# Beneficiary Change Request: Risks and Best Practices

Across markets and industries, fraud is increasing as perpetrators seek ever more creative and sophisticated means of achieving their ends. A beneficiary change request is a request to change the details of a beneficiary's account or accounts to which payments are made. A fraudster exploits weaknesses in a genuine change request process, changing genuine beneficiary account details to those of an account or accounts that he holds.

The rise in attempts to redirect payments from existing payment instructions by fraudulently changing bank details is one example of some of the sophisticated techniques fraudsters resort to. So how can you protect yourself against this threat to your security, and what might a typical fraud look like? Below we explore these in a little more detail.

### Recognise it for what it is...

Fraudsters thrive on being able to get past people by exploiting human psychology. What appears to be a legitimate wish to change secure information may be an illegitimate request to redirect payments from existing instructions. An attacker does this by passing off a real or forged company letterhead that they send to you as notification of a change to a beneficiary's banking details, or by posing as a new account manager before requesting changes. Both are frauds.

### Now adapt to tackle it head on...

The approaches taken by fraudsters may be ever-changing but that only makes it all the more important that you you frequently review your internal processes. Doing so gives you the opportunity to ensure that there are strong procedures in place to manage change requests to the payment details of beneficiary parties, procedures fraudsters won't be able to get past. The infographic here captures some of the things your can do right now to start.

### Good practices to help stop fraudulent beneficiary changes...

- Always create your own customer, supplier and payee profiles.
- Validate all change requests you receive, beyond the channel it came from.
- Independently confirm requests with established approved contacts to verify any asks.
- Confirm all agreements in writing with an established contact not with the requester.
- Make staff aware of fraud risks and what to do if they suspect fraud.
- Train staff to spot unexpected invoices or unusual payment requests.
- Use fraud-detection software to help identify risks as they emerge.
- Regularly review internal controls and procedures so they are fit-for-purpose.
- Send a small value test transaction to the new account and confirm receipt with the legitimate beneficiary.
- Require a maker/checker process for changing or adding beneficiaries.

## Red flags for fraudulent beneficiary change requests...

- Beware of even the slightest variations to email addresses and/or domain names ("spoofing" is where genuine email addresses are replicated in this way).
- Beware of requests to only contact suppliers via the numbers or contacts provided to you in received correspondence.
- Beware of requests for immediate or urgent payment changes, especially with plausible reasons for not being able to comply with your usual amendment procedures.
- Beware of publicly published information that might help fraudsters execute fraudulent beneficiary change requests, especially...
- Beware of sensitive information about suppliers published on websites or of employee details published on social networking sites.

Fraudsters will request beneficiary changes by email and phone, pretending to work for suppliers or associates.

### Keep this example in mind...

An accounts payable staff member receives an email from a supplier requesting a change of bank account details for his supplier.

The tone of the email is more formal than usual but, in accordance with company policy, the staff member replies that they require a signature verification callback.

The supplier responds that he is currently travelling and not available on the usual contact number. In his absence, though, he instructs the staff member to work with a colleague to make the beneficiary change. Soon after, this "colleague" calls accounts payable to verify the beneficiary change.

Once the beneficiary change is made, accounts payable receives an invoice from the supplier, which it processes and pays into the new bank account. A few days later, however, the usual contact at the supplier contacts accounts payable to confirm that not only did he not receive any payment, but he never requested a beneficiary change in the first place.

Here, the fraudster posing as the supplier contacted accounts payable initially by email. But fraudsters will request beneficiary changes over the phone too, pretending to work for known suppliers or associates. These attacks are precise, planned and well orchestrated. It's important to keep this in mind: that fraudsters will be patient and persistent, often making several attempts to successfully carry out the attacks they plan.

**Treasury and Trade Solutions**
**transactionservices.citi.com**



GRA29064 01/18