Creating an Effective Fraud Awareness Program

David Pollino, Title, Bank of the West

Professional Strategies – S13

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Agenda

- Why do you need customer awareness?
- How is it done today?
- Can we use social media?
- Are we really being effective?

WHY DO YOU NEED CUSTOMER AWARENESS?

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

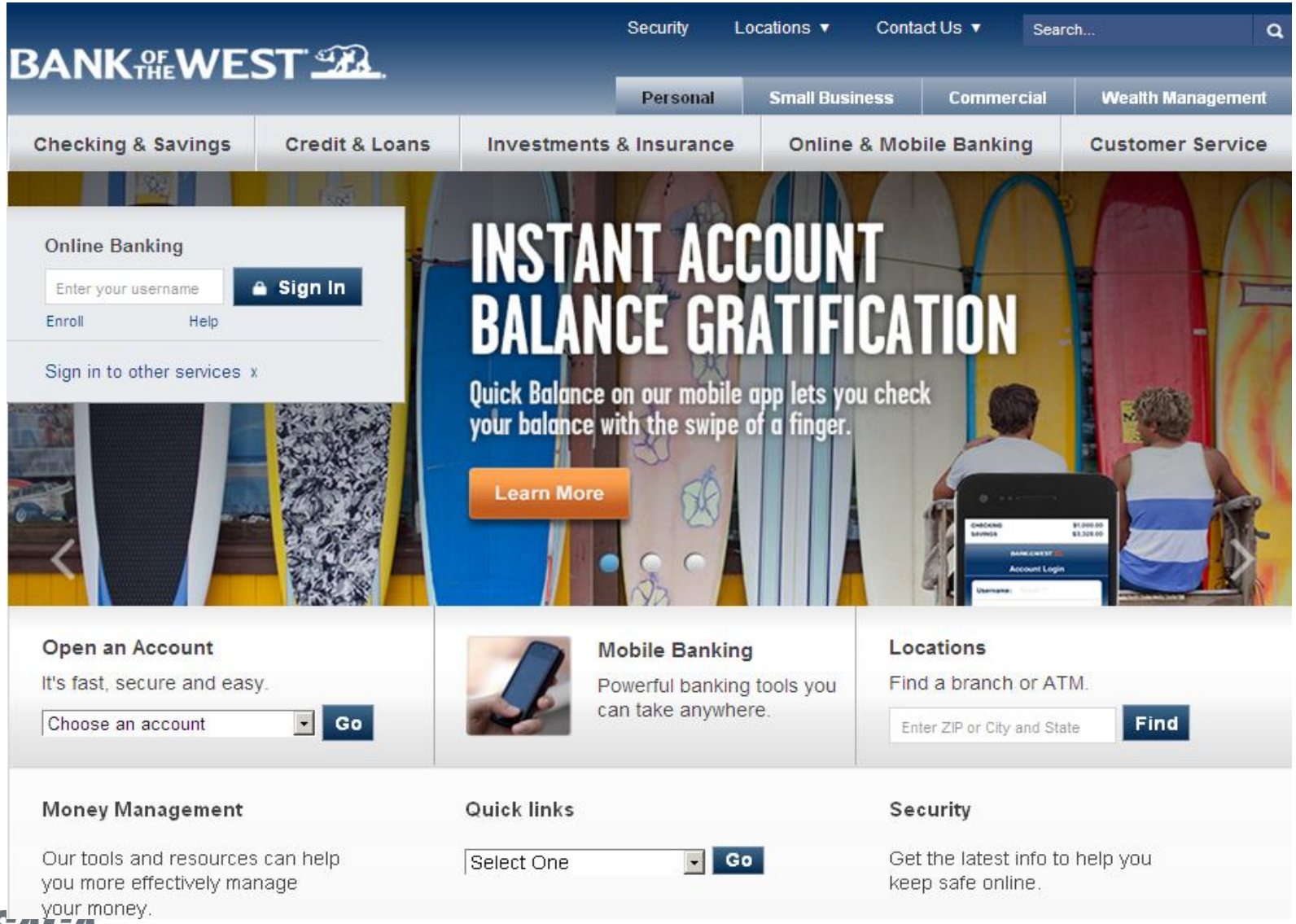
The Need

- Partnering with customers makes good business sense
  - Maintain customer trust
  - Have an ongoing dialog
- FFIEC relevant guidance:
  - "Management should implement a customer awareness program and **periodically evaluate its effectiveness**."
  - "… institutions should perform periodic risk assessments and adjust their control mechanisms as appropriate in response to changing internal and external threats."
  - "Financial institutions should review and update their existing risk assessments as new information becomes available, prior to implementing new electronic financial services, **or at least every twelve months**."

Source: FFIEC – 2005 / 2011 Authentication in and Internet Banking Environment

HOW IS IT DONE TODAY?

Most Common Method: Public Web Site



Broadcast / Splash Message

CREATED: 2012-12-20 16:21:27 PM

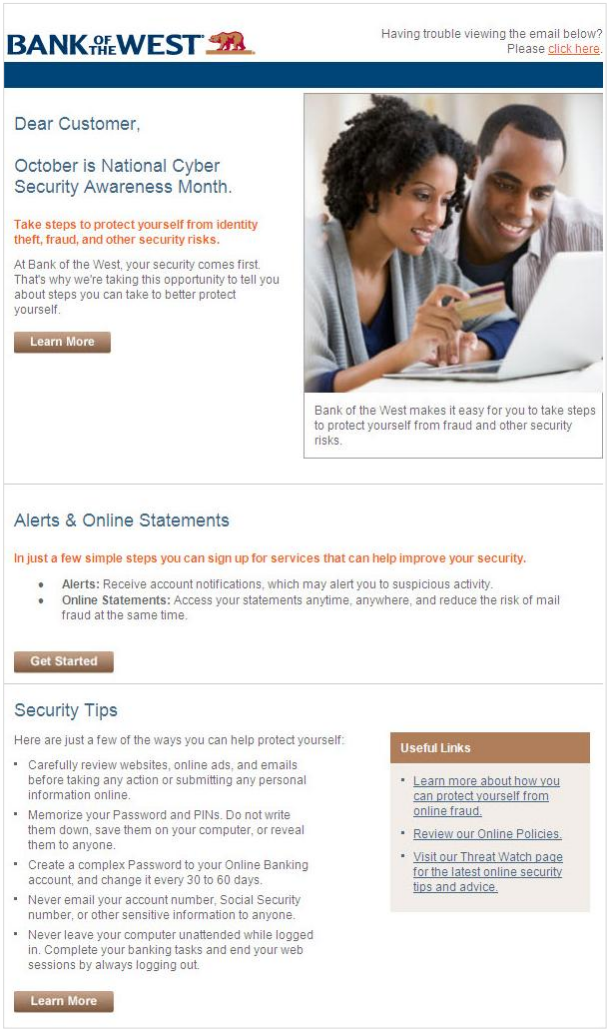
SUBJECT: Safe and Secure Computing Habits

During this busy time of year we want to remind you to practice safe and secure computing habits throughout the holiday season. We have been alerted to an increase in fictitious websites seeking security information. The bank will never solicit information requesting user id and passwords or other security information. Do not respond to requests asking for your user login credentials. Always report any suspicious requests and/or suspicious activity immediately to Cash Management Customer Service at 800-400-2781 or abuse@bankofthewest.com. We hope everyone will have a safe, secure and happy holiday season!

In the event that any customers inquire to you about protection from such phishing attempts, you can inform them about our free Trusteer Rapport service. Trusteer provides warnings in the event a customer is being subjected to a fictitious web site – and other on-line security capabilities. If the customer has not downloaded Trusteer already, please have them contact their assigned CCS Specialists for assistance on this matter. Information on Trusteer and downloading capability can be found on the Bank of the West web site at the following link:

https://www.bankofthewest.com/campaigns/online-security/rapport-security.html

News Letters / Handouts



BANK OF THE WEST

Having trouble viewing the email below? Please click here.

Dear Customer,

October is National Cyber Security Awareness Month.

Take steps to protect yourself from identity theft, fraud, and other security risks.

At Bank of the West, your security comes first. That's why we're taking this opportunity to tell you about steps you can take to better protect yourself.

Learn More

Bank of the West makes it easy for you to take steps to protect yourself from fraud and other security risks.

Alerts & Online Statements

In just a few simple steps you can sign up for services that can help improve your security.

- **Alerts:** Receive account notifications, which may alert you to suspicious activity.
- **Online Statements:** Access your statements anytime, anywhere, and reduce the risk of mail fraud at the same time.

Get Started

Security Tips

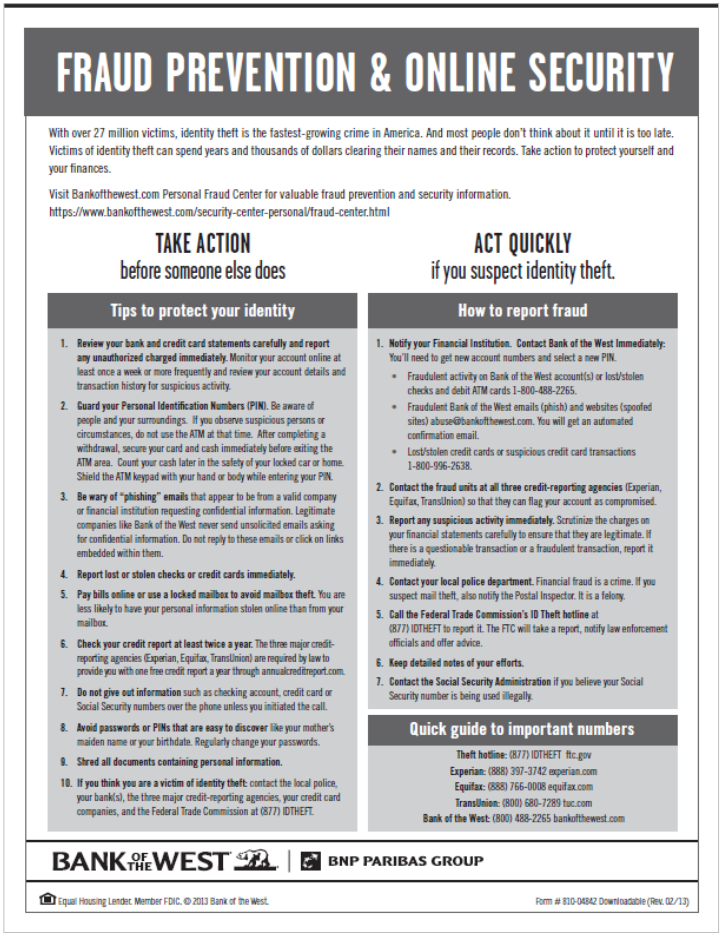
Here are just a few of the ways you can help protect yourself:

- Carefully review websites, online ads, and emails before taking any action or submitting any personal information online.
- Memorize your Password and PINs. Do not write them down, save them on your computer, or reveal them to anyone.
- Create a complex Password to your Online Banking account, and change it every 30 to 60 days.
- Never email your account number, Social Security number, or other sensitive information to anyone.
- Never leave your computer unattended while logged in. Complete your banking tasks and end your web sessions by always logging out.

Learn More

Useful Links

- Learn more about how you can protect yourself from online fraud.
- Review our Online Policies.
- Visit our Threat Watch page for the latest online security tips and advice.



FRAUD PREVENTION & ONLINE SECURITY

With over 27 million victims, identity theft is the fastest-growing crime in America. And most people don't think about it until it is too late. Victims of identity theft can spend years and thousands of dollars clearing their names and their records. Take action to protect yourself and your finances.

Visit Bankofthewest.com Personal Fraud Center for valuable fraud prevention and security information.
https://www.bankofthewest.com/security-center-personal/fraud-center.html

TAKE ACTION
before someone else does

ACT QUICKLY
if you suspect identity theft.

Tips to protect your identity

1. **Review your bank and credit card statements carefully and report any unauthorized charged immediately.** Monitor your account online at least once a week or more frequently and review your account details and transaction history for suspicious activity.
2. **Guard your Personal Identification Numbers (PIN).** Be aware of people and your surroundings. If you observe suspicious persons or circumstances, do not use the ATM at that time. After completing a withdrawal, secure your card and cash immediately before exiting the ATM area. Count your cash later in the safety of your locked car or home. Shield the ATM keypad with your hand or body while entering your PIN.
3. **Be wary of "phishing" emails** that appear to be from a valid company or financial institution requesting confidential information. Legitimate companies like Bank of the West never send unsolicited emails asking for confidential information. Do not reply to these emails or click on links embedded within them.
4. **Report lost or stolen checks or credit cards immediately.**
5. **Pay bills online or use a locked mailbox to avoid mailbox theft.** You are less likely to have your personal information stolen online than from your mailbox.
6. **Check your credit report at least twice a year.** The three major credit-reporting agencies (Experian, Equifax, TransUnion) are required by law to provide you with one free credit report a year through annualcreditreport.com.
7. **Do not give out information** such as checking account, credit card or Social Security numbers over the phone unless you initiated the call.
8. **Avoid passwords or PINs that are easy to discover** like your mother's maiden name or your birthdate. Regularly change your passwords.
9. **Shred all documents containing personal information.**
10. **If you think you are a victim of identity theft:** contact the local police, your bank(s), the three major credit-reporting agencies, your credit card companies, and the Federal Trade Commission at (877) IDTHEFT.

How to report fraud

1. **Notify your Financial Institution. Contact Bank of the West Immediately:** You'll need to get new account numbers and select a new PIN.
   - Fraudulent activity on Bank of the West account(s) or lost/stolen checks and debit ATM cards 1-800-488-2265.
   - Fraudulent Bank of the West emails (phish) and websites (spoofed sites) abuse@bankofthewest.com. You will get an automated confirmation email.
   - Lost/stolen credit cards or suspicious credit card transactions 1-800-996-2638.
2. **Contact the fraud units at all three credit-reporting agencies** (Experian, Equifax, TransUnion) so that they can flag your account as compromised.
3. **Report any suspicious activity immediately.** Scrutinize the charges on your financial statements carefully to ensure that they are legitimate. If there is a questionable transaction or a fraudulent transaction, report it immediately.
4. **Contact your local police department.** Financial fraud is a crime. If you suspect mail theft, also notify the Postal Inspector. It is a felony.
5. **Call the Federal Trade Commission's ID Theft hotline** at (877) IDTHEFT to report it. The FTC will take a report, notify law enforcement officials and offer advice.
6. **Keep detailed notes of your efforts.**
7. **Contact the Social Security Administration** if you believe your Social Security number is being used illegally.

Quick guide to important numbers

Theft hotline: (877) IDTHEFT ftc.gov
Experian: (888) 397-3742 experian.com
Equifax: (888) 766-0008 equifax.com
TransUnion: (800) 680-7289 tuc.com
Bank of the West: (800) 488-2265 bankofthewest.com

BANK OF THE WEST | BNP PARIBAS GROUP

Equal Housing Lender. Member FDIC. © 2013 Bank of the West. Form # 810-04842 Downloadable (Rev. 02/13)

Use the Media

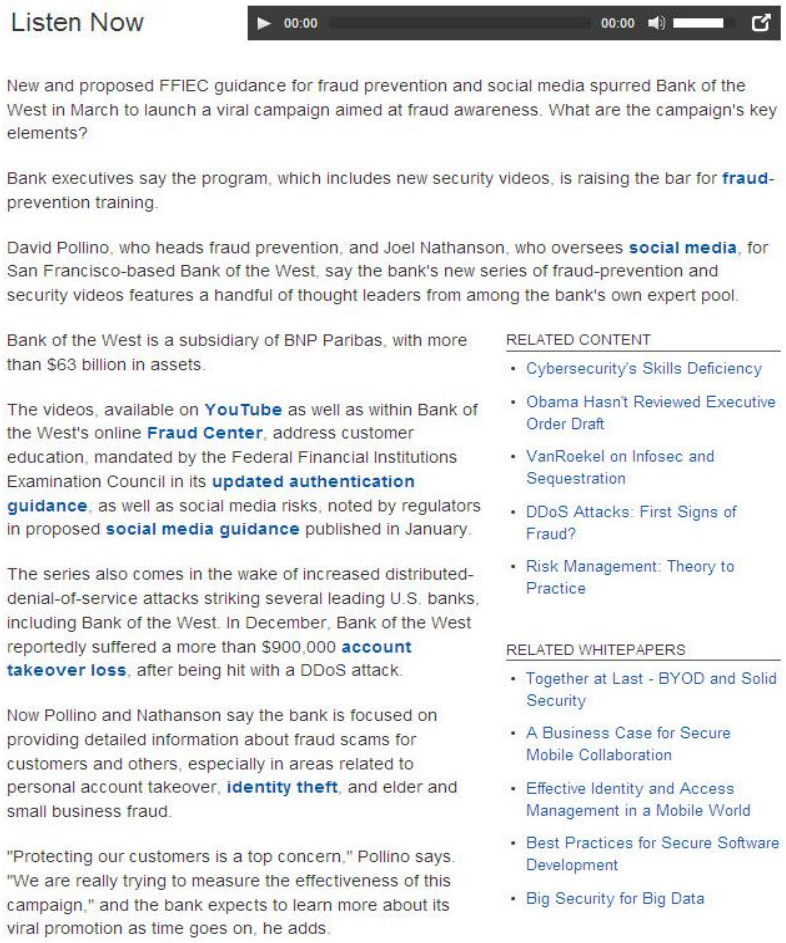
Home > Interviews

Fraud Awareness: A Banking Case Study

Inside Bank of the West's New Customer Education Program

By Tracy Kitten, April 1, 2013. Follow Tracy @FraudBlogger

Credit Eligible Email Tweet Like Share



Listen Now 00:00 00:00

New and proposed FFIEC guidance for fraud prevention and social media spurred Bank of the West in March to launch a viral campaign aimed at fraud awareness. What are the campaign's key elements?

Bank executives say the program, which includes new security videos, is raising the bar for **fraud**-prevention training.

David Pollino, who heads fraud prevention, and Joel Nathanson, who oversees **social media**, for San Francisco-based Bank of the West, say the bank's new series of fraud-prevention and security videos features a handful of thought leaders from among the bank's own expert pool.

Bank of the West is a subsidiary of BNP Paribas, with more than $63 billion in assets.

The videos, available on **YouTube** as well as within Bank of the West's online **Fraud Center**, address customer education, mandated by the Federal Financial Institutions Examination Council in its **updated authentication guidance**, as well as social media risks, noted by regulators in proposed **social media guidance** published in January.

The series also comes in the wake of increased distributed-denial-of-service attacks striking several leading U.S. banks, including Bank of the West. In December, Bank of the West reportedly suffered a more than $900,000 **account takeover loss**, after being hit with a DDoS attack.

Now Pollino and Nathanson say the bank is focused on providing detailed information about fraud scams for customers and others, especially in areas related to personal account takeover, **identity theft**, and elder and small business fraud.

"Protecting our customers is a top concern," Pollino says. "We are really trying to measure the effectiveness of this campaign," and the bank expects to learn more about its viral promotion as time goes on, he adds.

RELATED CONTENT

- Cybersecurity's Skills Deficiency
- Obama Hasn't Reviewed Executive Order Draft
- VanRoekel on Infosec and Sequestration
- DDoS Attacks: First Signs of Fraud?
- Risk Management: Theory to Practice

RELATED WHITEPAPERS

- Together at Last - BYOD and Solid Security
- A Business Case for Secure Mobile Collaboration
- Effective Identity and Access Management in a Mobile World
- Best Practices for Secure Software Development
- Big Security for Big Data

Trusteer

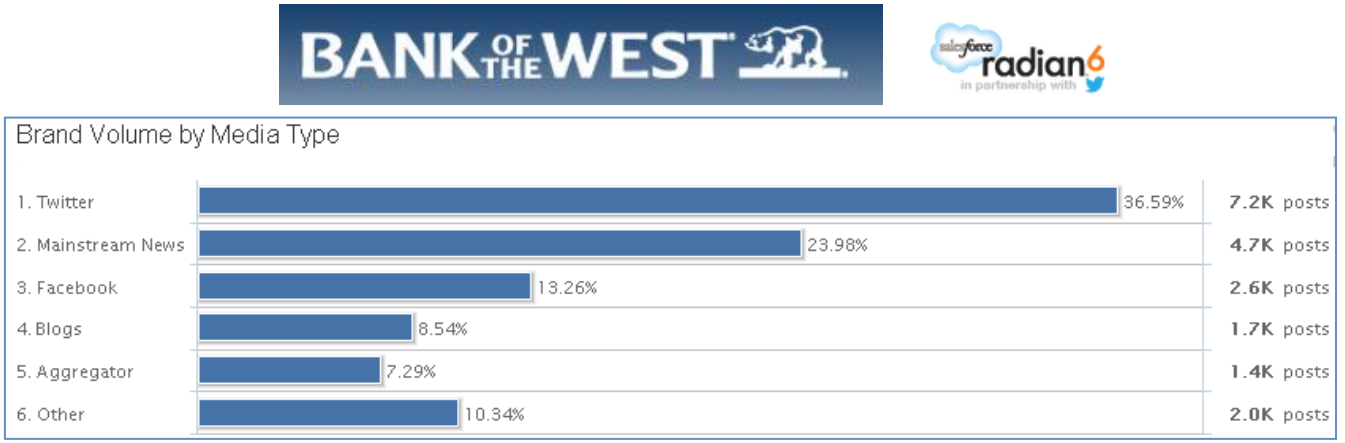

HOME
TRUSTEER RAPPORT
ONLINE BANKING SECURITY
SYSTEM AND SUPPORT
Online security to help keep you protected.
Get the high level of security and service you want with Trusteer Rapport.
Download Now*
FREE ONLINE FRAUD PROTECTION SOFTWARE FROM TRUSTEER
Trusteer Rapport
• Helps to create a safe connection between your web browser and Online Banking
• No configuration or maintenance
• Helps to protect your personal information, even if your PC is infected
Learn More
Online Banking Security
• Helps shield your information from malware
• Helps protect yourself from phishing techniques
• Add an additional level of security to your computer
Learn More
System and Support
• 24-hour customer support
• Windows® and Mac® compatible
• Supported by a variety of web browsers
Learn More

CAN WE USE SOCIAL MEDIA

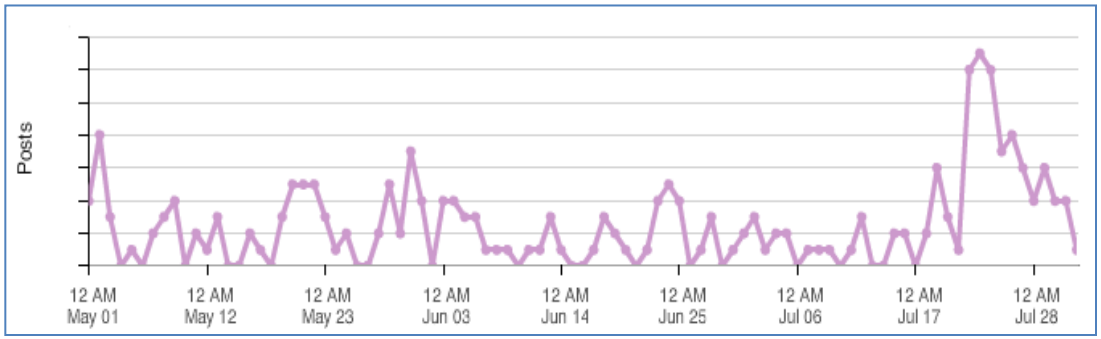
Social Content Monitoring and Reporting

Listening & Engagement

Social Reporting & Analytics



Post Volume

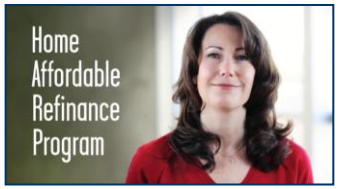


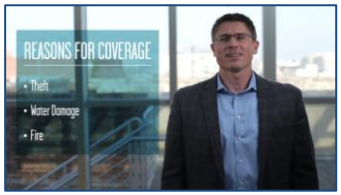
Trending Topics

ISACA San Francisco Chapter

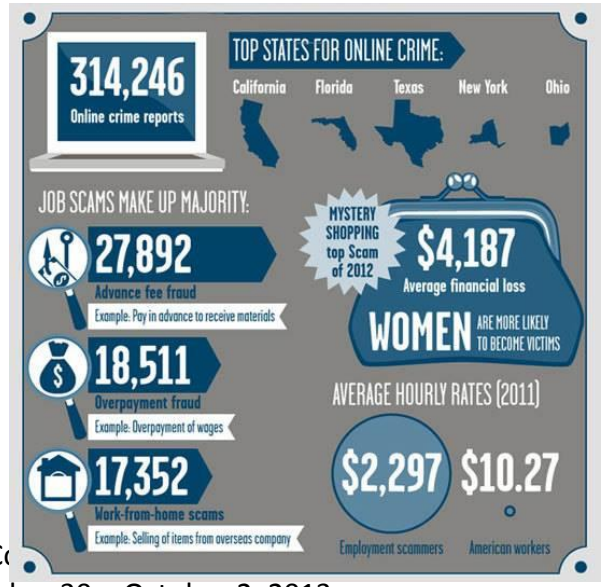
Fraud Education

"In Brief"
Expert Video Series



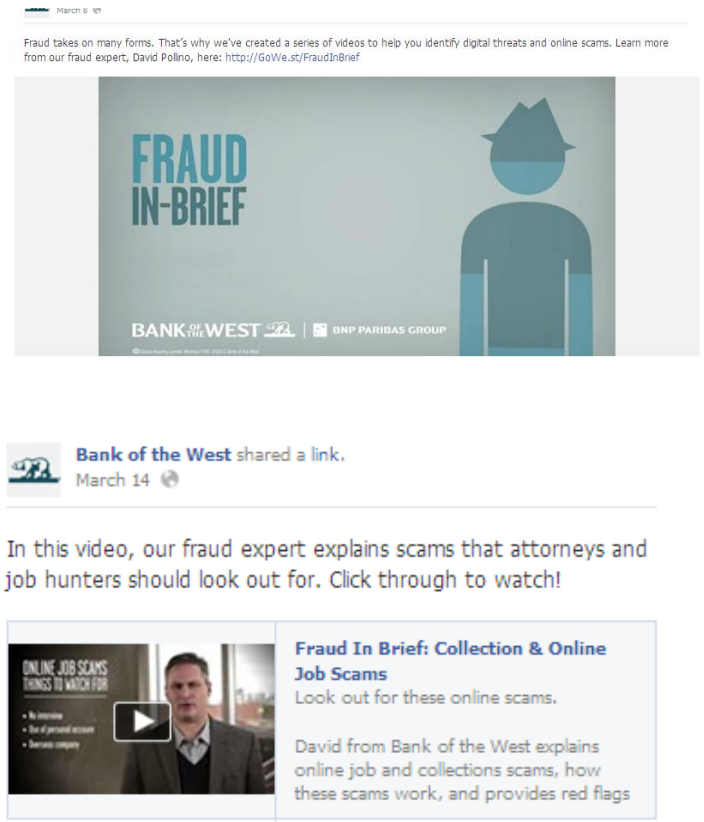


Social Content & Infographics



Fraud in Brief

- Created and published Fraud Videos on YouTube channel as part of “in brief” campaign
- Promoted fraud videos on Facebook and Twitter
- Example posts:
  - **FACEBOOK**:
    - Looking for the flexibility of a work-from-home job? Our fraud expert, David Pollino, gives you the scoop on some red flags to look out for when job hunting.
    - Attorneys should watch out for this online scam that offers big payouts for little work. Find out what it is in this video from our fraud expert, David Pollino.
  - **TWITTER:**
    - Working from home would be nice, but be careful you don’t get scammed when applying: [LINK] #TIPS #InBrief
    - Get a #workfromhome job offer without an interview? You could be getting scammed: [LINK] #InBrief



Facebook Posts

Bank of the West
March 19

Looking for the flexibility of a work-from-home job? Our fraud expert, David Pollino, shares some red flags to look out for when job hunting online in our latest In Brief video: http://GoWe.st/XiQUR1

Like · Comment · Share 1

Bank of the West
March 18

This week, we'll be sharing 5 tips from the IRS to help you avoid identity theft and tax return fraud. First up: Never carry your Social Security card or any documents with your SSN or Taxpayer ID number on them. Share this post with your friends and check back this week for more tips! http://gowe.st/128ItM"

Unlike · Comment · Share 8 2

Bank of the West
March 19

IRS tax season tip #2 : Don't give a business your Social Security number just because they ask. http://gowe.st/128ItM

Like · Comment · Share 5 2

Bank of the West
March 20

IRS tax season tip #3: Check your credit report often to correct any errors and monitor for fraudulent activity. http://gowe.st/128ItM Check back here tomorrow for another tax fraud prevention tip!

Like · Comment · Share 2

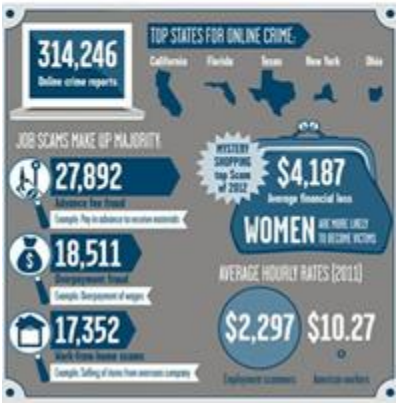
Bank of the West
May 2

Job seekers: Stay alert when looking for employment online. Our latest infographic may help you spot the warning signs of a job scam. Additional facts and helpful information here: http://GoWe.st/WorkedOver

Like · Comment · Share 14 2

Bank of the West
Yesterday

Our Chief Economist, Scott Anderson, said that June's jobs report "blew all expectations out of the water" with over 197,000 jobs gained last month. A large number of Americans are still looking for work, though, and a big portion is spent looking online. Don't let job scams get the best of you. Check out our infographic that offers helpful tips that can help keep you safe: http://GoWe.st/WorkedOver



Bank of the West
March 21

Avoid identity theft during tax season with this tip from the IRS:: Don't give personal information over the phone, Internet, or email unless you have initiated the contact or you are sure you know who you're dealing with. http://gowe.st/128ItM Share this post with your friends as a reminder to stay safe!

Like · Comment · Share 8 2

Bank of the West
March 22

Tax season tip #5: Use firewalls, anti-spam, anti-virus, and anti-phishing software (like Trusteer Rapport, which is free for Bank of the West customers http://gowe.st/128MLAP), and perform regular security updates and password changes. http://gowe.st/128ItM

Fill in the blank: I change my password every _____ days/weeks/months.

Like · Comment · Share 2

Social Media Engagement

- Customers respond to content
- Engage responses

ARE WE REALLY BEING EFFECTIVE?

Measuring Online Customer Awareness

"Financial institutions have made, and should continue to make, efforts to educate their customers. Because customer awareness is a key defense against fraud and identity theft, financial institutions should evaluate their consumer education efforts to determine if additional steps are necessary. Management should implement a customer awareness program and **periodically evaluate its effectiveness**. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their authentication credentials (e.g., ID/password), the number of clicks on information security links on Web sites, the number of statement stuffers or other direct mail communications, the dollar amount of losses relating to identity theft, etc"

Source: FFIEC – 2005 Authentication in and Internet Banking Environment

Approach

- **3 C's of Customer Awareness**
  - **Content** = annual review of content to satisfy compliance
  - **Clicks** = Alerts, security center visits, security center page views
  - **Customer engagement** = marketing of security features and tools, surveys

Questions

Thank You