Masquerading

David Pollino, SVP, Fraud Prevention Officer, Bank of the West

Cybersecurity Essentials – E13

Session Description

David Pollino will discuss solutions to the many security risks based on his experience with responding to a large number of fraud schemes and breaches that result in ACH fraud, wire fraud, and credit card fraud. Being prepared to proactively detect, respond and educate customers is critical. David will discuss examples and risks can be mitigated by the impacted organization.

Session Objectives:

1. Mitigation of Breaches
2. Finance Security Issues
3. Cybersecurity Awareness

About the Speaker

David Pollino

SVP, Fraud Prevention Officer, Bank of the West

David Pollino, SVP, Fraud Prevention Officer for Bank of the West, is responsible for fraud prevention oversight and education at the bank. Pollino was recently named a top ten influencer by Bank Information Security.

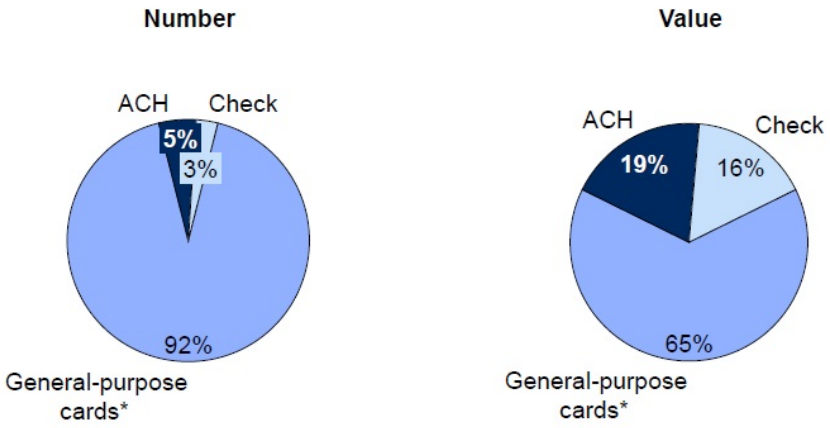
Prior to joining Bank of the West, Pollino served in senior fraud prevention positions for Wells Fargo, Washington Mutual, and Charles Schwab. During his career, Pollino has also worked as an information security consultant at @stake and UUNET advising Fortune 100 companies on information security issues.

Pollino is the author of RSA Press: Wireless security, The Hacker's Challenge Books 1, 2 and 3, and Hacking Exposed: Wireless.

Top 5 Fraud Threats

1. Card fraud
2. Online threats
3. Customer scams
4. New account
5. Internal Fraud

Exhibit 20: Distribution of unauthorized transactions (third-party fraud) in 2012



Figures may not add due to rounding.

*General-purpose cards include credit, debit, and prepaid purchases as well as ATM withdrawals.

https://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf

Know Your Enemy

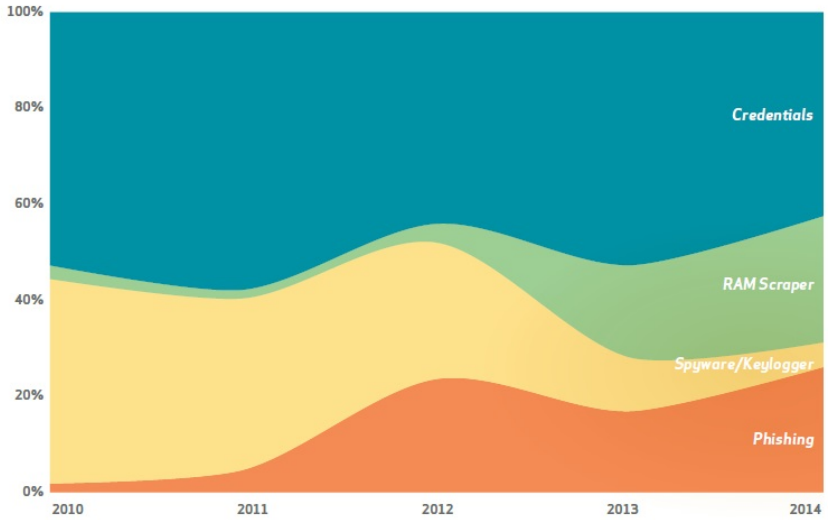
Principle 6 - The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

- **Nation-states and spies** — Hostile foreign nations who seek intellectual property and trade secrets for military and competitive advantage. Those that seek to steal national security secrets or intellectual property.
- **Organized criminals** — Perpetrators that use sophisticated tools to steal money or private and sensitive information about an entity's consumers (e.g., identity theft).
- **Terrorists** — Rogue groups or individuals who look to use the Internet to launch cyber attacks against critical infrastructure, including financial institutions.
- **Hacktivists** — Individuals or groups that want to make a social or political statement by stealing or publishing an organization's sensitive information.
- **Insiders** — Trusted individuals inside the organization who sell or share the organization's sensitive information

Principle 13 - The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

Source: COSO

Card Fraud – 2015 Verizon Breach Report

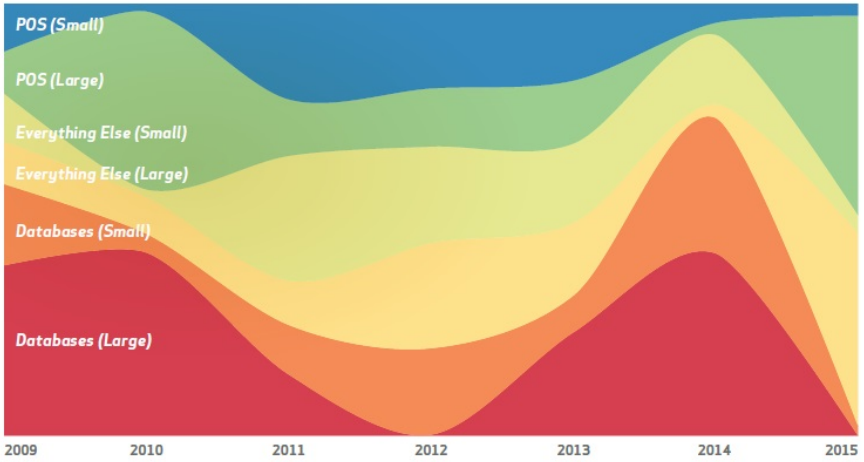


Ram scrapers

- "Your cash register has a virus"

Large Companies

- Big push before EMV



40 Yep, we did. That's how we roll. But, we're *really* fun at parties. Honest.

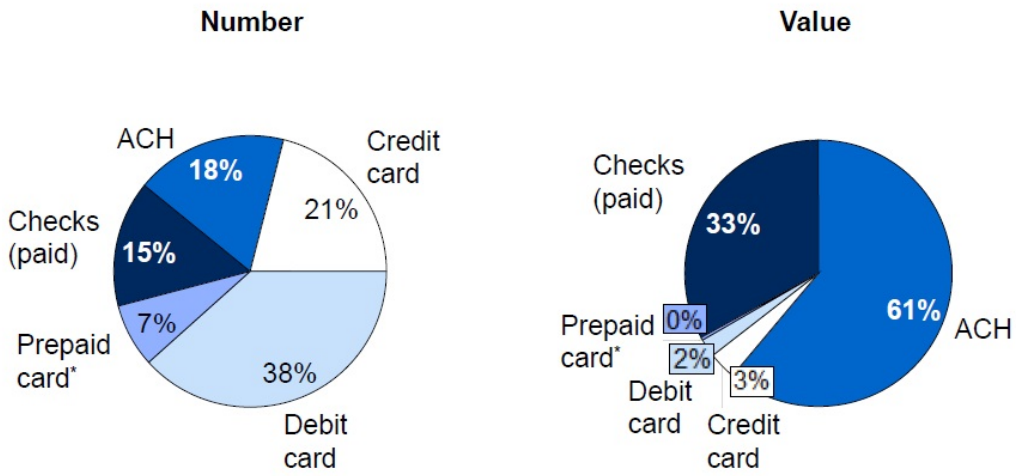
2015 DATA BREACH INVESTIGATIONS REPORT

Current State – ACH Fraud

- "Cards are typically used for point-of-sale (POS) transactions largely because of their convenience, while ACH payments tend to be used primarily for bill payment, payroll, and other larger-value transactions."

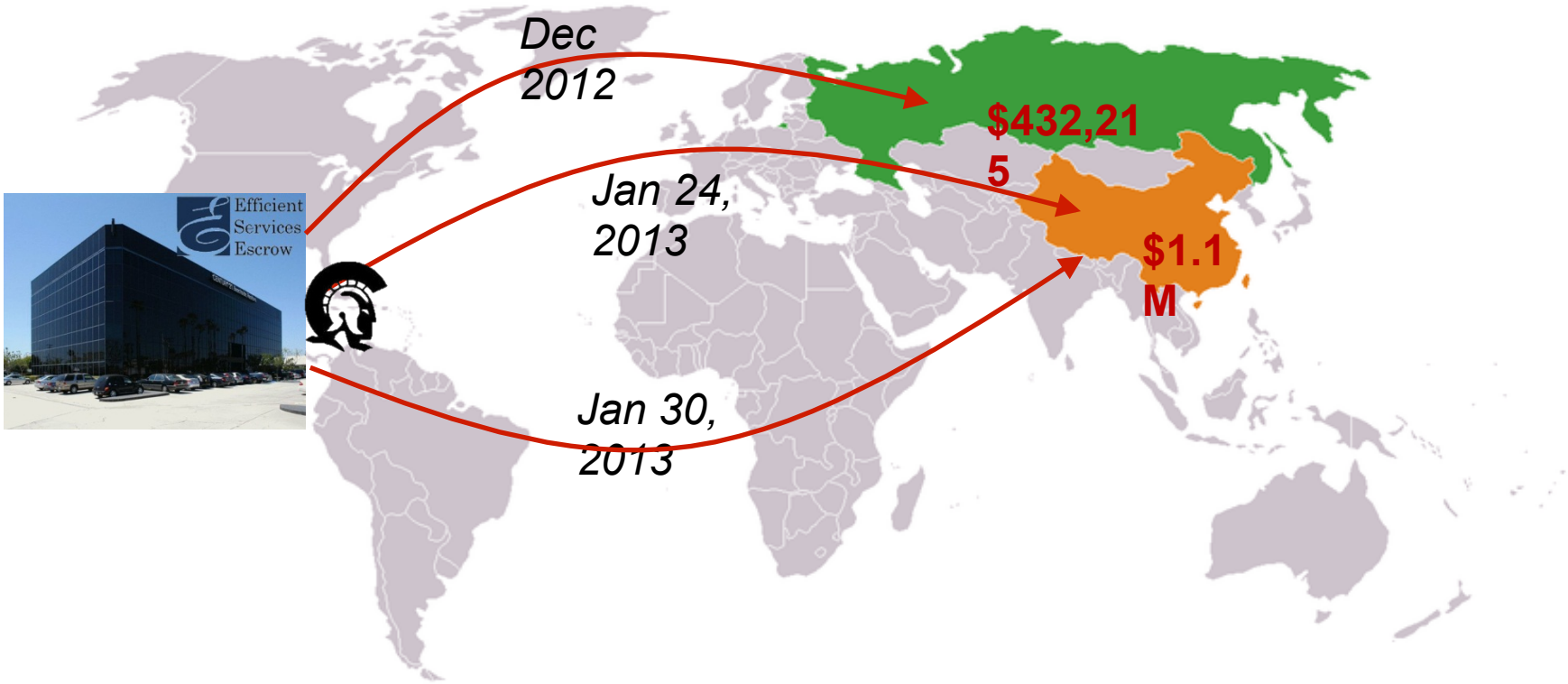
- Current Schemes
  - Online Account Takeover
  - Bill payment fraud
  - Peer to peer payments
  - Masquerading

Exhibit 3: Distribution of noncash payments in 2012



Source: https://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf

The Case of Efficient Services Escrow Group



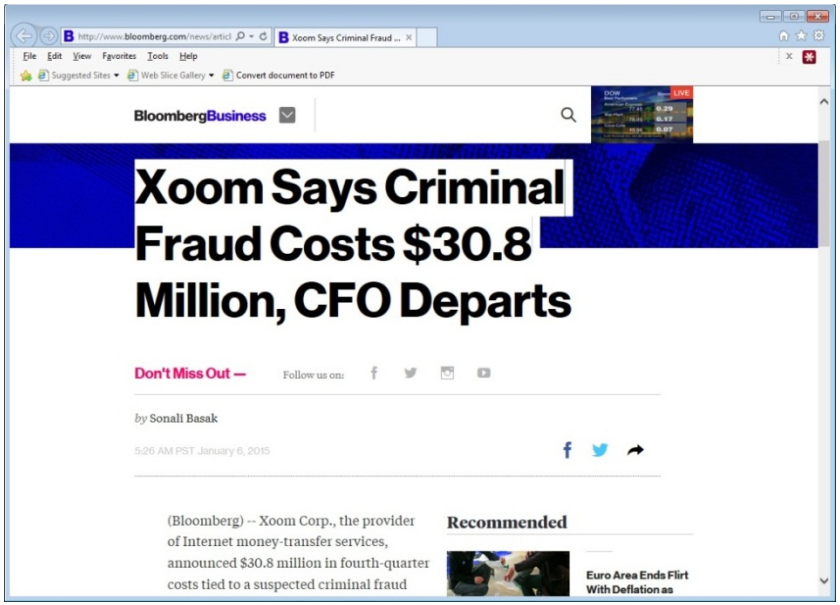
A suspected Trojan allowed hackers access to Efficient Services Escrow Group's computers. The hackers remotely initiated wire transfers to Russia and China on three separate occasions totaling $1.5 million.

Source: Krebs on Security; "$1.5 million Cyberheist Ruins Escrow Firm," http://krebsonsecurity.com/2013/08/1-5-million-cyberheist-ruins-escrow-firm/, August 7, 2013.

The Case of Efficient Services Escrow Group

- Efficient Services Escrow recovered only half of the funds and in March 2013, the firm was shut down by the California Department of Corporations.

- While the downfall of Efficient Services Escrow may have been due to its own shortcomings, the case sheds light on inadequacies of its Bank's security.



Source: Krebs on Security; "$1.5 million Cyberheist Ruins Escrow Firm," http://krebsonsecurity.com/2013/08/1-5-million-cyberheist-ruins-escrow-firm/, August 7, 2013.

What is Masquerading?

- Masquerading is a combination of social engineering and a confidence scam, using high-tech tools.
- A criminal impersonates a high-level executive at a company, often the CEO, and sends an email that looks like it came from that person, or calls, spoofing the executive's phone number.
- The attacks are waged against the bank's commercial customers, not the bank itself
- Attacks may include Spear-phishing, to takeover a legitimate e-mail account
- Then the criminal gets others in the organizations to do something, such as send a wire transfer or make an automated clearing house payment.
- The funds ultimately end up in a bogus account set up by the fraudster(s).

Masquerading Scheme Commonalities

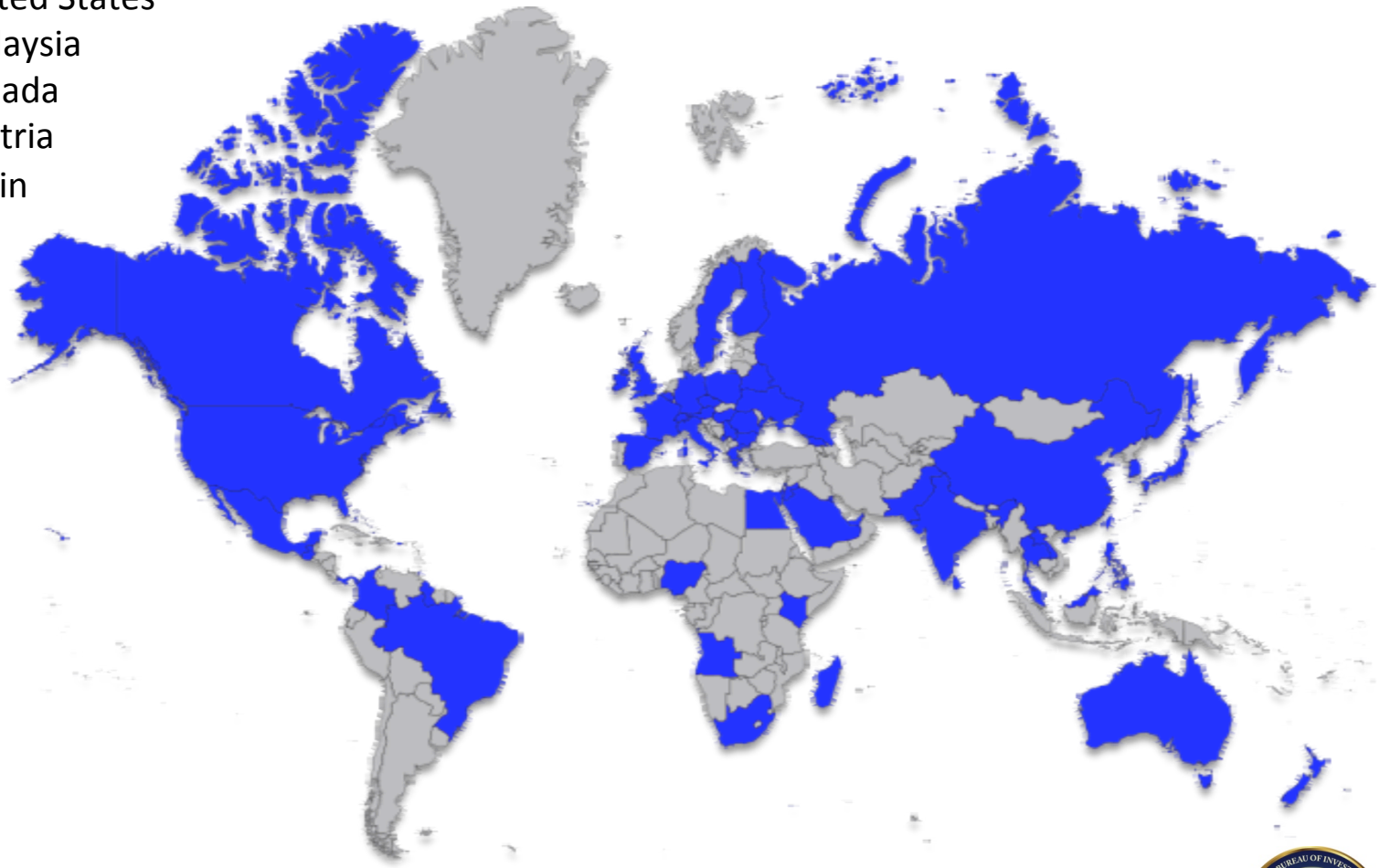
- Victims are generally from the United States, England and Canada, although there have been complaints from other countries such as Belgium.
- Victim businesses often trade internationally, usually through China.
- Most victims reported wire transfers are common business practice, so conducting transfers, including those for high-dollar amounts, is not unusual.
- Many victims receive fraudulent e-mail requests to transfer funds from an AOL, Gmail, or Hotmail address. However, there has been an increase in fraudulent transfers conducted through computer intrusion.
- Transfers traced by the victim's fraud department mainly lead to Asian banks in China or Hong Kong. However, transactions with banks in South Africa, Turkey and Japan have also been reported.

Source: http://www.ic3.gov/media/2014/140627.aspx

BEC Victims by Country

Top 5 Countries by Loss

1. United States
2. Malaysia
3. Canada
4. Austria
5. Spain



Masquerading Loss Statistics

The scam has been reported in all 50 states and in 79 countries. From October 2013 through August 2015, total losses reported amount to over $1.2 billion:

- Total U.S. Victims: **7,066**
- Total U.S. exposed dollar loss: **$747,659,840.63**
- Total non-U.S. victims: **1,113**
- Total non-U.S. exposed dollar loss: **$51,238,118.62**
- Combined victims: **8,179**
- Combined exposed dollar loss: **$798,897,959.25**

The FBI anticipates loss amounts and number of victims will continue to increase

Source: http://www.ic3.gov/media/2015/150827-1.aspx

Masquerading – Versions of the Scam

Based on complaints reported to IC3, there are four versions of this scam:

Version 1

A business, which often has a long standing relationship with a supplier, is asked to wire funds for invoice payment to an alternate, fraudulent account. The request may be made via telephone, facsimile or e-mail. If an e-mail is received, the subject will spoof the e-mail request so it appears very similar to a legitimate account and would take very close scrutiny to determine it was fraudulent. Likewise, if a facsimile or telephone call is received, it will closely mimic a legitimate request. This particular version has also been referred to as "The Bogus Invoice Scheme," "The Supplier Swindle," and "Invoice Modification Scheme."

Version 2

The e-mail accounts of high-level business executives (CFO, CTO, etc.) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is normally responsible for processing these requests. In some instances a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank "X" for reason "Y." This particular version has also been referred to as "CEO Fraud," "Business Executive Scam," "Masquerading," and "Financial Industry Wire Frauds."

Version 3

An employee of a business has his/her personal e-mail hacked. Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee's personal e-mail to multiple vendors identified from this employee's contact list. The business may not become aware of the fraudulent requests until they are contacted by their vendors to follow up on the status of their invoice payment.

Version 4

Victims report being contacted by fraudsters, who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam may occur at the end of the business day or work week or be timed to coincide with the close of business of international financial institutions.

Source: http://www.ic3.gov/media/2015/150827-1.aspx

Masquerading Awareness: BOTW Blog

BANK OF THE WEST

THE BLOG

5 questions that can help you prevent wire fraud

Category: Your Business | **Published:** 04/14/14 | **Share:**

Posted by David Pollino
Fraud Prevention

Wire fraud is a growing concern for businesses that can be difficult to detect before the damage is done.
Here is a common fraud scenario:

An employee receives an email purportedly from the CFO of the company requesting an immediate wire transfer from the business's bank account to an overseas account. The employee initiates and approves the outgoing wire transfer, and several thousand dollars are sent from the business's bank account. Unbeknownst to the

What your business may learn from the alleged Xoom Corp. fraud

Category: Your Business | **Published:** 01/07/15 | **Share:**

Posted by David Pollino
Fraud Prevention

Here's a multi-million-dollar reminder of the potential risks
fraud scheme known as masquerading: Xoom Corp. On D
determined that it had been the victim of a criminal fraud,
using employee impersonation to target the company's fin
them into transferring $30.8 million to overseas accounts.

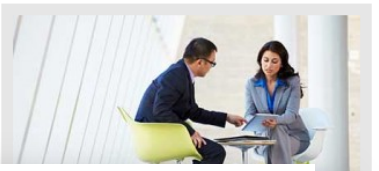
6 tips to protect against new cyber threat: masquerading

Category: Your Business | **Published:** 07/26/14 | **Share:**

Posted by David Pollino
Fraud Prevention

Wire fraud against businesses is taking on a new form. There's an emerging
that I've begun referring to as "masquerading."

d those of us
ndustry late
ed reports of
rading, in
ate an
ny to



Social-networking sa
business

Category: Your Business | **Published:** 10/0

Posted by David Pollino
Fraud Prevention

About 7% of persons age 16 or older were victims of identity theft in 2012, according to federal data. That's a one in 14 chance of being a victim.

The more you, your business, and your employees share publicly on social networks — even if it's posting a photo a squash blossom pizza you had while dining out — the easier it is for criminals to take and use your personal information. All the information you share is potentially useful to thieves involved in identity theft, fraud, impersonation, and

6 ways to help protect against the spreading threat of masquerading

Category: Your Business | **Published:** 05/21/15 | **Share:**

Posted by David Pollino
Fraud Prevention

It looks like masquerading — a type of wire fraud that is proving particularly difficult to thwart — may become a $1 billion industry this year.

Consider these possible examples:

- Xoom Corp. recently disclosed it lost $30 million through fraudulent money transfers.
- Ryanair disclosed it lost $5 million.
- Scoular Co., an Omaha-based commodities trading company, reportedly lost $17 million in an international email fraud scam.

Fraud Education in the Media

Fortifying Your Business: Bank of the West Manufacturing Report Highlights Fraud and Security Issues and Provides Preventative Measures for Small and Midsized Businesses

Second in Series of Manufacturing Papers Reveals Key Security Vulnerabilities

Share +1 Pin it

SAN FRANCISCO, Aug. 27, 2015 /PRNewswire/ -- Bank of the West announced today the publication of ***"Fortifying Your Business: Fraud and Security Measures for U.S. Manufacturers,"*** a paper by David Pollino, fraud prevention officer at Bank of the West, and the second in a series addressing challenges and opportunities that small and midsized manufacturers face. The report highlights threats manufacturers should be aware of, as well as measures that business owners can take to prevent them.

'Masquerading': New Wire Fraud Scheme

Bank of West Exec Offers Customer Protection Insights

By Tracy Kitten, July 28, 2014. Follow Tracy @FraudBlogger

A new impersonation scheme is taking aim at business executives to perpetuate ACH and wire fraud, says Bank of the West's David Pollino, who explains steps institutions should take now to protect their customers.

Federal a
attack, wh
espionage

BANK INFO SECURITY®

Biz Email Fraud Could Hit $1 Billion

Fighting New Wire Fraud Method Now a Top Priority for Banks

Tracy Kitten (FraudBlogger) · May 28, 2015 0 Comments

Wire fraud perpetrated via business email compromises has quickly become a top concern for banking institutions. **David Pollino**, bank fraud prevention officer at Bank of the West, now predicts wire fraud losses in the U.S. linked to such "masquerading" schemes could exceed $1 billion this year.

btn BANK TECHNOLOGY NEWS

This Banker Is on a Mission to Warn About 'Masquerading' Scams

by PENNY CROSMAN
AUG 1, 2014 1:30pm ET

PRINT
EMAIL
REPRINTS
COMMENT
TWITTER
LINKEDIN
FACEBOOK
GOOGLE+

David Pollino, a fraud prevention officer at Bank of the West, has been losing sleep lately over a type of cyberfraud for which he's coined a term — masquerading.

Masquerading is a combination of social engineering and a confidence scam, using high-tech tools. A criminal impersonates a high-level executive at a company, often the CEO, and sends an email that looks like it came from

Criminals Posing as CFOs to Commit Wire Fraud

They hack into companies' email, pretend to be senior executives and direct employees to make bogus financial transactions.

David McCann

August 13, 2014 | CFO.com | US

SHARE Share 7 Share 1 Share 2 Tweet 14

A new, fast-proliferating type of online fraud is posing yet another security threat to small and large companies alike. Bank of the West, which is taking a leadership role in publicizing the threat, calls it "masquerading."

It's a twist on a fraud attempt that became common in 2012, in which criminals hacked into companies' email or financial systems for purposes of altering communications between corporate executives and financial institutions. Now the bad guys have upped the ante by issuing

Fraud Education on Social Media

Bank of the West
January 6 ·

Do you know the signs of a masquerading scam? Find out in this short video.
http://gowe.st/Masquerading

Bank of the West @BankoftheWest · Jan 10
A masquerading scheme is one way confidentiality may backfire in your business. More from @DavidPollino: gowe.st/3q8l

Bank of the West @BankoftheWest · May 19
Alert: Fraudsters can take over or impersonate business emails to conduct wire fraud. Know the common signs: gowe.st/fbjc

Bank of the West @BankoftheWest · May 13
Do you know what masquerading is and how you may avoid it? Useful fraud info and tips: gowe.st/h5k5

Bank of the West @BankoftheWest · Jan 9
New from @davidpollino: How to ID & help prevent biz fraud known as #masquerading: gowe.st/Masquerading

Bank of the West @BankoftheWest · Sep 1
#Masquerading = "global fraud trend" with $1.2B in losses in under 2 years. @DavidPollino talks to @bankinfosecurity: bit.ly/1PJxr1P

Bank of the West @BankoftheWest · Jan 6
A multi-person approval process for high-dollar transactions could help protect against a new kind of #biz fraud. gowe.st/Masquerading

Bank of the West @BankoftheWest · Aug 7
Another costly example of the masquerading threat. @DavidPollino's 6 tips for protection: blog.bankofthewest.com/6-ways-to-help… twitter.com/briankrebs/sta…

Bank of the West What's one way to help prevent masquerading, a new type of business fraud? David Pollino explains in this :60 Security Download. https://lnkd.in/bavByaM

:60 Security Download: Masquerading
gowe.st · What is masquerading, and how can you help prevent it? Bank of the West's David Pollino offers tips in this short video.

Bank of the West @BankoftheWest · Sep 10
Are you surprised by the number of companies that were targets of masquerading scams? Report: GoWe.st/mfgsecurity

In 2015, for the third consecutive year, three in five companies were targets of payments fraud.

BANK OF THE WEST
BNP PARIBAS GROUP

Source: Association for Financial Professionals

Tips for Prevention

1. Confirm that any request to initiate a wire is from an authorized source within the company.

2. Double- and triple-check email addresses to help ensure messages are not coming from a fraudulent domain with a slightly different address than your company's domain.

3. Slow down. Be on high alert for possible fraud anytime wire transfer instructions include tight deadlines.

4. Be suspicious of requests for confidentiality. Whenever wire transfer instructions specify to keep the transaction secret, you should verify the legitimacy of the source of this request. Speak to the executive or manager requesting the transaction by phone or in person. If you still have doubts, speak to another senior executive.

5. Similar to checks for paying large purchase orders, wire transfers over a certain dollar threshold may be matched to a reference number to help ensure they are linked to an approved purchase or service.

6. Use two-factor authentication to verify vendor changes and transfer requests.

ACH / Card Fraud Future

- ACH payments continue to grow
- EMV will make an impact
  - Increase in fraudulent ACH payments
  - CNP fraud will increase
  - New account abuse
  - Attack of contact center
- Same day payments
  - Low dollar, high frequency
  - Mobile based payments
  - Similar to ApplePay?

Questions?

Thank you

Speaker Details	
Company	Bank of the West
Title	SVP, Fraud Prevention Officer
Facebook URL	https://www.facebook.com/BankoftheWest
LinkedIn URL	https://www.linkedin.com/company/bank-of-the-west
Twitter URL	https://twitter.com/bankofthewest
YouTube	https://www.youtube.com/user/BankoftheWest
E-mail	David.Pollino@bankofthewest.com
Website	http://blog.bankofthewest.com/author/pollino_david/