

GUIA DE SENSIBILIZAÇÃO DOS CONSUMIDORES PARA A FRAUDE

Small World Financial Services Group

Coletivamente ou individualmente referidas como "Empresa" ou "Grupo SWFS"

Versão 1	Maio	2013
Versão 2	Março	2017
Versão 3	Abril	2020
Versão 4	Novembro	2022



POLÍTICA DE CLASSIFICAÇÃO DE INFORMAÇÕES

Classificação da informação: Interna

Acesso: Acesso concedido a todos os empregados, fornecedores, clientes, comerciantes ou empreiteiros do Pequeno Mundo. A autorização de acesso a partes externas só será concedida por gestores de departamento e informada ao Comité de Ética (o "CE").

Cópia: Apenas o pessoal autorizado (Acesso) será autorizado a criar cópias físicas e digitais do documento. Armazenamento: Cópias físicas não serão deixadas visíveis quando não assistidas. O armazenamento lógico seguirá as regras de restrição de acesso.

Transmissão: O documento só será partilhado por pessoal autorizado a recetores previamente autorizados utilizando canais encriptados ou, pelo menos, a encriptação do ficheiro. As chaves e/ou senhas nunca serão partilhadas através do mesmo canal. As cópias físicas serão entregues ao destinatário e enviadas através de um serviço de correio seguro, se necessário.

Destruição: As cópias em papel serão descartadas utilizando uma trituradora. A destruição lógica das cópias será feita por qualquer parte autorizada após o fim da vida útil (fim de utilização) da cópia acima referida. A destruição completa do documento será acordada pelo Global Compliance Office.



Tabela de conteúdos

1. Introdução	4
2. Abuso Fraudulento de Transferências de Dinheiro	5
3. Exemplos de Fraude	5
3.1 Fraude Nigeriana	6
3.2 Esquemas de Lotaria	7
3.3 Romance	7
3.4 Fraude de Idosos	7
3.5 Envio de dinheiro a um estranho	8
3.6 Familiar com necessidade	8
3.7 Esquemas de Empréstimos	8
3.8 Esquemas de Taxa Antecipada	9
3.9 Mulas de Dinheiro	10
3.10 Oferta de Automóveis Usados	10
3.11 Compra de um Veículo	11
3.12 Anúncios em Jornais	11
3.13 Comerciantes Desonestos	11
3.14 Fraude "Sidi Salem"	12
3.15 Fraude na Venda de Ações	12
4. Sinais de uma possível fraude	13
5. Dicas para Clientes	13
6. Denúncia de Fraude	14



1. Introdução

O objetivo deste Guia de Sensibilização para a Fraude dos Clientes é sensibilizar para o modus operandi utilizado pelos fraudadores contra o nosso sistema de transferência de dinheiro. Este manual dirige-se a clientes, empregados e agentes do Small World Financial Services Group (doravante "Small World" ou "SWFS").

A gestão dos riscos de fraude é um objectivo-chave para o Small World. Em primeiro lugar, existe a obrigação de proteger o nosso sistema de se tornar um instrumento para atividades fraudulentas e existe a obrigação de alertar os nossos clientes para tais atividades. Em segundo lugar, a Small World quer proteger a sua reputação como um fornecedor global fiável de serviços de transferência de dinheiro. A nossa empresa tomará medidas contra qualquer forma de atividade criminosa, quer se trate de branqueamento de capitais, financiamento do terrorismo ou fraude.

Neste manual, fornecemos-lhe detalhes sobre potenciais esquemas de fraude. Serão também discutidos exemplos práticos de como os autores de fraudes operam. Finalmente, dar-lhe-emos algumas dicas importantes para se proteger e evitar tornar-se uma vítima de fraude.



2. Abuso Fraudulento de Transferências de Dinheiro

A fraude relacionada com as transferências de dinheiro é cometida contra duas vítimas diferentes:

- 1. Clientes que transferem dinheiro para um beneficiário fraudulento
- 2. Funcionários ou agentes que trabalham para a Small World

O primeiro grupo, os nossos clientes, é a vítima mais visada. Os clientes podem tornar-se vítimas de vários esquemas utilizados por burlões para se apropriarem ilegalmente do dinheiro do cliente ou para roubar dinheiro de outros através do cliente. Além disso, a pessoa que opera o sistema Small World, para realizar encomendas para os nossos clientes, pode ser vítima de fraude. Neste caso, os infratores tentam aceder ao sistema de transferência de dinheiro abusando da palavrapasse do seu sistema. Na secção seguinte deste manual, encontrará alguns estudos de caso que discutem diferentes tipos de esquemas de fraude.

Fraude de transferência de dinheiro centrada no cliente:

Ao contar uma história credível, os autores das fraudes motivam as suas vítimas a transferir dinheiro para beneficiários desconhecidos e pouco fiáveis.

3. Exemplos de Fraude

Nesta seção, discutiremos as características da fraude de transferência de dinheiro. Exemplos gerais de fraudes:

- 1. Compras pela Internet ou em leilão;
- 2. Impostos ou outras taxas para reivindicar prêmios de lotaria;



- 3. Adiantamentos ou taxas de empréstimos;
- 4. Oportunidades de investimento;
- 5. Situações de emergência com alguém que você conheceu online;
- 6. Trabalhos que podem ser feitos a partir de casa, mas que precisam de uma taxa para formação.

Além desses exemplos – é claro – existem outros tipos de fraude de transferência de dinheiro e novos tipos surgem regularmente. No entanto, geralmente eles têm características semelhantes que você pode aprender a reconhecer. Abaixo, discutiremos alguns tipos de fraude com mais detalhes, para que você tenha uma boa ideia de que tipo de características devem ser observadas.

3.1 Fraude Nigeriana

Os infratores tentam primeiro contactar potenciais vítimas em grande escala através da Internet ou do correio eletrónico. As vítimas recebem uma oferta lucrativa; esta pode ser um contrato, um bilhete de lotaria vencedor ou uma herança que pode ser reclamada. No caso de um "esquema romântico", fotografias de homens e mulheres bonitos tiradas da Internet são anunciadas em sites ou fóruns de encontros. Caso a vítima reaja a esta primeira proposta, são solicitadas informações pessoais à vítima e são enviados documentos adicionais para tornar a oferta mais credível. Pouco tempo depois, os clientes são solicitados a enviar um adiantamento a fim de reclamar a totalidade do montante, ou a "data na Internet" revela-se de repente com necessidade de dinheiro. Os pedidos de dinheiro continuam até as vítimas ficarem desconfiadas e deixarem de pagar. O dinheiro para a fraude nigeriana será geralmente enviado da América do Norte, Europa Ocidental ou Península Arábica para vários países da África Ocidental. Especialmente a Nigéria, Costa do Marfim, Senegal, Togo, Gana e Benin são comuns como destino final do dinheiro. No entanto, os infratores utilizam cada vez mais intermediários na Europa Ocidental para receberem o dinheiro e o enviarem para a África Ocidental. Isto coloca uma barreira adicional entre o infrator e a vítima. Quando estes intermediários são estabelecidos na Europa, as transações podem ser divididas em fundos recebidos dos mandantes noutros países ocidentais, por um lado, e transferências para beneficiários na África Ocidental, por outro.



3.2 Esquemas de Lotaria

Os esquemas de lotaria envolvem vítimas que recebem e-mails ou cartas prometendo enormes ganhos, invariavelmente de uma lotaria estrangeira que afirma que foram atribuídos números vencedores à vítima. A vítima é solicitada a contactar os organizadores e a enviar dinheiro para cobrir os custos administrativos para divulgar os ganhos - que não existem.

3.3 Romance

Conheceu alguém através de um anúncio pessoal, e-mail, sala de chat ou uma mensagem instantânea? Pediram-lhe para enviar dinheiro para viajar ou para os ajudar financeiramente? Isto é uma fraude. Qualquer dinheiro recebido por esta pessoa não pode ser recuperado e você perderá qualquer dinheiro enviado.

3.4 Fraude de Idosos

Um estranho começa uma relação próxima consigo e oferece-se para gerir as suas finanças e bens. Por outro lado, as assinaturas em documentos não se assemelham à sua própria assinatura. Não se deixe enganar na separação do seu dinheiro através de esquemas de abuso financeiro. Os burlões tentarão manipulá-lo para transformar propriedade e/ou dinheiro, e isto pode deixar o seu dinheiro, conta corrente ou mesmo as suas poupanças de vida completamente destruídas numa única transação. Os esquemas de abuso financeiro podem assumir muitas formas, incluindo fraude de telemarketing, roubo de identidade, empréstimos predatórios, e esquemas de melhoria da habitação e de planeamento imobiliário. Nunca confie o seu dinheiro a alguém que não conheça.



3.5 Envio de Dinheiro a um Estranho

A Small World nunca recomenda o envio de dinheiro a um estranho. Qualquer dinheiro recebido por um estranho não pode ser recuperado e, infelizmente, não receberá o seu dinheiro de volta.

3.6 Familiar com Necessidade

Recebeu uma chamada telefónica de um neto ou de um membro da família? Por outro lado, um "advogado" ou "agente da polícia" lá com o seu familiar? Estão desesperados por terem sido detidos no Canadá por não terem licença de pesca ou por capturarem uma espécie de peixe protegida? Tiveram um acidente de automóvel? Estão a pedir dinheiro para pagar multas ou para a reparação de automóveis? Um parente telefonou porque precisa de dinheiro para um membro da família em necessidade médica ou de medicamentos? Isto é um SCAM! Use de precaução ao enviar dinheiro em qualquer uma destas situações. As pessoas que telefonam podem solicitar que envie dinheiro para qualquer parte do mundo. Se não puder verificar com o membro da sua família (chamando o número que tinha antes desta chamada, e não o "novo número" que a pessoa que liga lhe dá) que estão a pedir dinheiro e não têm a certeza sobre a transação, não envie o dinheiro. Ficará com prejuízo por qualquer dinheiro que transfira.

3.7 Esquemas de Empréstimos

Recebeu um e-mail ou uma carta sobre a obtenção de um empréstimo? Foi-lhe pedido para enviar dinheiro para taxas de empréstimo, impostos, taxas de serviço, pagamentos adiantados, ou qualquer outro motivo? Isto é um "SCAM" (Esquema). Não envie dinheiro a uma empresa de empréstimo para obter um empréstimo. Se o dinheiro for transferido e recebido, não poderá ser recuperado. O dinheiro que enviou será perdido.

Os criminosos estão sempre à procura de novas formas de roubar dinheiro a vítimas inocentes. Uma forma de o fazerem é convencendo o seu cliente (doravante referido como "vítima") a enviar-lhes dinheiro através do nosso serviço de transferência de dinheiro. O criminoso utiliza



técnicas inteligentes para defraudar a vítima. Estes criminosos visam aqueles que estão com a sorte em baixo, aqueles que perderam recentemente o seu emprego, ou aqueles que estão a lutar para cumprir obrigações financeiras durante esta dura economia. No exemplo seguinte, o criminoso apresenta-se como um agente de empréstimos (doravante referido como "criminoso") para um banco ou outra instituição financeira e concentra-se nos indivíduos que necessitam de um empréstimo muito necessário. Estes indivíduos contactam a vítima via telefone, e-mail, ou pelo correio tradicional e explicam que foram pré-qualificados para receber um empréstimo de até 5.000 euros. O criminoso oferece juros baixos, pagamentos mensais baixos, e aprova o empréstimo com pouca ou nenhuma verificação de crédito. Mesmo que a vítima possa ser cética no início, o criminoso assegura à vítima com certeza que receberá o empréstimo dentro de um período de uma semana. Como demonstração de boa fé, o criminoso instrui a vítima a utilizar o nosso serviço de transferência de dinheiro para pagar os primeiros cinco meses do empréstimo. A vítima concorda em pagar adiantado 1.000 euros pelo empréstimo (200 euros por mês, vezes 5 meses, é de 1.000 euros). No final da semana, a vítima percebe que o empréstimo não foi depositado na sua conta bancária. A vítima tenta então contactar o criminoso, mas apercebe-se de que o número de telefone já não está em serviço. A vítima envia então um e-mail ao criminoso, mas não recebe qualquer resposta. A última opção da vítima é cancelar a transação e receber um reembolso total. A vítima, contudo, não é elegível para receber um reembolso, porque até lá o criminoso já levantou o dinheiro. Este chamado esquema de empréstimo foi concebido para roubar o dinheiro do seu cliente.

3.8 Esquemas de Taxa Antecipada

Num esquema de taxas adiantadas, a vítima paga dinheiro a um defraudador na expectativa de receber algo de maior valor, por exemplo, um empréstimo, contrato, investimento, presente, etc. Recebem então pouco ou nada em troca. Este esquema também envolve coisas como a venda de produtos ou serviços, férias, prémios, ofertas de investimento e prémios de lotaria.



3.9 "Mulas" de Dinheiro

O fenómeno da mula de dinheiro pode ser descrito da seguinte forma. As organizações criminosas tentam atrair as pessoas através de anúncios de emprego na Internet. Aqueles que concordam com isto são geralmente desempregados ou jovens. Têm de conceder acesso à sua conta bancária para a qual o dinheiro é transferido, geralmente do estrangeiro. O titular da conta tem então de levantar o dinheiro em numerário pouco tempo depois de receber o dinheiro e transferi-lo para o estrangeiro utilizando uma agência de transferência de dinheiro. Os indivíduos envolvidos podem reter 10% do dinheiro depositado como comissão. Os contratos de trabalho enviados por correio eletrónico parecem muito profissionais e completos. As empresas parecem ser genuínas e querem oferecer às pessoas a oportunidade de ganhar algum rendimento adicional. É impressionante que as empresas russas estejam frequentemente envolvidas como potenciais empregadores. Os fundos transferidos para a conta são muitas vezes o produto de um esquema de "phishing", que é um esquema na Internet. As pessoas são atraídas para um falso website bancário e pedidas para introduzir dados bancários pessoais. Como tal, os fraudadores podem obter números de cartões de crédito para levantar dinheiro das contas sem o conhecimento das vítimas. Estas são geralmente contas bancárias em bancos alemães, belgas e dinamarqueses.

3.10 Oferta de Automóveis Usados

Este golpe em particular começa com um anúncio num site ou revista de automóveis onde, por exemplo, um vendedor inglês está tentando vender um carro top de gama a um preço reduzido. O vendedor geralmente diz que está no exterior, num país como Espanha ou Portugal, e que precisa vender o carro rapidamente. Eles dizem às vítimas que não podem ver o carro uma vez que já se encontra na empresa de transporte. Na verdade, não há carro nenhum e as vítimas já enviaram o dinheiro quando percebem que isto é uma FRAUDE.



3.11 Compra de um Veículo

Encontrou um grande veículo online ou num anúncio com um preço demasiado bom para ser verdade? Está a ser-lhe pedido que envie o pagamento de entrada através de uma transferência de dinheiro da Small World? Infelizmente, é uma Fraude. Não envie dinheiro para o veículo ao vendedor ou a um representante de pagamento. O burlão da compra do veículo pode tentar convencê-lo a pagar através da Small World para evitar o imposto sobre vendas e obter um ótimo preço. Podem até enviar-lhe uma carta ou e-mail de autenticação dizendo-lhe que comprou o artigo, mas para o entregar é preciso primeiro transferir fundos. Não receberá um carro ou camião. Uma vez o dinheiro transferido e recebido, não poderá ser recuperado e, infelizmente, ficará perdido qualquer dinheiro que tenha transferido.

3.12 Anúncios em Jornais

Encontrou algo para venda nos classificados ou em qualquer tipo de anúncio de jornal? Pediramlhe para pagar o artigo através de uma transferência de dinheiro SWFS? Isto é uma Fraude. Não utilize uma transferência de dinheiro para comprar um artigo a um estranho. Não é seguro utilizar um serviço de transferência de dinheiro quando se tenta comprar um artigo.

3.13 Comerciantes Desonestos

Os comerciantes desonestos (ou "chamadas falsas") aparecem sem serem convidados nas casas das pessoas apresentando um negócio legítimo ou troca. Elas são muitas vezes membros de grupos criminosos e altamente organizados e se deslocam pelo país em busca de áreas com uma elevada população de idosos ou comunidades diversificadas. São conhecidos por compartilhar informações sobre áreas adequadas à exploração criminosa. Cobram deliberadamente muito por serviços insatisfatórios ou desnecessários, danificam propriedades propositadamente para obter o trabalho, deixando o trabalho inacabado, e usam um comportamento agressivo e intimidante para extorquir dinheiro. Os comerciantes desonestos exercem uma pressão extrema sobre as pessoas vulneráveis para obterem dinheiro, acompanhando-os por vezes a instituições



financeiras para levantarem dinheiro, e muitas vezes extorquir dinheiro à vítima durante um período prolongado. Muitas pessoas idosas ficam cada vez mais isoladas após a perda de um parceiro e a manutenção do seu jardim e casa exterior pode indicar a sua vulnerabilidade, tornando-as mais suscetíveis à exploração por criminosos.

3.14 Fraude "Sidi Salem"

Este tipo de fraude teve origem principalmente na Tunísia, mas propagou-se agora a vários países europeus, tais como França, Itália, Alemanha e Bélgica. O nome fraude "Sidi Salem" refere-se a pessoas na Tunísia que vendem vinho. O mesmo método é também utilizado sob outras formas semelhantes à fraude nigeriana. Alega-se que a pessoa envolvida ganhou uma mala cheia de dinheiro e é solicitada a pagar taxas de desalfandegamento ou taxas legais por este dinheiro. Os autores da fraude tentarão atingir o maior número possível de potenciais vítimas, principalmente por telefone. Eles vendem vinho de alta qualidade a preços excessivos em comparação com o preço do mercado europeu. Devido ao preço elevado, as vítimas respondem inicialmente que não estão interessadas, as vítimas são então contactadas repetidamente e por vezes, várias vezes ao dia. A maioria das vítimas são pessoas idosas, preferem ceder e aceitar a oferta para que o assédio cesse. Grandes quantidades de dinheiro estão envolvidas nas transações, por vezes até dezenas de milhares de euros dentro de alguns meses. Além disso, as vítimas que efetivamente recebem o vinho concordam que se trata de um simples vinho de mesa.

3.15 Fraude na Venda de Ações

A fraude de venda de quotas (ou telemarketing) consistem em enviar à vítima chamadas ou correspondências não solicitadas sobre investimentos. Estas são tipicamente provenientes de "corretores" com base no exterior que tem como alvo os acionistas europeus, oferecendo-se para as vender o que acaba muitas vezes por ser ações de alto risco sem valor em investimentos nos E.U.A. ou no Reino Unido. Os "corretores" podem ser muito persistentes e extremamente persuasivos.



4. Sinais de uma Possível Fraude

É difícil saber se um cliente está a ser exposto por fraude, mas alguns dos indicadores típicos de que uma pessoa está a ser exposta por fraude são:

- Pessoa idosa (no entanto, todas as idades estão hoje em dia a ser contactadas por burlões).
- Nome ocidental.
- Ocupação Reformado, desempregado, etc.
- Envio de pagamentos de faturação, pagamentos de bens/serviços tais como honorários de advogados ou taxas alfandegárias e pagamento de material/veículo tais como tratores, automóveis ou ouro.
- O envio é de/localizado num país bem desenvolvido e o envio para um país em desenvolvimento (local beneficiário) que não faz sentido.
- Múltiplos perfis no nosso sistema (devido ao limite de conhecimentos técnicos, os idosos tendem a criar novos perfis).
- Múltiplos beneficiários em diferentes países do terceiro mundo.

5. Dicas para Clientes

Nesta secção final, fornecemos-lhe algumas dicas importantes a fim de deter os autores de fraudes. A observação destas dicas irá reduzir significativamente o risco de se tornar uma vítima de fraude.

Dicas para os clientes porem fim aos autores de fraudes:

Nunca envie dinheiro para alguém que não conheça pessoalmente.



- Nunca envie dinheiro primeiro para obter algo em troca mais tarde, como para uma lotaria, um emprego, ou um empréstimo.
- Não acredite numa história de emergência de alguém que diz ser um familiar sem verificar se a pessoa é realmente seu familiar.
- Não acredite em ofertas que indicam que uma transferência de dinheiro é a única forma possível de pagamento.
- Pense antes de agir, uma oferta que parece "boa demais para ser verdade" geralmente é "boa demais para ser verdade".
- Esteja ciente de que não há proteção contra a perda de uma transferência de dinheiro fraudulenta

6. Denúncia de Fraude

Se você acha que descobriu uma tentativa ou um caso de fraude, por favor informe-nos imediatamente através dos contatos abaixo:

PAÍSES DA EUROPA CENTRAL -

Luxemburgo 020301681

reportfraud.lu@smallworldfs.com

França 0178904614

reportfraud.fr@smallworldfs.com

Portugal (+351) 213 849

279reportfraud.pt@smallworldfs.com

Bélgica 28888468

reportfraud.be@smallworldfs.com

Alemanha 002146704046

reportfraud.ge@smallworldfs.com

Holanda 204125099

reportfraud.ne@smallworldfs.com

Áustria 0720775495

report fraud. au@smallworldfs. com



PAÍSES DO NORTE DA EUROPA - Tel: +46101 013 160

Suécia reportfraud.sw@smallworldfs.com Dinamarca reportfraud.dk@smallworldfs.com Noruega reportfraud.no@smallworldfs.com Finlândia reportfraud.fi@smallworldfs.com

ITÁLIA - Telefone: 026784141

reportfraud.it@smallwordfs.com

REINO UNIDO Telefone: +44 (0) 2073781100

reportfraud.uk@smallworldfs.com

IRLANDA Telefone: +35318728528

reportfraud.ie@smallworldfs.com

GRÉCIA Telefone: +34 914251540

reportfraud.gr@smallworldfs.com

CHIPRE Telefone: +44 (0) 2073781100

reportfraud.cy@smallworldfs.com

SUÍÇA Telefone: +41 44 508 3318

reportfraud.ch@smallworldfs.com

ESPANHA Telefone: +34 914251540

reportaFRAUDE.es@smallworldfs.com

ÁFRICA Telefone: +225 22487619 / + 22542202089

reportfraud.af@smallworldfs.com

EUA Telefone 212-268-9290

reportfraud.us@smallworldfs.com

CANADÁ Telefone: 1-877-268-6458

reportfraud.ca@smallworldfs.com

BRASIL Telefone: São Paulo +551135649080



Fora de São Paulo: 0800 7179700 reportfraud.br@smallworldfs.com

OUTROS PAÍSES Telefone: +44 (0) 2073781100

reportfraud.oc@smallworldfs.com