

Tools, Tips and Techniques to Mitigate Fraud

September 2017

Bank of America 
Merrill Lynch

Agenda

- Email Threats
- Establish Controls
- Fraud Invoice Schemes
- Reducing Risk

Bank
Merrill

Email Threats

Bank
Merrill

What it all Means

PHISHING

Infected files/malicious links sent through email

SPOOFING

Email messages with a forged sender address

SMISHING

Infected files/malicious links sent through SMS message

MASQUERADING

Attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification



Classic Phishing

- Looks like a legitimate correspondence from the company
- Wording does not have the level of refinement expected from an authentic company message
- Has an attention getter – high dollar amount of a cell bill in this example
- Embedded links activate malware download on your device
- Some individuals click on the links and may not even recognize they don't have a relationship with the company

CallMe.org | [Support](#) | [myCallMe Account](#)

Your wireless bill is ready to view

Dear Customer,

Your monthly wireless bill for you account is now available online.



Total Balance Due: \$1720.40

[Log in](#) to myCallMe to view your bill and make a payment. Or [register now](#) to manage your account online. By dialing *PAY (*729) from your wireless phone, you can check your balance or make a payment – it's free.

Smartphone users: [download the free app](#) to manage your account anywhere, anytime.

Thank you
CallMe Online Services
callme.org

Contact Us
[CallMe Support](#) – quick & easy support is available 24/7.

[Device Tutorials](#)
Information specific about your phone

[Smart Controls](#)
Block calls, set mobile purchase limits, manage usage, and more

[Payment Arrangements](#)
Explore your options for arranging a payment plan

PLEASE DO NOT REPLY TO THIS MESSAGE

[©2012 CallMe Intellectual Property](#). All rights reserved. CallMe, The CallMe logo and marks contained herein are trademarks of CallMe Intellectual Property. CallMe Inc. provides products and services under the CallMe brand.
[Privacy Policy](#)

[Get Piece of Mind](#)
Set up secure AutoPay from your checking account.
[Learn more](#)
[Go Paperless](#)
Save time, money and the environment.
[Learn more](#)
[Online Deals!](#)
Shop the Best Deals in your area for Phone, TV, Internet and Wireless.
[Learn more](#)

E-Mail Monitoring/Insertion

Is anyone monitoring your emails or that of the recipient?

1. Message between 2 companies on the payment of an invoice.
 - Payment received. Questioning payment on second invoice.
2. Research reveals payment on second invoice is legitimately owed.
3. Email Insertion
 - Reading the interaction between companies
 - Sees that a payment is going to be sent
 - Alerts sender something is wrong with primary bank account.
 - Funds need to be sent to an alternate account while bank is researching issue.
 - Salutation different than prior emails
 - Language not crisp
 - Uses Caps and alert phrases
4. Confirmation that payment was sent to the criminal's account.

4

From: Chris@othercompany.com
Sent: Wednesday, June 1, 2015 10:30am
To: Joe@mycompany.com
Subject: Invoice payment #R64274

Joe, Payment was sent. Let me know if you need the confirmation number.

From: Joe@mycompany.com
Sent: Wednesday, June 1, 2015 10:20am
To: Chris@othercompany.com
Subject: Invoice payment #R64278

Dear Chris,

Please pay attention to this mail, about payment there is now change in our bank account details . We received an alert from our BANK about present security challenges which they are faced with, noting that there were several unauthorized access and withdrawals to our company account . So presently our bank confirmed that we should STOP all incoming payments to the account until the bank complete their security update. Please send the payment to our subsidiary account.

Beneficiary Bank: ABCD Hong Kong
Beneficiary Name: EMCA (HK) Limited
Beneficiary Address: 10/GF, Superluck Ind. Centre Phase 3, 37 Sha Tsui Rd, Tsuen Wan
Account No: 073-029562-658
Bank Code: 003
SWIFT Code: ABCDHHKHHKH
Branch Address: 17 Queen's Road West, HK. Hong Kong
Thank you.

From: Chris@othercompany.com
Sent: Wednesday, June 1, 2015 10:10am
To: Joe@mycompany.com
Subject: Invoice payment #R64274

Joe,
I researched the invoices and you are correct. Found the second invoice R64274 . I will go ahead and process the payment for \$283,011.67 to the same account.

Thanks.

From: Joe@mycompany.com
Sent: Wednesday, June 1, 2015 9:45am
To: Chris@othercompany.com
Subject: Invoice payment #R64278

Hi Chris,
The payment mentioned below was well received. Thank you.
However, I found out you skipped one invoice R64274 which is referring to the shipping ticket #115320 (see attached). May I ask you if #115320 and #115317 were duplicated, because you paid R64278 referring to #115317. These two separate tickets for ROR-185 300lbs at the same PO number, but I received separately.

Please advise.
Joe

1

2

3

Some Phishing schemes involve mimicking internal emails.

- Based on easy to obtain information (Social media sites, Professional associations, company website) the perpetrator of fraud knows key players and their roles in your company.
- Domain names are registered that sound like your company; but involve intentional misspellings.
- Initial message is fake but appears to be coming from Senior executives within the company
- Focus on confidentiality and urgency

If you receive an email such as this:

- Contact the sender by an alternate method to validate the instruction
- Follow your authentication procedures
- Employ dual controls prior to making payment changes or processing payments
- Validate that correspondence is legitimate

From: Treasurer@mycompany.com
Sent: Tuesday, July 8, 2014 11:17am
To: chris.smith@mycompany.com
Subject: FW: Wire Transfer

This is the third one. We are pulling the confirmation now and will send to you.

From: Treasurer@mycompany.com
Sent: Wednesday, June 11, 2014 11:30am
To: chris.smith@mycompany.com
Subject: FW: Wire Transfer

FYI, this needs to get processed today. I checked with (insert name here) to get your help processing it along. I will assume we take care of any vendor forms after the fact. I can send an email directly to (insert name here) or let you drive from here. Let me know.

From: Treasurer@mycompany.com
Sent: Wednesday, June 11, 2014 9:59am
To: chris.smith@mycompany.com
Subject: FW: Wire Transfer

Process a wire of \$73,508.32 to the attached account information. Code it to admin expense. Let me know when this has been completed.

Thanks.

-----Forwarded message-----

From: CEO@rnycompany.com
Sent: Wednesday, June 11, 2014 6:45am
To: Treasurer@mycompany.com
Subject: Wire Transfer

Insert name (Treasurer),

Per our conversation, I have attached the wiring instructions for the wire. Let me know when done.

Thanks. Insert name, (CEO)

Look at the spelling of the words and names carefully

CEO@mycompany.com

CEO@rnycompany.com

Ransomware

Emerging fraud trend

Ransomware is a type of malware that restricts access to the infected computer system

- Demands ransom to remove the restrictions
- Some forms systematically encrypt files on the system's hard drive
- Difficult or impossible to decrypt without paying the ransom for the decryption key, some may simply lock the system and display messages to coax the user into paying
- Most ransomware enters the system through attachments to an email message

For consideration

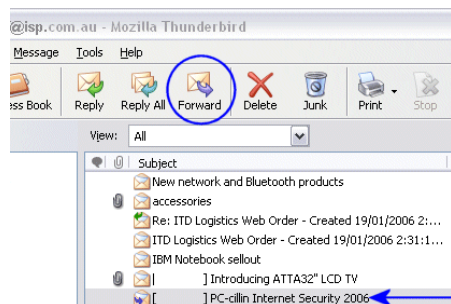
- Up to date anti-virus software
- Email gateway security products
- Employee education

Ransomware Brand Names





Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this second-factor authentication early in the relationship and outside the email environment to avoid interception by a hacker



Do not use the "reply" option to respond to an email with transaction activity or approvals for payments. Instead, use the "forward" option and either type in the correct email address or select it from the email address book to make sure real email address is used



Beware of sudden changes in business practices. For example, if suddenly asked to contact a representative at their personal email address when all previous official correspondence has been on a company email, verify via other channels that you are still in communication with your legitimate business associate

Fraudulent Invoice Schemes

Bank
Merrill

Fraudulent Invoices

Another trend impacting companies is the Fraudulent Invoice:

- It is a variation on the Phishing emails.
- Fraudster mails an invoice to the company; often addressed to the AP department
- Invoice has description of “Investment”
- Invoice usually includes remittance information including the account to which funds are to be paid

If you receive an Invoice such as this:

- Verify the company is an approved existing and current trading partner
- Verify it is for an actual purchase or work performed by the company
- Confirm the account on the invoice is what you have on file for the company
- Caution – do not add a new vendor, with a new account, and pay an invoice all in the same step

Ning Trade co. Ltd.

Invoice

To: ABC Company **Ship to:** Ning Trade co. Ltd. April 1, 2014

QUANTITY	DESCRIPTION	UNIT PRICE	PRICE
1	Investment	826.770€	826.770€

SEND PAYMENT TO :

Company: Ning Trade co. Ltd.
COUNTRY: CHINA
ACCOUNT: 156023820100
Swift: CZCB CN 2 X
Bank name: ZHEJIANG CHOUZHOU COMMERCIAL BANK CO LTD

SUBTOTAL	826.770€
SALES TAX	
TOTAL	826.770€

PAYMENT INSTRUCTIONS : QUICK SWIFT

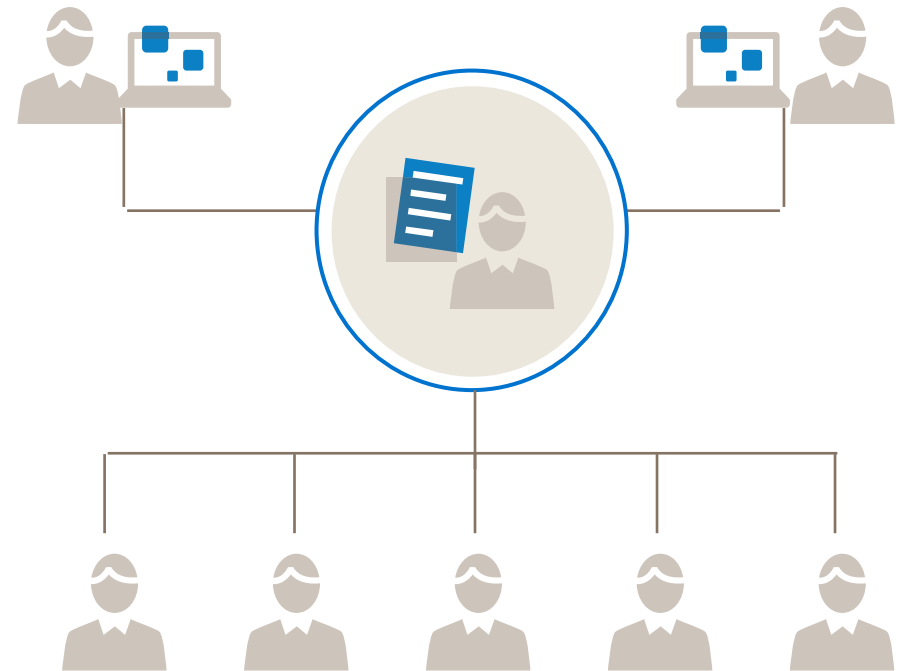
Ning Trade co. Ltd.
Register Number : 6065988 contact@ninqxiaenbei.trade.com

Reduce Risk Exposure

Bank
Merrill

Establish Segregation Of Duties

- If you're giving employees access to your accounts, limit access to sensitive functionality such as payment transactions.
- Set up your account so that any payments scheduled by one employee must be approved by a separate user.
- Set up approval limits around transactions. This can be done by transaction amount, type of transaction.
- Set up e-mail or mobile notifications to multiple members of your management team if any payments are initiated over a certain amount.
- Request notifications of any significant changes in your balances so that any problems can be addressed immediately.



Offline

- Have more than one person review bank reconciliations.
- Require more than one signature for checks over a set amount.
- Make sure there is dual control over the physical check stock.

Fraudsters are increasingly targeting companies that conduct online business, employing sophisticated tools designed to compromise your system and surrender control of your computer.

DOCUMENT an action plan now

Develop a sound internal process for transactions using the highest industry standards. Communicate and enforce the plan across the organization.

Create a separate plan to respond to an information compromise event. Keep in mind that an information breach may impact treasury activities.

EDUCATE your team on best practices

Establish other communication channels such as telephone calls, to verify significant transactions.

Do not use the "reply" option to respond to an email with transaction activity or approvals for payments.

TAKE ACTION

To understand actions you can take to help your company reduce the risks associated with fraud, review [online security tips and best practices](#) to get started today.



Bank experts and industry leaders share trends, tools and tactics for all business segments through video vignettes, case studies, podcasts, and featured white papers.

Learn more: [managing fraud risk website](#)

Consider solutions to help reduce your exposure to fraud.

- **Notifications**
- **Check and ACH Positive Pay**
- **Prepaid and Corporate cards**

#1

FRAUD PROTECTION AND IDENTIFY SAFETY CARD SOLUTIONS

Source: Javelin Strategy & Research, 2014

#1

AMONG ONLINE BANKING SERVICES PEERS

Fraud prevention and monitoring
Security administration and compliance
Source: Greenwich Associates Online Services Benchmarking, 2014

There is a Direct Correlation Between Employee Fraud Education and Decreased Number of Successful Fraud Attacks

Fraud Awareness Training

- Don't assume employees understand email and internet risks
- Set rules for personal internet usage – tell them why
- Articulate employee policies for the monitoring of their computer activity
- Formal training: don't rely only on your company's email or intranet to inform employees of email and internet policies and procedures
- Consider restricting the ability to load/download data on your company computers
- Show employees how to recognize threats and convey the consequences of those threats
- Be explicit about what to look for to identify a malicious email
- Explain that users will keep passwords in a secure place and not to share them with coworkers
- Provide frequent reports of new threats and statistics of how many viruses have been caught within your organization
- Never turn off security protection on your computer and stay current with updates
- Do not use your personal computer for company business
- Do not connect to the internet through suspect wireless networks (e.g., Wi-Fi from a café)
- Forward suspicious emails to the company's designated email security team (include the email address)
- Open only identifiable attachments from known sources. Financial institutions and government agencies never ask you to enter personal data, such as passwords, SSN, account numbers, etc

Appendix

Bank
Merrill

Malware

- Malicious Software; software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

DDOS

- Distributed Denial of Service – is an attack where multiple compromised systems – which are usually infected with a [Trojan](#) – are used to target a single system causing incoming traffic to flood the victim

Man In The Browser (MITB)

- A threat related to Man in the Middle where a web browser is infected by a proxy Trojan that allows web pages and transactions to be modified covertly, invisible to both the user and the application.

Phishing

- The act of attempting to acquire information such as usernames, [passwords](#), and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an [electronic communication](#). Phishing emails may contain links to websites that are infected with [malware](#).

SMishing

- Is a form of criminal activity using [social engineering](#) techniques. SMS phishing uses cell phone text messages to deliver the bait to induce people to divulge their personal information. The hook (the method used to actually capture people's information) in the text message may be a website URL, but it has become more common to see a telephone number that connects to an automated voice response system.

Glossary of Terms (Cont'd)

Trojan

- Malware Trojan that uses fake pop up ads to force the infected victim to buy malicious software to repair it or any type of drive-by downloads to load bad software

Keystroke Logging

- Is the action of recording or logging the keys struck on the a keyboard (to capture user IDs, passwords, etc.)

Spyware

- Is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge

Disclaimer

"Bank of America Merrill Lynch" is the marketing name for the global banking and global markets businesses of Bank of America Corporation. Lending, derivatives, and other commercial banking activities are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., member FDIC. Securities, capital markets, strategic advisory, and other investment banking activities are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and members of [SIPC](#), and, in other jurisdictions, locally registered entities. Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

This document is intended for information purposes only and does not constitute a binding commitment to enter into any type of transaction or business relationship as a consequence of any information contained herein.

These materials have been prepared by one or more subsidiaries of Bank of America Corporation solely for the client or potential client to whom such materials are directly addressed and delivered (the "Company") in connection with an actual or potential business relationship and may not be used or relied upon for any purpose other than as specifically contemplated by a written agreement with us. We assume no obligation to update or otherwise revise these materials, which speak as of the date of this presentation (or another date, if so noted) and are subject to change without notice. Under no circumstances may a copy of this presentation be shown, copied, transmitted or otherwise given to any person other than your authorized representatives. Products and services that may be referenced in the accompanying materials may be provided through one or more affiliates of Bank of America, N.A.

We are required to obtain, verify and record certain information that identifies our clients, which information includes the name and address of the client and other information that will allow us to identify the client in accordance with the USA Patriot Act (Title III of Pub. L. 107-56, as amended (signed into law October 26, 2001)) and such other laws, rules and regulations.

We do not provide legal, compliance, tax or accounting advice. Accordingly, any statements contained herein as to tax matters were neither written nor intended by us to be used and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed on such taxpayer.

For more information, including terms and conditions that apply to the service(s), please contact your Bank of America Merrill Lynch representative.

Investment Banking Affiliates are not banks. The securities and financial instruments sold, offered or recommended by Investment Banking Affiliates, including without limitation money market mutual funds, are not bank deposits, are not guaranteed by, and are not otherwise obligations of, any bank, thrift or other subsidiary of Bank of America Corporation (unless explicitly stated otherwise), and are not insured by the Federal Deposit Insurance Corporation ("FDIC") or any other governmental agency (unless explicitly stated otherwise).

This document is intended for information purposes only and does not constitute investment advice or a recommendation or an offer or solicitation, and is not the basis for any contract to purchase or sell any security or other instrument, or for Investment Banking Affiliates or banking affiliates to enter into or arrange any type of transaction as a consequent of any information contained herein.

With respect to investments in money market mutual funds, you should carefully consider a fund's investment objectives, risks, charges, and expenses before investing.

Although money market mutual funds seek to preserve the value of your investment at \$1.00 per share, it is possible to lose money by investing in money market mutual funds. The value of investments and the income derived from them may go down as well as up and you may not get back your original investment. The level of yield may be subject to fluctuation and is not guaranteed. Changes in rates of exchange between currencies may cause the value of investments to decrease or increase.

We have adopted policies and guidelines designed to preserve the independence of our research analysts. These policies prohibit employees from offering research coverage, a favorable research rating or a specific price target or offering to change a research rating or price target as consideration for or an inducement to obtain business or other compensation.

Copyright 2015 Bank of America Corporation. Bank of America N.A., Member FDIC, Equal Housing Lender.