Ahead for Business

NatWest

Social Engineering

Vishing

- Contact is made by telephone
- Caller purports to be from your bank, the police or a fraud agency
- Purpose is to get you to reveal confidential information

Phishing

- Contact is made by email
- Sender impersonates well known companies such as banks
- Purpose is to get you to click on a link or attachment

NatWest

Vishing

- Contact is made by telephone
- Caller purports to be your bank, police or fraud agency
- Purpose is to get you to reveal confidential information

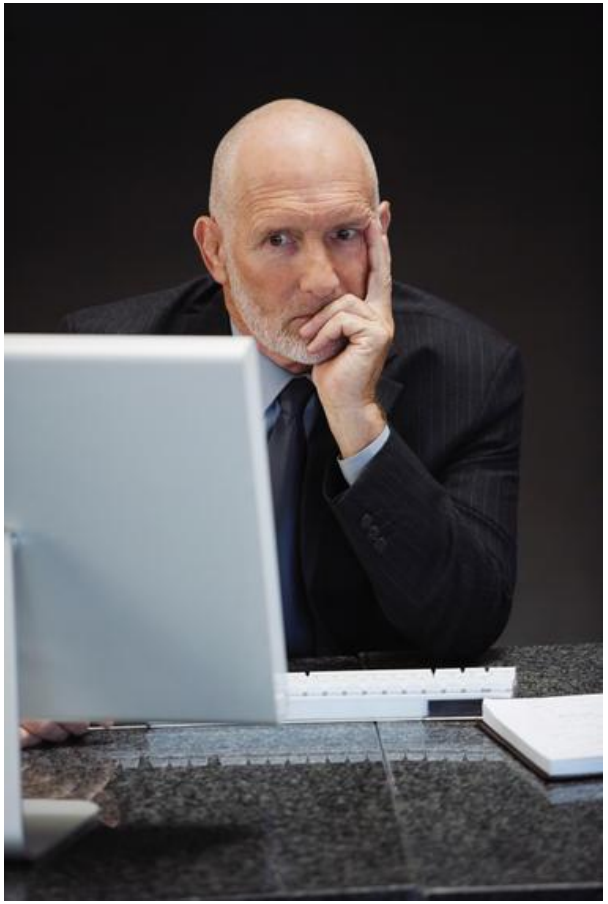
NatWest

Case Study – A re-enactment

- Large Corporate Client
- Call received regarding incoming payment
- Some information was provided by caller
- Caller suggested all payments were frozen
- Requested information from the client to ‘unfreeze’

Case Study – What was happening?

- High pressure situation
- Homework done
- Used information given to her
- Reference number given
- Telephone number given
- Line held open



Case Study – What happened next?

- 2 x £70,000
- 1 x £7,000,000
- One beneficiary account
- 10 transfers
- Bank actions
- Contact from the fraudster
- Police involvement - OCG identified

Phishing

- Contact is made by email
- Sender impersonates well known companies
- Purpose is to get you to click on a link or attachment

NatWest

Phishing – Email examples

‘There is a multi-media message available for you to view’

‘Confirmation of your recent booking is attached’

‘We could not deliver a parcel to you’

‘A complaint has been filed against you’

‘Receipt of online VAT submission’

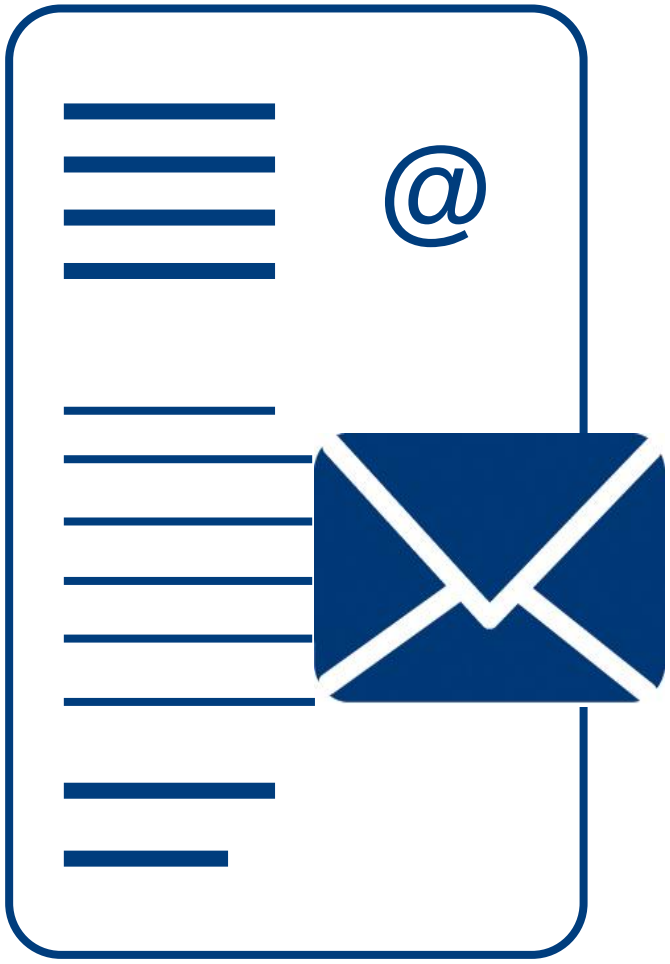
Phishing – Email spoofing

The email address can be a *direct** or *indirect*** version of a genuine email domain

The body content can be a replica of a genuine message or use our logos

Hyperlinks can be masked to show as something more genuine, such as rbs.co.uk.

Name of an employee, their position and/or department can be copied



*Direct spoofing is replicating domains that we own; for example: spoof@rbs.co.uk or fake@natwest.com.
** Indirect email domain spoofing uses a non-affiliated email domain but often a spoofed (friendly) 'From' field.

NatWest

Phishing – Case study

From: Bankline Administration [mailto:FAX.Bankline.Administration@rbs.co.uk]
Sent: 22 April 2013 12:23
To:
Subject: RBS Bankline Password Reset Form
Importance: High

Thank you for your telephone call.

Please find the Re-activation form attached, send one per user ensuring only one box is selected in section 3.

Please be aware when choosing a new pin and password for the service, it is important not to use pin/passwords that you have used before but to use completely different details.

If you require any further assistance then please do not hesitate to contact us on 0845 300 4108 or via www.rbs.co.uk and one of our associates will be happy to assist you.

Regards

Bankline Product Support

Reset Form.zip (22 B)

NatWest

Phishing – Case study

From: Bankline Administration [mailto:FAX.Bankline.Administration@rbs.co.uk]
Sent: 22 April 2013 12:23
To:
Subject: RBS Bankline Password Reset Form
Importance: High

Thank you for your telephone call.

Please find the Re-activation form attached, send one per user ensuring only one box is selected in section 3.

Please be aware when choosing a new pin and password for the service, it is important not to use pin/passwords that you have used before but to use completely different details.

If you require any further assistance then please do not hesitate to contact us on 0845 300 4108 or via www.rbs.co.uk and one of our associates will be happy to assist you.

Regards

Bankline Product Support

Reset Form.zip (22 B)

NatWest

Never, Never, Never

We will NEVER ask for your full pin and password to log in to online banking

We will NEVER ask you to provide PIN and password or smartcard codes over the telephone

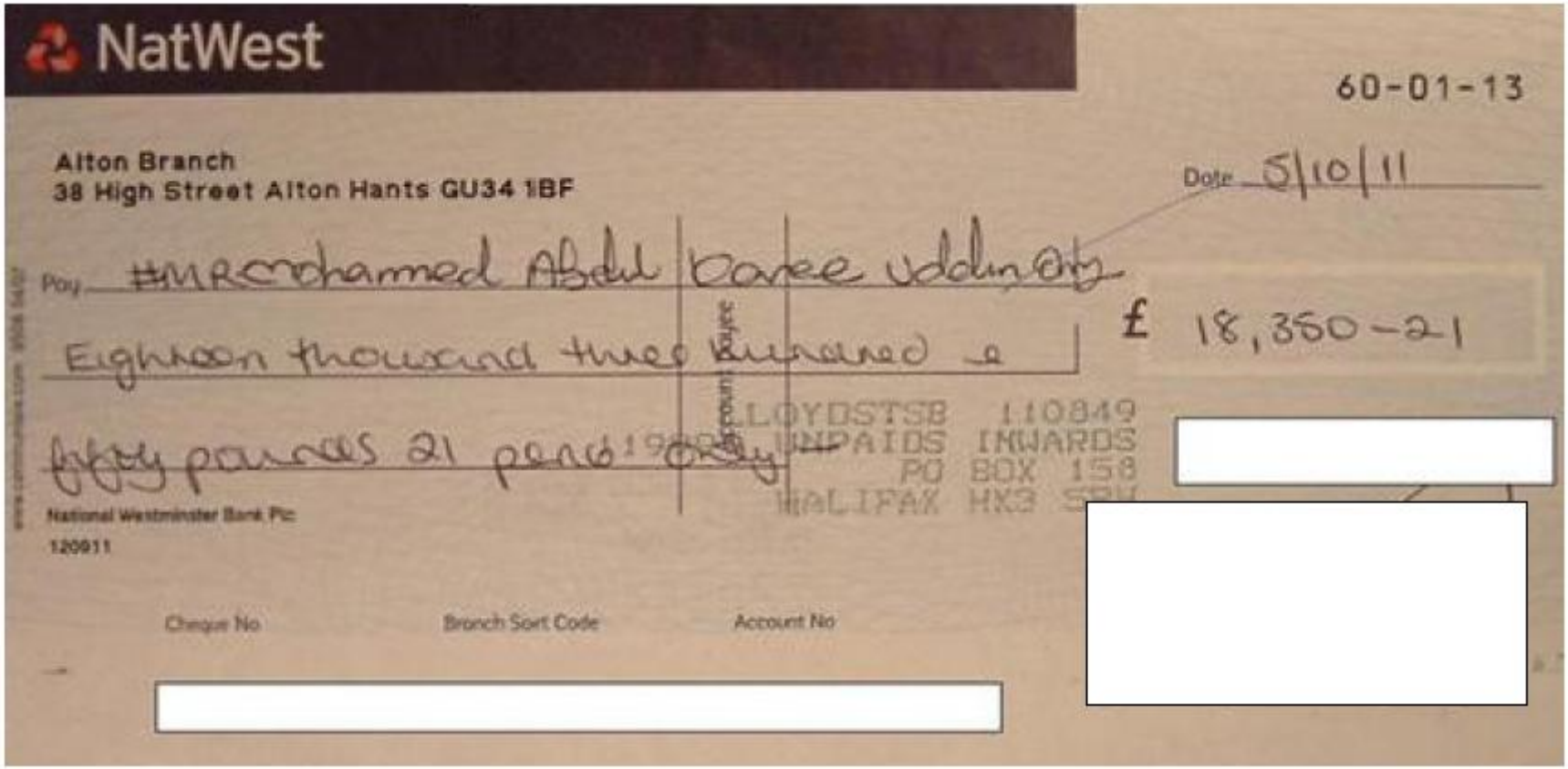
We will NEVER ask for any Smartcard codes to complete log-in; these are generally only used to authorise payments

Trusteer

We recommend you download Trusteer Rapport – FREE security software available from rbs.co.uk/onlinesecurity

NatWest

!SCAM! Altered cheque - Handwritten



NatWest

!SCAM! Cheque and payable orders fraud

Good housekeeping

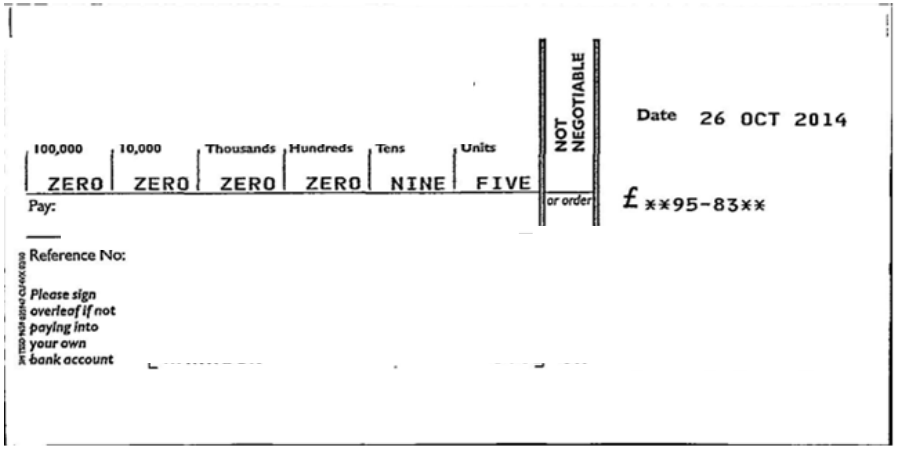
- Limit the number of books you hold
- Check the middle and back of book
- Store cheque books securely

When issuing cheques

- Do not leave any gaps
- Recorded and special delivery
- Where possible, include references

Reconciliation

- Reconcile frequently
- Reconciler should not be the issuer
- Verify why the cheque was issued



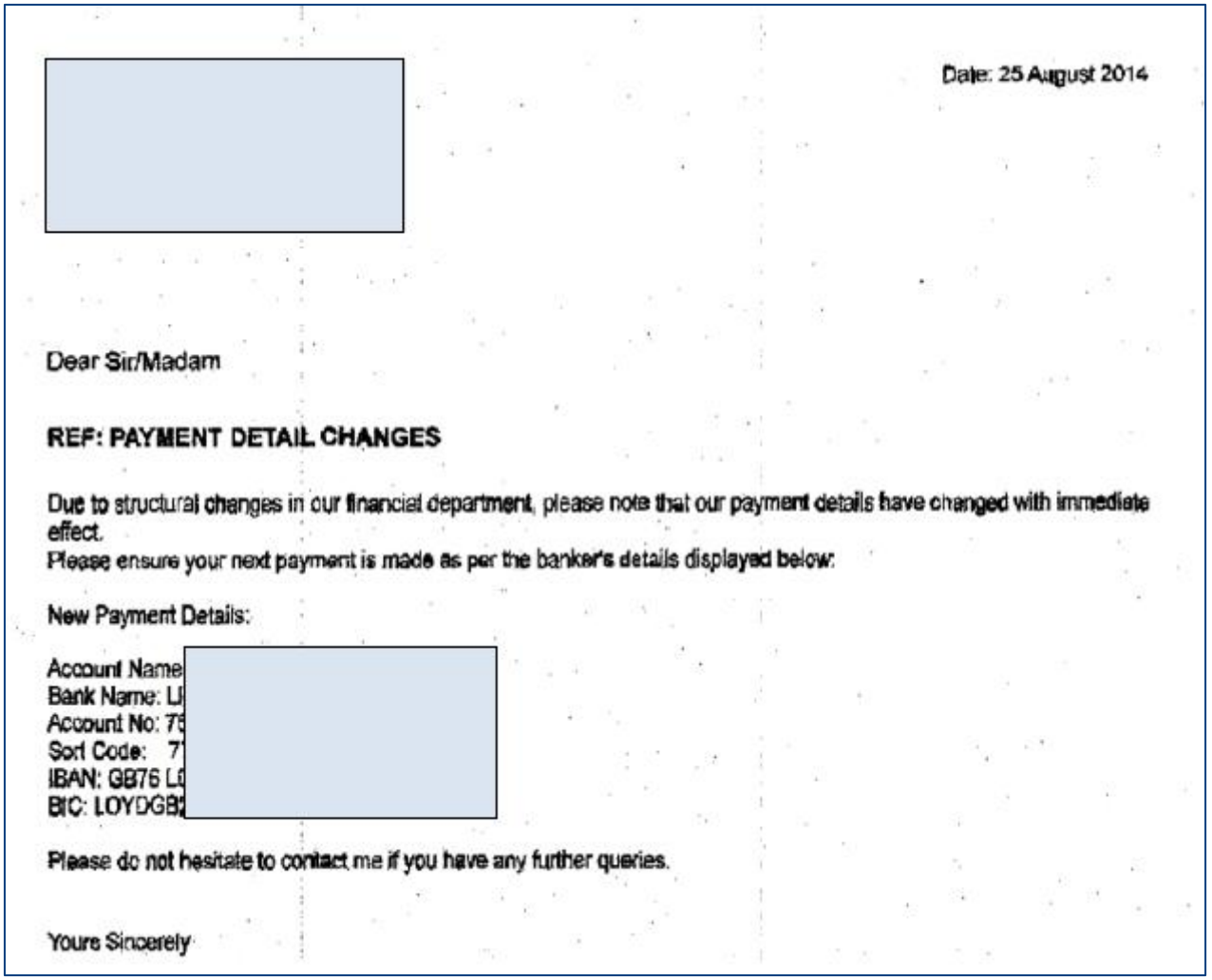
NatWest

!SCAM! Mandate Fraud

How does it work?
Change of bank details instruction is given – sometimes by phone initially
Following the phone call, a fax or email ‘confirmation’ may be received
It appears to be on headed paper or from a genuine email address
It may refer to genuine people within each business
Purpose is to get you to change the details you make payments to
This ensures future payments are now made to the fraudster

NatWest

!SCAM! Mandate Fraud



Date: 25 August 2014

Dear Sir/Madam

REF: PAYMENT DETAIL CHANGES

Due to structural changes in our financial department, please note that our payment details have changed with immediate effect.
Please ensure your next payment is made as per the banker's details displayed below:

New Payment Details:

Account Name:
Bank Name: LL
Account No: 75
Sort Code: 7
IBAN: GB76 LO
BIC: LOYDGB2

Please do not hesitate to contact me if you have any further queries.

Youre Sincerely

NatWest

!SCAM! Mandate Fraud

Mr J Singh
ABC Limited
8th Floor
Building A
Somewhere
Somehow

ABC Limited

Unit 1,
An Industrial Estate,
Somewhere,
Somehow
aboxy@abcltd.co.uk

Dear Mr Singh,

Further to our telephone conversation, please accept this letter as written confirmation of our change of bank details.

All future setlements should be made to -

Account number: 12345678
Sort code: 000000

I would be grateful if you could update your records without delay.

Please contact me directly on 07777 777777 should you have any queries.

With kind regards,

Amanda Boxy
Finance Manager, ABC Ltd

What can you do?
Check for irregularities
Contact the supplier using an independently sourced number
Confirm correct details with supplier before payment is made
Email confirmation of payments that have been made to the supplier
Undertake a proactive review of recent and pipeline requests
Speak with other employees responsible for this type of request

NatWest

In summary and Q&A

Security warning:

We will **never** ask for PINS, passwords or smartcard security codes over the telephone in any circumstances.

If in doubt, call the Bankline Helpdesk.

Only individuals who have authorised access to NatWest Bankline should proceed beyond this point. For the security of customers, any unauthorised attempt to access customer bank information will be monitored and may be subject to legal action.

NatWest