETOR RESPONSÁVEL
NOME COMPLETO _____ ENDEREÇO _____ TELEFONE _____

1 Neste Manual, um "Agente" se refere a qualquer Agente Principal, Agente da Rede, Delegado Autorizado ou Agente Independente com o qual a Western Union tenha um relacionamento contratual estabelecido para vender, fornecer produtos ou prestar serviços da Western Union a consumidores. Os Subagentes que operam com base em um contrato assinado por um Agente Principal ou sua empresa matriz também deverão seguir esta política. Esses agentes incluem os que fazem transações sob as marcas Western Union, Orlandi Valuta e Vigo.

2. Objetivo

O objetivo desta P&P é estabelecer as medidas e os processos de prevenção contra fraudes que todos os Agentes da Western Union devem implementar. Esta P&P fornece descrições de diferentes tipos de fraudes e transações que foram usadas no passado para fraudar consumidores e Agentes da Western Union. Ela também descreve os comportamentos dos consumidores que indicam que um consumidor pode ser vítima de fraude ou outros crimes. Todos os FLAs devem observar o comportamento dos consumidores como parte do processo de transferência de dinheiro e devem conseguir identificar os consumidores que apresentam esses comportamentos. Esta P&P também descreve situações que podem indicar que o Agente está sendo direcionado como uma vítima de fraude. O treinamento e a conscientização são a base deste programa antifraude.

3. Tipos de golpes de fraude ao consumidor

A seguir, há uma lista dos golpes de fraude ao consumidor que foram observados. Observe que essa lista apresenta exemplos de golpes de fraude que foram observados, mas pode não incluir todos os possíveis golpes de fraude. Todos os FLAs devem conseguir reconhecer esses golpes para ficarem em alerta quando um consumidor agir ou fizer declarações que indiquem que ele é uma possível vítima de fraude. Os métodos dos criminosos para fraudar os consumidores evoluem com o tempo; portanto, essa lista poderá ser atualizada periodicamente. O Suporte ao Agente da Western Union está disponível para oferecer assistência se o Agente tiver dúvidas sobre esses cenários.

GOLPE DE TAXA ANTECIPADA OU PRÉ-PAGAMENTO

A vítima é solicitada a efetuar o pagamento de taxas antecipadas por serviços financeiros que nunca são prestados. Muitas vezes, as vítimas enviam uma sucessão de transações para pagamento de várias taxas iniciais. Métodos: cartão de crédito, concessão, empréstimo, herança, investimento.

GOLPE DE ANTIVÍRUS

Alguém entra em contato com a vítima alegando ser de uma empresa bem conhecida de computadores ou software e informando que um vírus foi identificado no computador da vítima. A vítima é informada que o vírus pode ser removido e o computador protegido por uma pequena taxa com um pagamento via cartão de crédito ou transferência de dinheiro. Na verdade, não há vírus no computador e a vítima acaba perdendo o dinheiro que enviou para obter a proteção.

GOLPE DE CARIDADE

Alguém entra em contato com a vítima por e-mail, correio ou telefone pedindo o envio de uma doação por transferência de dinheiro a um indivíduo para ajudar vítimas de um recente evento atual, como um desastre ou uma emergência (como uma enchente, um terremoto ou um ciclone). Organizações de caridade legais nunca pedirão que doações sejam enviadas a um indivíduo por meio de um serviço de transferência de dinheiro.

GOLPE DE EMERGÊNCIA

A vítima é levada a acreditar que está enviando fundos para ajudar um amigo ou um ente querido em uma necessidade urgente. A vítima envia o dinheiro com urgência, já que a preocupação natural da vítima com um ente querido é explorada.

GOLPE DE EMPREGO

A vítima responde a uma publicação de vaga, é contratada para o emprego fictício e recebe um cheque falso para despesas relacionadas ao trabalho. O valor do cheque ultrapassa as despesas da vítima e a vítima envia os fundos restantes de volta usando uma transferência de dinheiro. O cheque é devolvido por falta de fundos e a vítima é responsável pelo valor total.

GOLPE DE CHEQUES FALSOS (FALSIFICAÇÃO)

As vítimas recebem um cheque como parte de um golpe e são orientadas a depositá-lo e a usar os fundos para despesas de emprego, compras pela Internet, compras em mystery shopping etc. O cheque é falso (falsificado) e a vítima é responsabilizada por quaisquer fundos usados do cheque. Lembre-se de que os fundos de um cheque depositado em uma conta não devem ser usados até que o cheque seja oficialmente compensado, o que pode levar semanas.

GOLPE DOS AVÓS

Esse golpe é uma variação do golpe de emergência. Uma pessoa entra em contato com a vítima fingindo ser um neto em perigo, ou uma pessoa de autoridade, como um médico, policial ou advogado. O fraudador descreve uma situação de emergência ou urgência (fiança, despesas médicas, fundos de viagem de emergência) que envolve o neto e que exige o envio imediato de uma transferência de dinheiro. Nenhuma emergência ocorreu de fato e a vítima que enviou o dinheiro para ajudar seus netos perdeu seu dinheiro.

GOLPE DE IMIGRAÇÃO

A vítima recebe uma ligação de alguém que alega ser um oficial de imigração, dizendo que há um problema com o registro de imigração da vítima. Informações pessoais e detalhes confidenciais relacionados ao status de imigração da vítima podem ser fornecidos para fazer com que a história pareça ser mais legítima. Um pagamento imediato é exigido para corrigir quaisquer problemas com o registro da vítima e pode haver a ameaça de deportação ou detenção caso o pagamento não seja feito imediatamente por transferência de dinheiro.

GOLPE DE COMPRAS PELA INTERNET

A vítima envia dinheiro para a compra do item solicitado on-line (por exemplo, animais de estimação, carros). Muitas vezes, os itens são anunciados no Craigslist, eBay, Alibaba, etc. Depois que o dinheiro é enviado, a vítima nunca recebe o produto.

GOLPE DE IMPOSTO

Alguém entra em contato com a vítima alegando ser de uma agência governamental e diz que ela deve impostos, que devem ser pagos imediatamente para evitar detenção, deportação ou suspensão da carteira de habilitação/passaporte. A vítima é instruída a enviar uma transferência de dinheiro ou comprar um cartão de débito pré-carregado para pagar os impostos. As agências governamentais nunca pedirão o pagamento imediato ou ligarão falando sobre impostos sem primeiro ter enviado uma fatura.

GOLPE DE LOTERIA OU OUTRO PRÊMIO

A vítima é informada que ganhou na loteria, um prêmio ou um sorteio e que deve enviar dinheiro para cobrir os impostos ou as taxas sobre os ganhos. A vítima pode receber um cheque corresponde a parte dos ganhos e, assim que o cheque é depositado e o dinheiro enviado, o cheque é devolvido por falta de fundos.

GOLPE DE COMPRAS EM MYSTERY SHOPPING

O fraudador entra em contato com a vítima por meio de um site de empregos ou a vítima responde a um anúncio sobre uma oportunidade de emprego para avaliar um serviço de transferência de dinheiro. O fraudador geralmente envia um cheque à vítima para depósito e instrui a vítima a enviar uma transferência de dinheiro, retendo parte do cheque como pagamento. A vítima envia o dinheiro, o fraudador o recebe e, quando o cheque é devolvido por falta de fundos, a vítima é responsabilizada pelo valor total.

GOLPE DE PAGAMENTO EXCEDENTE

O fraudador envia à vítima um cheque que parece válido como pagamento por um serviço ou produto. Normalmente, o valor do cheque ultrapassa o valor que a vítima espera receber, e o fraudador pede à vítima para devolver o valor excedente fazendo uma transferência de dinheiro. Quando o cheque é devolvido, a vítima assume o valor total.

GOLPE DE RELACIONAMENTO

A vítima é levada a acreditar que tem uma relação pessoal com alguém que conheceu on-line, geralmente pelas mídias sociais, em um fórum on-line ou em um site de relacionamento. Muitas vezes, a vítima está envolvida emocionalmente e costuma se referir ao beneficiário como noivo.

GOLPE DE PROPRIEDADE DE ALUGUEL

A vítima envia dinheiro para depósito em uma propriedade de aluguel e nunca recebe acesso à propriedade. A vítima também pode ser o proprietário que recebe um cheque do locatário e é solicitado a enviar uma parte do cheque de volta usando uma transferência de dinheiro, mas o cheque é devolvido por falta de fundos.

4. Responsabilidades dos Atendentes

Os Atendentes devem ser treinados antes de realizar transações da Western Union para poder identificar os tipos de esquemas de fraude, transações e comportamentos do consumidor que indicam que um consumidor pode ser vítima de fraude. Se as respostas, o comportamento ou os padrões de transação do consumidor indicarem que ele pode ser vítima de fraude, o FLA poderá se recusar a enviar a transação.[2]

2 Se houver requisitos para relatar uma transação que foi recusada porque o FLA suspeitou de fraude, o FLA deverá seguir os requisitos específicos de relatório.

4.1 INDICADORES DE FRAUDE NO COMPORTAMENTO DO CONSUMIDOR — LADO DO ENVIO

Todos os FLAs são responsáveis por entender os comportamentos do consumidor descritos abaixo. A Western Union está apresentando os comportamentos típicos dos consumidores para o envio de transações que podem indicar que um consumidor é vítima de fraude. A seguir, há os comportamentos do consumidor dos quais o FLA deve estar ciente para poder identificar uma possível vítima de fraude e fazer perguntas adicionais ao consumidor sobre a transação.

- Consumidores que parecem apreensivos ou confusos, especialmente os idosos e adultos dependentes.
- Consumidores que parecem muito ansiosos para enviar dinheiro.
- Consumidores que expressam preocupação sobre como enviar dinheiro em caso de emergência.
- Consumidores que parecem empolgados ou ansiosos com a ideia de receber uma grande soma em dinheiro ou de "realizar o negócio do século".
- Consumidores que dizem que estão comprando algo que lhes foi vendido por telefone. Os Agentes da Western Union não podem processar um pagamento em dinheiro ou cartão pré-pago que seja resultado de uma chamada de telemarketing. Consulte Transações Proibidas de Telemarketing a seguir.
- Consumidores que podem estar enviando dinheiro pela primeira vez e fazem perguntas sobre o processo.

NOTA: É necessário perguntar a todos os consumidores idosos e adultos dependentes se eles conheceram a pessoa a quem estão enviando dinheiro porque são altamente vulneráveis a fraude on-line por telefone.

4.2 INDICADORES DE FRAUDE DE TRANSAÇÕES — LADO DO ENVIO

O FLA deve estar ciente dos cenários a seguir e fazer perguntas adicionais aos consumidores sobre a transação, pois pode haver evidências de fraude ou outros crimes.

- Consumidores que fazem várias transações em um único dia ou no decorrer de poucos dias.
- Consumidores que desejam proteger ou atrasar sua transferência de dinheiro usando uma pergunta de teste.
- Consumidores que enviam dinheiro para si mesmos e, depois, mudam o beneficiário da transação.

4.3 INDICADORES DE FRAUDE NO COMPORTAMENTO DO CONSUMIDOR — LADO DO PAGAMENTO

Os seguintes comportamentos são exemplos de indicações de que um consumidor pode estar realizando uma transação induzida de modo fraudulento na loja do Agente:

- Consumidores que apresentam comportamentos suspeitos, como ficar parado ou agir com nervosismo, evitar fazer contato visual, conferir o telefone para ver instruções e ficar observando o local.
- Vários indivíduos entram na loja e apenas uma pessoa faz a transação (geralmente os outros ficam parados perto da porta).
- Consumidores que parecem confusos, não estão familiarizados com o modo de usar a Western Union® ou que estão seguindo instruções de alguém por telefone que está recebendo a transferência.
- Consumidores que admitem que nunca conheceram pessoalmente o remetente ou que possam ter sido orientados a dizer que conheceram pessoalmente o remetente.
- Consumidores que estão seguindo a direção de alguém por telefone ou que está fora da loja enquanto recebe uma transação.

4.4 INDICADORES DE FRAUDE DE TRANSAÇÕES — LADO DO PAGAMENTO

O FLA deve estar ciente dos exemplos a seguir de tipos de transações e fazer perguntas adicionais aos consumidores sobre a transação, pois pode haver evidências de fraude ou outros crimes.

- Consumidores que recebem transações com nomes diferentes ou variações de ortografia.
- Consumidores que recebem valores incomuns ou não padrão de transações em um curto período.
- Consumidores que recebem um número alto incomum de transações em um curto período.
- Consumidores que recebem várias transações que exigem uma pergunta de segurança.
- Consumidores que recebem várias transações de vários remetentes, sem nenhuma relação de parentesco aparente.
- Consumidores que recebem várias transações de vários estados, cidades ou países diferentes.
- Consumidores que frequentemente recebem e enviam transações, especialmente quando as transações são enviadas para fora do país do Agente, nas quais o valor enviado corresponde ao valor que está sendo pago. Preste muita atenção quando um consumidor que recebe um pagamento imediatamente tenta enviar os fundos recebidos a outra pessoa.
- Um consumidor que saca dinheiro e, em seguida, entrega visivelmente o dinheiro a outra pessoa dentro ou fora da loja do Agente.

5. Transações Proibidas de Telemarketing

A FTC (Federal Trade Commission, comissão federal de comércio) dos Estados Unidos alterou sua TSR (Telemarketing Sales Rule, regra de vendas de telemarketing), com vigência a partir de 13 de junho de 2016. As novas regras proíbem que os vendedores e operadores de telemarketing aceitem transferências de dinheiro ou fundos carregados em um cartão pré-pago de consumidores dos EUA como pagamento por mercadorias ou serviços oferecidos ou vendidos por telemarketing. A Western Union e seus Agentes também podem violar a TSR ao facilitar a transferência de fundos a um operador de telemarketing, pelo menos quando estiverem cientes de que o vendedor ou operador de telemarketing esteja violando a regra ou se evitarem saber disso de maneira consciente.

A TSR define "telemarketing" amplamente para cobrir praticamente qualquer transação comercial que envolva o uso de um telefone para fazer ou receber chamadas entre um consumidor localizado em um estado e um operador de telemarketing ou vendedor em outro estado ou país. Por exemplo, a Western Union ou uma loja do Agente da Western Union poderá violar a regra transferindo fundos de um consumidor dos EUA para um operador de telemarketing ou vendedor em relação a uma promoção de férias "gratuitas" ou com muitos descontos, golpes de prêmios ou sorteios ou vendas de revistas "com desconto". Se o Agente ou o FLA suspeitar que o consumidor possa estar enviando fundos para um operador de telemarketing ou que o destinatário dos fundos pode ser um operador de telemarketing, o Agente deverá interromper a transação e relatar o evento ao Contato Designado da Western Union para o Agente.

6. O que fazer quando houver suspeita de fraude

Há etapas que o FLA pode seguir para impedir fraudes contra os consumidores em sua loja. Como o FLA está presente quando o consumidor está enviando fundos induzidos por fraude, a função do FLA na prevenção contra fraudes é essencial. Esta seção descreve as medidas que o FLA pode tomar se houver uma tentativa de transação de fraude e como acompanhamento depois que o consumidor ou o fraudador deixar a loja.

6.1 CONVERSANDO COM O CONSUMIDOR

Caso o FLA observe qualquer um dos comportamentos ou indicadores de transação para remetentes de dinheiro descritos em *Indicadores de fraude no comportamento do consumidor — Lado do envio ou Indicadores de fraude de transações — Lado do envio*, o FLA deverá:

- perguntar ao consumidor por que está enviando dinheiro;
- perguntar ao consumidor se a pessoa que receberá o dinheiro é alguém que o consumidor conhece pessoalmente (face a face);
- se os fundos estiverem sendo enviados para uma "emergência", pedir que o consumidor verifique se há uma emergência real antes de enviar o dinheiro;
- instruir o consumidor compartilhando estas recomendações:
  - "Nunca enviar dinheiro para alguém que você não conhece pessoalmente."
  - "Nunca enviar dinheiro para uma emergência, a menos que você tenha verificado que há uma emergência."
  - "Nunca enviar fundos que o consumidor recebeu por cheque até que o cheque seja compensado, o que pode levar semanas."
- dar ao consumidor o folheto de Conscientização sobre Fraudes da Western Union (se disponível) e pedir que ele acesse http://wu.com/fraudawareness;
- se o FLA suspeitar que um consumidor é vítima de uma fraude, dizer ao consumidor que não é possível enviar o dinheiro para sua própria proteção;
- informar ao consumidor que existe a suspeita de fraude e que ele deve verificar se a transação está sendo enviada por um propósito legítimo;
- se você enviar uma transação que acredita estar sendo feita suspeita de uma fraude, entre em contato com a Linha Exclusiva Antifraude da Western Union para suspender a transação. Entre em contato com seu Contato Dedicado da Western Union se não tiver certeza do número de telefone correto da linha exclusiva antifraude para seu país;
- se um consumidor chegar à loja do Agente para reclamar que foi vítima de uma fraude usando produtos e serviços da marca Western Union, o Agente deverá ligar para a linha exclusiva antifraude da Western Union para relatar a fraude ou instruir o cliente sobre como ligar para a linha exclusiva antifraude. O Agente deve também fornecer informações sobre prevenção contra fraude ao consumidor.

6.2 SEGUINDO OS PROCEDIMENTOS ADEQUADOS DE PAGAMENTO

Os Atendentes sempre devem seguir os procedimentos adequados de pagamento para garantir que as informações fornecidas pelo consumidor correspondam ao que está registrado no sistema de ponto de venda. O FLA deve verificar os seguintes campos na tela antes de efetuar o pagamento:

- o Número de Controle de Transferência de Dinheiro,
- o valor do pagamento,
- a área (país, cidade ou município) onde o pagamento deve ser efetuado,
- o país (local) de onde os fundos foram enviados, e
- o nome do remetente.

Além dessas informações sobre a transação, o FLA deve garantir que a identificação do consumidor que está efetuando o pagamento corresponde à que está no sistema de ponto de venda. A identificação fornecida pelo consumidor que recebe os fundos deve:

- ser atual (dentro da validade),
- ser aceitável sob as regras locais de PLD do país (por exemplo, é necessário apresentar um documento de identificação oficial com foto?),
- ser original e inalterada, e
- conter o nome e sobrenome do consumidor, além de uma fotografia do consumidor que corresponda ao indivíduo que está coletando os fundos.

Se o FLA suspeitar de fraude, também deverá fazer perguntas abertas que façam com que o consumidor que recebe o pagamento pense em suas respostas. (Uma pergunta aberta é aquela que não pode ser respondida com um simples "sim" ou "não".) O FLA deve prestar atenção às respostas do consumidor a essas perguntas e determinar se elas fazem sentido. Ele também deve prestar atenção ao comportamento do consumidor, como nervosismo ou verificar o telefone ou anotações antes de responder. O FLA deve escolher perguntas que sejam adequadas à situação e pode usar perguntas diferentes das fornecidas abaixo se elas funcionaram bem no passado. Alguns exemplos de perguntas abertas são:

- "Como você conhece a pessoa que enviou o dinheiro?"
- "Onde e quando você conheceu o remetente?"
- "Por que esse dinheiro foi enviado a você?"
- "Com que frequência você usa a Western Union?"
- "Alguém pediu que você viesse ao Agente coletar o dinheiro?"

Se o FLA suspeitar de fraude, recomenda-se que ele peça ao destinatário uma segunda forma de identificação. Essa segunda forma de identificação deve ser um documento que corresponda ao nome da primeira forma de identificação, por exemplo, uma conta de telefone, água ou eletricidade. Solicitar uma segunda forma de identificação poderá ajudar o FLA a impedir que um indivíduo colete o dinheiro de uma transação induzida de modo fraudulento. Essa segunda forma de identificação serve para fins de verificação e não precisa ser registrada.

As transações que um FLA suspeitar que estejam relacionadas a fraude não devem ser pagas. O FLA deverá informar ao consumidor que a transação não está disponível no momento. Se o FLA não efetuar o pagamento dos fundos porque suspeita de fraude, deverá relatar a transação a seu Contato Dedicado da Western Union. Se o Agente precisar registrar Relatórios de Transações (ou Atividades) Suspeitas, o Diretor de Conformidade Designado deverá seguir as regras e os procedimentos para registro de relatórios de transações suspeitas do país.

7. Preocupações de segurança do FLA

Se o FLA estiver preocupado com sua segurança, poderá enviar os fundos, mas deverá entrar em contato imediatamente com a Western Union para suspender qualquer transação que foi enviada. Se a loja do Agente estiver equipada com o botão de fraude no lado do envio, ele deverá encaminhar a transação à Western Union para revisão. Da mesma forma, se o FLA estiver preocupado com sua segurança pessoal no lado do pagamento, deverá pagar a transação. Se a loja do Agente estiver equipada com o botão de fraude no lado do pagamento, ele deverá encaminhar a transação à Western Union e informar ao consumidor que a transação não está disponível.

8. Protegendo-se contra fraudes contra Agentes

Os Agentes e suas lojas também podem ser vítimas de fraude. As fraudes contra Agentes são fraudes cometidas contra a loja do Agente que geram um prejuízo financeiro para a loja. Esta P&P exige que os Agentes implementem treinamento e procedimentos para todos os funcionários, a fim de evitar fraudes contra Agentes. Esse tipo de fraude pode acontecer de diferentes formas. A seguir, há os métodos comuns para fraudar Agentes. Observe que esses cenários podem não se aplicar a todos os sistemas de transferência de dinheiro, como a transferência de dinheiro por telefone.

8.1 FRAUDE CONTRA AGENTES COMETIDA POR TELEFONE

Os fraudadores ligam para a loja do Agente e tentam induzir o FLA a oferecer acesso aos sistemas de computador do Agente. Assim que têm acesso, os fraudadores usam o sistema de ponto de venda para enviar dinheiro sem que a loja do Agente possa coletar fundos pela transação. Eles também podem baixar vírus de computador prejudiciais ou fazer com que o FLA baixe-os involuntariamente. O FLA deve estar ciente dos tipos de fraude abaixo para evitar ser vítima de fraude.

ACESSO REMOTO

Um fraudador liga para uma loja do Agente como se fosse da Western Union ou um representante de serviços técnicos da rede alegando que o sistema da Western Union precisa ser atualizado. O funcionário do Agente concorda em estabelecer uma conexão de apoio por computador usando um software de acesso remoto. Em seguida, o fraudador pode assumir o controle do computador e enviar transações sem que a loja do Agente colete fundos.

INVASÕES DE COMPUTADOR

Um funcionário do Agente clica em um link em um e-mail ou acessa um site e, involuntariamente, baixa um software mal-intencionado no computador que oferece os serviços da Western Union. Esse software mal-intencionado, por meio de registradores de pressionamento de teclas, captura os IDs e senhas do operador da Western Union, que podem ser usadas posteriormente por fraudadores para enviar transações.

TRANSAÇÕES DE TESTE

Um fraudador liga para uma loja do Agente para pedir que o funcionário do Agente insira dados de uma transação como uma sessão de teste ou treinamento; por fim, isso resulta na realização de uma transação sem a coleta de fundos.

ENTRADAS DE CÓDIGO

Um fraudador liga para uma loja do Agente e instrui o funcionário do Agente a inserir códigos no sistema da Western Union para corrigir um problema técnico ou atualizar o sistema do ponto de venda. Quando o funcionário do Agente segue as instruções do fraudador, inserindo um número de cartão com 16 dígitos e um valor em dólares com 5 dígitos, ele recarrega um cartão pré-pago que pertence ao fraudador.

8.2 FRAUDE CONTRA AGENTES COMETIDA POR E-MAIL

As fraudes por e-mail (também chamadas de phishing) visam a fazer com que o FLA ou qualquer outro funcionário do Agente ofereça involuntariamente ao fraudador o acesso aos sistemas de computador internos do Agente. O phishing também pode ser feito por telefone celular ou mensagem de texto. Esse tipo de fraude visa a roubar informações pessoais ou enviar códigos ou softwares mal-intencionados ao computador ou telefone celular do Agente. Todos os FLAs que têm acesso aos computadores do Agente devem ser treinados para evitar serem vítimas de phishing.

A seguir, há indicadores que o FLA pode procurar para ajudar a identificar um possível e-mail de phishing:

- um remetente desconhecido,
- uma correspondência não solicitada,
- uma correspondência inesperada,
- saudações genéricas,
- solicitações de informações pessoais,
- um senso de urgência, e
- gramática ruim ou erros de ortografia.

Se o FLA acreditar que pode estar lendo uma fraude por phishing, deverá:

- **FAZER:** passar o mouse sobre os links do e-mail para ver o site ao qual o link está direcionando o usuário.
- **FAZER:** excluir todos os e-mails que parecem suspeitos.

O funcionário NÃO deverá fazer o seguinte com uma suspeita de fraude de phishing:

- **NÃO:** clicar em links de e-mails que parecem suspeitos. Basta clicar em um link para baixar arquivos prejudiciais em seu computador ou dispositivo móvel.
- **NUNCA:** fornecer suas credenciais de login ou outras informações pessoais confidenciais a ninguém por telefone ou e-mail. Isso pode dar a um criminoso cibernético um fácil acesso às suas contas on-line ou ao seu computador.

8.3 COMO PROTEGER O AGENTE CONTRA FRAUDES

Para reforçar a segurança da loja do Agente e ajudar a impedir que a loja do Agente seja vítima de fraude, NUNCA realize qualquer uma das seguintes ações:

- NUNCA efetue uma transação de transferência de dinheiro sem coletar fundos.
- NUNCA insira informação no sistema da Western Union por telefone.
- NUNCA aceite conexão de suporte de um computador, a menos que tenha feito contato com a Western Union ou com o escritório sobre esse problema, mesmo que o autor da chamada afirme que ele seja da Western Union ou do serviço técnico da rede.
- NUNCA baixe software de uma fonte desconhecida ou insira CD/USB fornecido pelos serviços da Western Union.
- NUNCA insira uma transação de treinamento/teste no sistema ativo. Se utilizar o WUPOS,™ verifique o status do sistema no canto superior direito da tela.
- NUNCA retorne ou faça uma ligação para a Western Union usando um telefone fornecido pelo autor da chamada. Utilize somente números fornecidos pela Western Union em documentos oficiais da empresa.

Realize estas ações técnicas para proteger a loja do Agente contra fraudes.

- Os computadores com serviços da Western Union devem executar somente software suportado pelo setor e devem ser atualizados/corrigidos em tempo hábil, quando solicitado. Certifique-se de instalar programas antivírus, antispyware e de firewall; defina uma atualização automática/execução automática para proteção diária.
- Não execute recursos externos de e-mail.
- Desative portas USB, disquetes e CD-ROMS nos computadores usados para prestar serviços da Western Union.
- Defina o horário designado de operação no sistema da Western Union para que o sistema de transferência de dinheiro não fique ativo após o expediente. Desligue o computador após o horário designado de operação.
- Os funcionários devem bloquear seus computadores ao sair de suas estações de trabalho.
- Exclua os IDs de operador de qualquer funcionário desligado ou demitido.
- Os IDs e senhas de operador nunca devem ser compartilhados com ninguém, inclusive outros funcionários ou qualquer pessoa que solicite senhas por e-mail ou mensagem de texto. As senhas devem ser alteradas a cada 90 dias.

9. Práticas diárias de prevenção contra fraude

Há práticas comuns que o Agente deve implementar que podem ajudar a impedir fraudes contra os consumidores e contra o Agente. Elas incluem:

- revisar os materiais de treinamento em Conscientização sobre Fraudes fornecido à sua loja pela Western Union;
- revisar todos os alertas de fraudes da Western Union publicados no sistema de transferência de dinheiro ou no AgentPortal (essas mensagens contêm informações oportunas de alerta sobre fraudes);
- nunca permitir que os consumidores vejam a tela do computador ao inserir informações da transação;
- nunca permitir que pessoas não autorizadas acessem o espaço atrás do balcão ou próximo à área de transações da Western Union; e
- nunca responder a e-mails, chamadas telefônicas ou faxes que solicitem informações de contas da Western Union, como números das contas, IDs dos terminais, IDs e senhas dos operadores. A Western Union jamais ligará para um Agente e solicitará essas informações. Não responda se alguém ligar para o Agente e pedir acesso ao sistema, senhas ou outros protocolos de segurança.