CONFIDENCIAL — USO INTERNO

Relatório de Incidente de Segurança

Movimentações financeiras não autorizadas em produção (PIX e TED), autoria, origem do acesso e contenção junto ao BACEN

Instituição: MONETARIE SCD S.A.
ISPB: 46026562 · **CNPJ:** 46.026.562/0001-05
Data: 21/07/2026
Ambiente: Produção (monetarie-greenfield-prod)

1. Sumário do incidente

Em 20/07/2026, entre 16h25 e 16h57 (horário de Brasília), foram originadas quatro movimentações financeiras a partir de contas institucionais da própria MONETARIE SCD, todas destinadas à empresa **JF CONSULTORIAS E REPRESENTAÇÃO COMERCIAL LTDA** (CNPJ 58.269.513/0001-82). Apenas uma delas efetivou: um **PIX de R$ 200.000,00**, que foi liquidado pelo BACEN. As outras três (um PIX e duas TED) foram rejeitadas ou não concluíram, e não movimentaram recursos.

A apuração forense (somente leitura sobre os registros de produção: bancos de dados das cabines PIX e SPB, banco do Core, logs de acesso no CloudWatch, trilhas de autenticação e os logs da própria VPN de origem) identificou a autoria de forma inequívoca e conduziu a contenção do valor efetivado.

Autoria: as operações foram criadas por **Marco Aurélio Montenegro Brazil** (`marco.brazil@monbank.net`), usuário administrador autenticado, através da VPN corporativa da MonBank, a partir do endereço público real `200.155.150.126` .

Não houve invasão externa. O acesso usou credencial administrativa válida, com autenticação na VPN, e as telas legítimas de envio manual. Não há indício de força bruta, exploração de falha ou origem anônima.

Contenção executada junto ao BACEN: abertura de **MED 2.0 (Recuperação de Valores)** sobre o PIX efetivado e **Marcador de Fraude** contra a conta recebedora da JF Consultorias (seção 7).

2. As quatro movimentações

Pagador em todas: MONETARIE SCD (ISPB 46026562). Recebedor em todas: JF CONSULTORIAS E REPRESENTAÇÃO COMERCIAL LTDA (CNPJ 58.269.513/0001-82). Horários em UTC e, entre parênteses, em Brasília (BRT = UTC menos 3h).

#	Trilho	Valor	Situação real	Identificador	Criação
1	PIX (envio)	**R$ 200.000,00**	**LIQUIDADO** (recurso saiu)	`E2E E46026562202607201952kmxwrabwzgd`	19:52:01Z (16:52)
2	PIX (envio)	R$ 200.000,00	Rejeitado pelo PSP recebedor	`E2E E46026562202607201956 2j7sk6c3u7y`	19:57:06Z (16:57)
3	TED (STR0008)	R$ 432.000,00	Rejeitada no R1 do BACEN (tela: em análise manual)	`NumCtrlIF MON20260720957753618`	19:35:58Z (16:35)
4	TED (STR0008)	R$ 738.000,00	Não concluída (estado failed; tela: Criada)	`NumCtrlIF MON20260720757109907`	19:25:15Z (16:25)

Somente o item 1 movimentou recursos. Os itens 2, 3 e 4 não resultaram em débito efetivo.

3. Autoria e origem real do acesso

A trilha de autenticação da cabine PIX (`monetarie_auth.audit_logs`) registra, com IP e navegador, cada ação do operador:

Hora (UTC)	Ação	Detalhe	Resultado
19:48:59	LOGIN falhou	tentativa em pixadmin.monetarie.internal	401
19:49:09	**LOGIN ok**	`marco.brazil@monbank.net` (usuário 100)	200
19:52:01	**Criar transação**	PIX R$ 200.000,00 para a JF (ISPB 02038232)	201 (liquidou)
19:56:21	Consulta de chave	DICT do recebedor JF (documento 58269513000182)	200
19:57:06	**Criar transação**	PIX R$ 200.000,00 para a JF (ISPB 05203605)	201 (rejeitou)

Identidade do operador

Nome: MARCO AURÉLIO MONTENEGRO BRAZIL
Login (cabine PIX): `marco.brazil@monbank.net` (usuário 100)
Conta administrativa (Core): `f33ae4a7-799c-4a36-be67-26832c73f31b`, criada em 17/07/2026, status `pending_mfa_setup`
Usuário na VPN (Pritunl): `marco-brasil`, organização `monbank-interno`, servidor `monbank-prod`
Navegador: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:152.0) Firefox/152.0 (Windows 10)

Origem real (endereço público) e caminho do acesso

Endereço público real: `200.155.150.126`
Provedor do endereço: Telium Telecomunicações Ltda (CNPJ 07.272.054/0001-55), Brasil
Concentrador VPN: instância EC2 `i-0127c0d13bfc3e8a7` (`monbank-vpn-interna-prod`, Ubuntu/Pritunl), IP interno `10.50.4.151`
MFA na VPN: presente (fatores `otp + pin`) para o usuário marco-brasil

Evidência direta do log de conexão da VPN (saída do OpenVPN gerida pelo Pritunl), com o endereço público real e o usuário:

```
2026-07-20 17:27:02  200.155.150.126:18977  TLS: Username/Password authentication deferred for username 'marco-brasil'
2026-07-21 10:59:25  200.155.150.126:58881  TLS: Username/Password authentication deferred for username 'marco-brasil'
```

O mesmo endereço público (200.155.150.126) aparece de forma consistente nas conexões do usuário, que trafegam pelo concentrador VPN da MonBank (IP interno 10.50.4.151) até as aplicações.

4. Rastreamento por transação

4.1. PIX R$ 200.000,00 — LIQUIDADO (item 1)

EndToEndId: `E46026562202607201952kmxwrabwzgd` (mensagem 14753, pacs.008)
Criação / liquidação: 20/07 19:52:01Z / 19:54:03Z (confirmada por camt.054 do BACEN)
Pagador: MONETARIE SCD, CNPJ 46026562000105, conta 7686, agência 0001

Recebedor:	JF Consultorias, CNPJ 58269513000182, conta 554324, agência 3315, ISPB 02038232
Conta debitada:	conta institucional da própria Monetarie (id interno 2627)
Canal:	tela de envio manual do pix-admin (`/transactions/new`), via `POST /api/v1/transactions`
Registro no ledger:	transfer TigerBeetle `DDA4C483DFA6FE1110920ECA89B17D02`

Após a criação, os logs mostram o operador acompanhando a transação em tempo real (detalhe, linha do tempo, saldo). O recurso saiu da conta institucional e foi liquidado pelo BACEN.

4.2. PIX R$ 200.000,00 — REJEITADO (item 2)

EndToEndId: `E46026562202607201956 2j7sk6c3u7y` (mensagem 14785). Criado às 19:57:06Z, desta vez com o recebedor informado em ISPB diferente (`05203605`). Rejeitado pelo PSP recebedor. Sem débito efetivo.

4.3. TED R$ 432.000,00 — REJEITADA (item 3)

NumCtrlIF: `MON20260720957753618`. STR0008 em estado `r1_rejected` (rejeitada no R1 do BACEN; na tela consta como em análise manual). Pagador na conta institucional 2627, recebedor JF (ISPB 02038232). Não liquidou.

4.4. TED R$ 738.000,00 — NÃO CONCLUÍDA (item 4)

NumCtrlIF: `MON20260720757109907`. STR0008 em estado `failed` (na tela consta como Criada). Pagador na conta institucional 2630, recebedor JF (ISPB 02038232). Não liquidou.

5. Contexto de governança de segurança

- O time da **Vulci** (desenvolvedora) solicitou reiteradamente à Monetarie a **definição das regras de segurança** do ambiente e **nunca as recebeu**, inclusive no que se refere à **habilitação e obrigatoriedade de MFA** para os administradores. As contas administrativas envolvidas permanecem com status `pending_mfa_setup` justamente por ausência dessa definição.
- O cadastro de administradores do ambiente é responsabilidade do time da Monetarie, e foi o **time da Monetarie** quem cadastrou o usuário administrador utilizado neste incidente (em 17/07/2026). É esse cadastro que concede os poderes empregados nas operações.
- Observação técnica relevante: o operador possuía MFA na camada de VPN (fatores otp + pin), mas a camada de aplicação (Core e pix-admin) seguia sem MFA, pela pendência de definição acima. Uma política de segurança formal teria tornado o MFA obrigatório também no money-path e estabelecido alçada de aprovação para valores elevados.

6. Contenção executada junto ao BACEN

Sobre o único item que efetivou (PIX de R$ 200.000,00), foram registradas duas ações no DICT de produção do BACEN, ambas assinadas digitalmente pela Monetarie e confirmadas pela resposta do BACEN:

6.1. MED 2.0 — Recuperação de Valores

Identificador BACEN: `94889900-4bf7-477e-9d51-c6a8e10530bd`
Status no BACEN: **AWAITING_ANALYSIS** (aguardando análise)
Participante reportante: 46026562 (MONETARIE SCD)
Transação raiz: `E46026562202607201952kmxwrabwzgd`
Tipo de situação: FRAUDULENT_ACCESS (acesso fraudulento)
Contato informado: gabriel@monetarie.com / +5548991411426
Grafo de rastreamento: maxHops **2 (máximo)** , maxTransactions 5 (máximo), hopWindow PT2H (máximo), minTransactionAmount 0,01
Envio: 21/07/2026 14:03:07Z, CorrelationId `A20260721110334914460265620BFD75`

Confirmada por consulta subsequente ao BACEN, cuja resposta veio assinada pela Autoridade Certificadora do SERPRO. A partir daqui o BACEN conduz a análise e o PSP recebedor (ISPB 02038232) é acionado para bloqueio e devolução do valor.

6.2. Marcador de Fraude contra a conta recebedora

Identificador BACEN: `5ce23971-3942-4762-bd1d-aa0505946a31`
Status no BACEN: **REGISTERED** (registrado)
Alvo: CNPJ 58.269.513/0001-82 (JF Consultorias e Representação Comercial Ltda)
Tipo de fraude: SCAMMER_ACCOUNT (conta engajada em fraude)
Participante reportante: 46026562 (MONETARIE SCD)
Registro: 21/07/2026 14:18:48Z, CorrelationId `A20260721111848240460265623F4530`

O marcador sinaliza ao ecossistema PIX que o CNPJ recebedor está associado a fraude, reforçando a análise da recuperação e alertando demais participantes.

Base normativa: API DICT do BACEN, Recuperação de Valores (MED 2.0) e Marcação de Fraude, conforme https://www.bcb.gov.br/content/estabilidadefinanceira/pix/API-DICT.html.

7. Conclusão e recomendações

O evento se classifica como **movimentação originada por usuário administrador autenticado**, a partir da VPN corporativa da MonBank (endereço público real 200.155.150.126), e não como invasão de sistema por agente externo. Somente o PIX de R$ 200.000,00 efetivou; sobre ele já foi aberta a recuperação junto ao BACEN e registrado o marcador de fraude contra o recebedor.

Ações urgentes recomendadas:

1. Acompanhar a MED 2.0 `94889900-...` até o desfecho (bloqueio/devolução pelo PSP recebedor).
2. Definir formalmente as regras de segurança do ambiente, tornando o **MFA obrigatório** para administradores e para toda operação de money-path, e implantando alçada de aprovação (maker-checker) e limites por operador para PIX/TED de alto valor.
3. Revisar os acessos administrativos e o alcance da VPN da MonBank ao ambiente de produção da Monetarie.
4. Preservar as evidências deste relatório para eventual apuração formal e comunicação aos órgãos competentes.

Relatório produzido por análise técnica sobre registros de produção (somente leitura). Horários em UTC salvo indicação em contrário. Documento confidencial de uso interno da Monetarie.