(2026-07-27 Versão alternativa R3)

Interpelação Escrita

Deputado José Maria Pereira Coutinho

"Falhas graves na prevenção e nos mecanismos de bloqueio dos sistemas de pagamento electrónico das instituições financeiras locais perante burlas por código QR e problemas de reembolso aos consumidores lesados"

O nosso **Gabinete de Atendimento aos Cidadãos** tem vindo a receber regularmente, nos últimos dois anos, inúmeros pedidos de apoio e queixas de cidadãos que foram lesados através de sistemas de pagamento automático integrados em aplicações para telemóvel.

No dia 24 de Junho de 2026, a Polícia Judiciária (PJ) emitiu um aviso de alerta público, no qual registou 10 queixas de burla praticadas através da plataforma Facebook. Os burlões induzem as vítimas a ler códigos QR de origem desconhecida sob o pretexto de supostos reembolsos. Os prejuízos dos primeiros 10 casos variavam entre os 410 e as 17 383 patacas, com um montante global agregado de cerca de 52 000 patacas.

Posteriormente, na conferência de imprensa realizada a 14 de julho de 2026, a PJ informou que, apenas no período compreendido entre 7 e 13 de julho, foram registados mais 36 casos idênticos de burla online, resultantes da vinculação fraudulenta de contas. O prejuízo total das vítimas ultrapassou as 240 000 patacas, existindo uma vítima com perdas que atingiram as 37 000 patacas. A única medida preventiva anunciada na ocasião consistiu na exibição de um aviso de alerta aquando da vinculação das contas a plataformas terceiras, sem qualquer mecanismo de bloqueio automático de operações suspeitas.

Esta sequência de acontecimentos revela que decorreram cerca de 20 dias entre a primeira divulgação pública desta modalidade de burla (24 de junho) e a adopção de uma medida mínima, limitada a um aviso visual (14 de julho). Neste intervalo, não foram implementadas intervenções imediatas de bloqueio de riscos, quer pela entidade gestora das contas, quer pelas autoridades competentes responsáveis pela supervisão das instituições privadas da área financeira em causa.

Acresce que a Autoridade Monetária de Macau (AMCM) publicou a Guideline on Risk Management of Electronic Banking, cujo capítulo «FRAUD MONITORING» estabelece obrigações imperativas para todas as instituições autorizadas:

a)Criar um mecanismo eficaz de monitorização de burlas, apto a prevenir, detectar e bloquear transacções excepcionais ou atividades invulgares de forma tempestiva;

b)Acompanhar permanentemente a evolução das técnicas de burla e atualizar regularmente os sistemas de monitorização sempre que surjam novas ameaças;

c)Definir procedimentos formais de tratamento de incidentes fraudulentos, incluindo a suspensão imediata de transacções de alto risco para avaliação, o contacto com o cliente por canal seguro e a escalada rápida de incidentes graves à direcção da instituição.

1. Face ao número crescente de vítimas e ao aparente incumprimento dos requisitos regulamentares definidos pela AMCM, nomeadamente o sistema de pagamentos visado dotado de um mecanismo automatizado de bloqueio para dois tipos de operações: (i) transacções fraudulentas identificadas por padrões de risco, nomeadamente a vinculação a plataformas terceiras não credenciadas através de códigos QR anónimos; e (ii) sequências consecutivas de operações de elevado valor executadas após a vinculação externa da conta. Deste modo e para o futuro que medidas eficientes e eficazes vão ser implementadas pelas entidades competentes para evitar que incidentes desta natureza ou semelhantes não venham a repetir?

2. Tendo a PJ detectado e divulgado publicamente esta nova modalidade de burla por código QR associado a supostos reembolsos no dia 24 de Junho de 2026, e registado um aumento exponencial de casos ao longo dos 20 dias subsequentes até 13 de Julho. No futuro, que medidas eficazes e eficientes vão ser implementadas de uma forma sistematizada para que no âmbito da prevenção e emissão de informações de alerta à população sejam as mesmas implementadas incutindo mais da celeridade na divulgação evitando-se prejuízos aos cidadãos?

3. Os sucessivos registos de perdas avultadas por parte das vítimas demonstram que, após a vinculação fraudulenta das respectivas contas, os burlões conseguem efectuar transacções de valor considerável sem que o sistema solicite a validaçãoatravés da palavra-chave pessoal do utilizador. Esta realidade revela a existência de falhas estruturais no sistema de pagamento automático, as quais permitem a execução de transacções de elevado montante sem confirmação por senha do titular após a ligação a plataformas externas. Neste contexto, que medidas correctivas foram ordenadas pela AMCM ao operador em falta para colmatar estas

falhas de segurança e qual o prazo estabelecido para a sua resolução integral ?

José Maria PEREIRA COUTINHO
Assinatura digital
2026.08.03
13:01:03 +0800