

# Faces of Fraud in the 21<sup>st</sup> Century

---

Jamie Wells, SVP  
**Treasury Management**  
**Wells Fargo Bank**

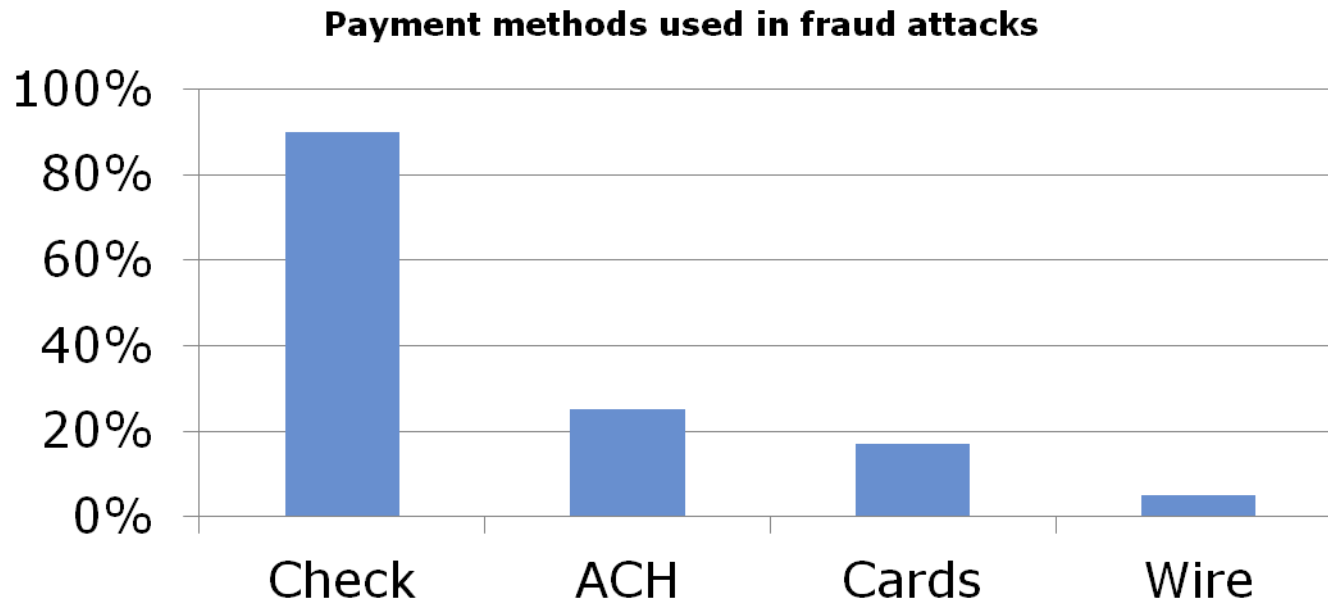
2012 AOA Annual Conference

Together we'll go far



# Fraud facts

- Fraud accounts for more than \$200 billion in losses each year in the U.S.<sup>1</sup>
- 73% of organizations experienced attempted or actual payments fraud in 2009<sup>2</sup>



1. First Data Fraud Trends 2010 2. 2010 AFP Payments Fraud and Control Study

# Online fraud

# The threat is real...

- **Malware attacks exploding**

The incidence of malware infections grew tenfold in 2009

Bankinfosecurity.com, "Top 8 Security Threats of 2010," March 2010

- **Phishing attacks double**

There were at least 126,697 phishing attacks in the second half of 2009, more than double the 55,698 attacks recorded in the first half

Global Phishing Survey: Trends and Domain Name Use 2H2009  
May 2010 Anti Phishing Working Group

- **Online fraud hits 3 out of 4 companies**

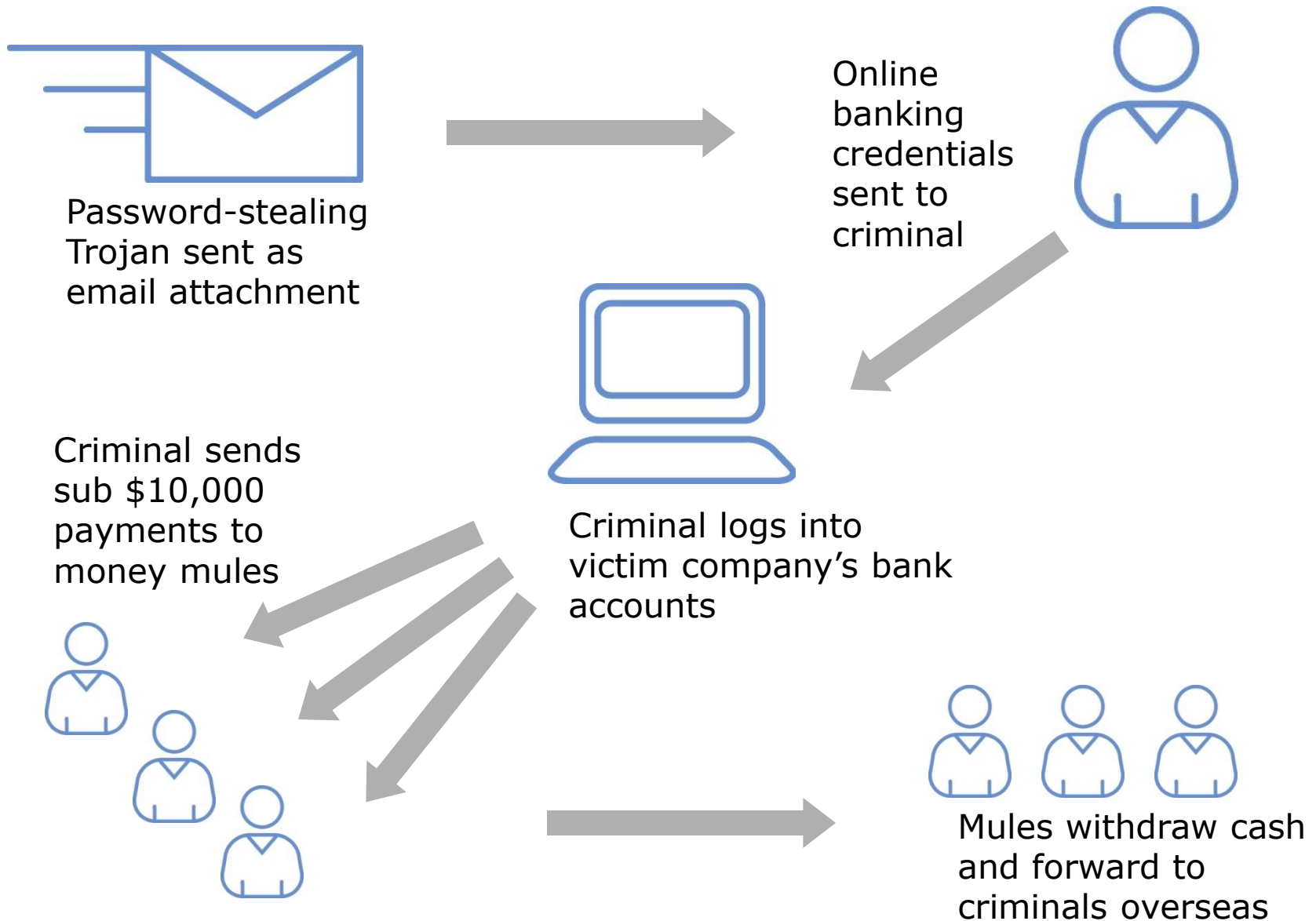
75% of enterprises surveyed experienced some form of cyber attack in 2009

Symantec State of Enterprise Security Report 2010

# Online fraud basics

- The online fraudster's goal is simple: steal online banking credentials, set up online transactions and transfer money undetected
- Attacks are sophisticated, pervasive and always changing
  - Increasingly rendering traditional prevention tactics/tools ineffective
  - Can defeat most anti-virus and anti-malware solutions

# Business account takeover



# Common fraudster techniques

- Social engineering
  - Manipulating people into performing actions or divulging confidential information by impersonating a trustworthy entity in an electronic communication
- Malware
  - MALicious softWARE installed on a computer without a user's consent
  - Records keystrokes and screen shots, redirects the browser, displays fake web pages and/or allows fraudsters to impersonate the customer in online transactions
  - Carriers of malware include infected documents attached to emails, links in emails that connect to an infected site, infected search engine results and documents, videos and photos posted on legitimate sites, particularly social networking sites
- Combination of social engineering and malware
  - Social Engineering is used in order to trick a user in order to infect them with malware

# How can you identify a bogus site?

Commercial Electronic Office Sign On - Windows Internet Explorer

http:wellsite.com/

File Edit View Favorites Tools Help

WELLS FARGO

Locations | Contact Us | Home

Personal Small Business Commercial About Us

Return to Commercial Services

**Commercial Electronic Office®**

Company ID  
User ID  
Password

Sign On Forgot Password?

Trouble Logging in?

- [Password Reset Tutorial](#)
- [First Time Sign On Tips](#)

Additional Information

- [Online Fraud Protection](#)
- [System Requirements](#)

Not yet enrolled in our commercial Internet services?  
Discover the power of the CEO® business portal today.  
[View Our Online Solutions](#) | [Contact Us](#)

About Wells Fargo | Careers | Privacy, Security & Legal | Sitemap

© 1999 - 2011 Wells Fargo. All rights reserved.

Local intranet 100%

Notice the URL

- wells Fargo.com and ceoportal do not appear in it.
- There is no “s” after “http,” so it is not a secure site.

Look for a padlock icon in one or more positions on the page. It indicates this is a secure site.

# Experi-Metal Inc. wire fraud

Attack – Spear phishing

- Controller received email purportedly from bank, clicked on link, and was diverted to “bank” website
- Gave up personal and company IDs and passwords
- Thieves used credentials to send 93 wire transfers in **6 ½ hours** to accounts in Russia, Estonia, Scotland, Finland, China, and U.S
- \$1,901,269 stolen; all but \$560,000 recovered

# SuperValu phishing scam to accounts payable

Attack – social engineering

- E-mails claiming to be from American Greetings and Frito-Lay provide new account numbers for payments
- Over 4 days, SuperValu wires \$6.4 million to HSBC account for American Greetings, \$3.6 million to Frito-Lay account at Arkansas bank

Source: *Supervalu becomes victim of e-mail scam*, Boston Globe, October 20, 2007

# There is no “silver bullet”

You must employ a layered approach that focuses on:

- **Prevention** – Lowering the likelihood of successful compromise
- **Detection** – Ensuring compromises can be reliably and rapidly detected
- **Response** – Knowing what to do when you have been compromised

# Prevention

# Educate employees, raise awareness

- Protecting online banking credentials is paramount in defending against online account takeover
- One of the most important steps you can take is to educate your employees on what the threats are, how to recognize them and what to do if they think a threat presents itself

# Institute dual control for executing all payment transactions and self administration

- Initiate ACH and wire transfer payments under dual control – someone initiates, another approves **from a different computer**
- Be cognizant of collusion risks – select approvers that are less likely to collude (i.e. in another office)

# Use a dedicated computer to conduct online banking activity

- Online commercial banking customers execute all online banking activities from a dedicated computer where email and web browsing are not possible
- Significantly reduces your exposure to malware pharming of your banking credentials

# Use multi-factor authentication to access your banking portal

- Simply having a username and password does **not** constitute multi-factor authentication
- Adding a physical security token, something in the users possession (and thus satisfying multi-factor requirements), provides additional protection from online threats

# Update antivirus programs

- Ensure your company's firewalls, servers and client applications or systems are updated with all vendor-recommended patches and that your company's antivirus and antispyware software is installed and updated regularly

# Protect your network

- Identify trusted Web sites for your business and block access to any Web address that is not relevant to your employees' business needs

# Institute transaction and daily limits

- Review company and account limits
- Evaluate averages and determine whether upper limits are excessively high

# Diligent user management

- Audit users on a regular basis, especially those with transaction privileges
- Review user privileges often to ensure no one has unauthorized or unnecessary access
- Limit **transaction** privileges to an absolute minimum – needs only basis
- Separation of duties for key money movement activities

# Detection

# Monitor and reconcile accounts and transactions on a daily basis

- Reconciling your operating accounts daily is one of the most effective ways to catch suspicious activity as soon as possible, limiting further or substantial damage
- Establish internal processes to review key operating accounts and...accounts in which you issue checks!
- Automate more of your reconciliation using account reconciliation services

**Immediately call your customer service group if you notice anything out of the ordinary**

# Use notification/alert services

- Sign up to receive text or e-mail notifications alerting you of electronic debits to your accounts
  - Positive Pay Exceptions notifications
  - Wire notifications – incoming/outgoing
  - ACH Fraud Filter notifications
  - Balance threshold notifications

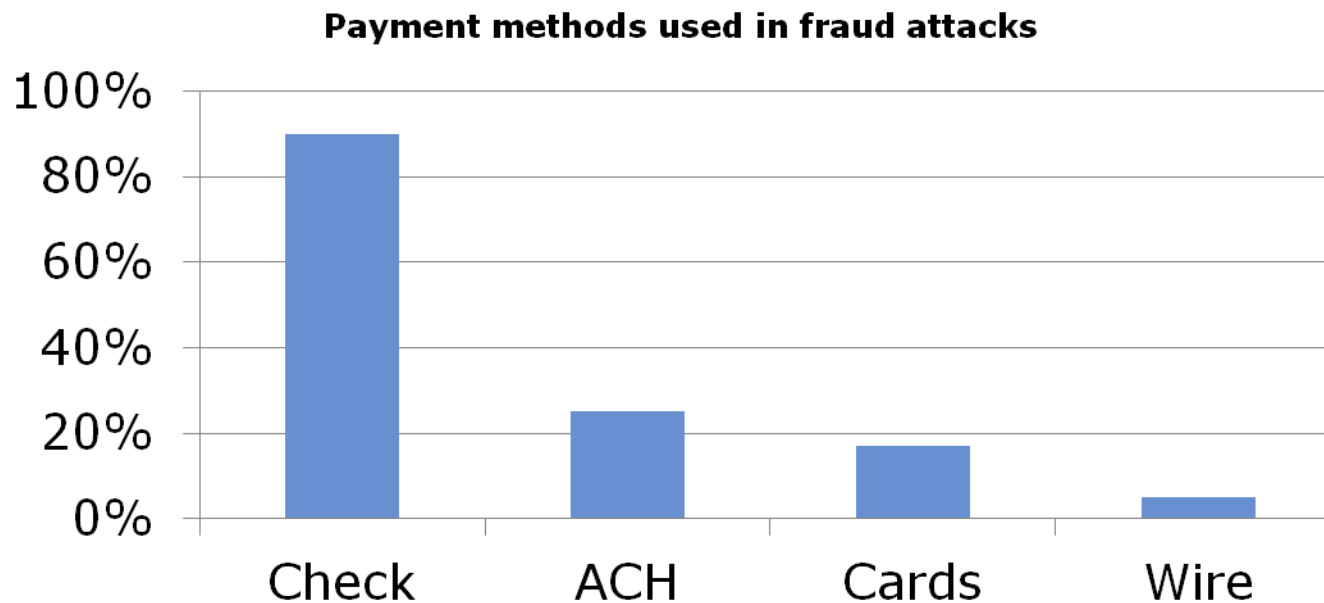
# Laws/regulations governing online fraud

- Regulation E:
  - Federal law that provides **consumers** with protections from unauthorized electronic fund transfers (EFT)
  - **Exceptions** – Reg E protections do **not** apply to wire transfers, or EFTs from **business** accounts
- Uniform Commercial Code Article 4A:
  - Governs funds transfers from a business account (ACH & Wire) and wire transfers from a business or consumer account
  - Defines “ordinary care” and “commercially reasonable standards”

# Check fraud

# Checks remain the most prevalent form of payment fraud

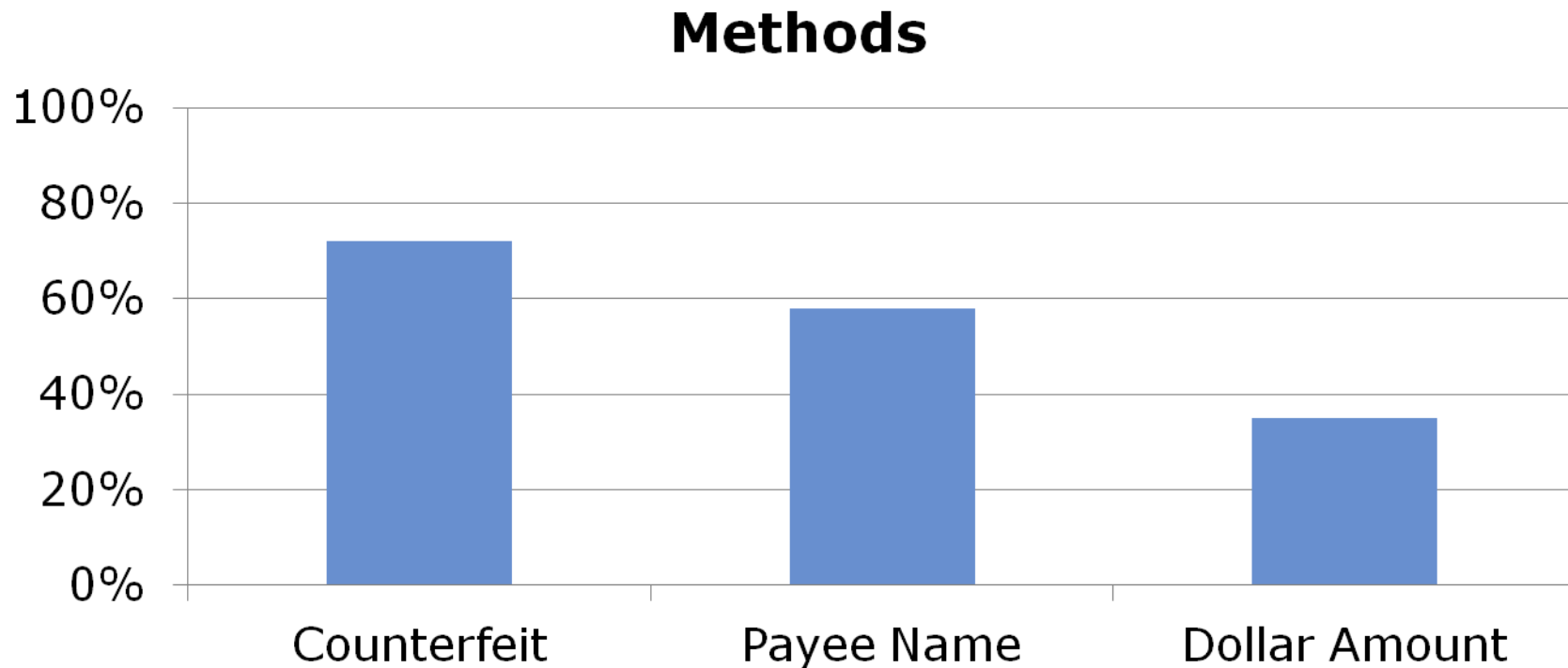
- We still write lots of checks
- Checks are touched/seen more than any other payment form – easy target



Source: 2010 AFP Payments Fraud and Control Survey

© 2010 Wells Fargo Bank, N.A. All rights reserved. Member FDIC

# Most common check fraud methods



- 78% of check fraud is perpetrated by stolen check data used to create counterfeit checks
- Accounts Payable and disbursement accounts are most common targets with payroll accounts running a close second

Source: 2010 AFP Payments Fraud and Control Survey

# How to reduce the risk of check fraud

- **Don't write checks**

- Move to electronic payments wherever possible - ACH, Card, Wire

- Leverage bank services

- Positive Pay, Reverse Positive Pay, Payee Validation\*, Teller Positive Pay

- Shred unused checks including those you process with a remote deposit capture solution (subject to recommended retention guidelines)

- Consider outsourcing check printing

**\*Almost 60% of check fraud victims experienced altered payee names on checks**

\* 2009 AFP Payments Fraud Survey

# ACH Fraud

# ACH is not immune to fraud

- Fraudulent ACH debits often originate from – a compromised check!
- Multiple ways ACH fraud can impact your business:
  - As a passive Receiver of unauthorized ACH debits against your account
  - As an active Originator of e-Check transaction – consumers providing fraudulent information to make purchases
  - Redirect vendor payments to fraudulent accounts

# Services to protect against ACH fraud

- ACH Debit Block – block any ACH debit coming to your account; consider for depository only accounts
- ACH Fraud Filter options:
  - Review-service option - you review unauthorized transactions and make pay/return decisions
  - Stop-service option - Wells Fargo will automatically stop and return to originators all ACH transactions presented against your accounts, except those you have preauthorized

# Know Your Money

# How to detect counterfeit money

- The public has a role in maintaining the integrity of U.S. currency
- Look at the money you receive. Compare a suspect note with a genuine note of the same denomination and series, paying attention to the quality of printing and paper characteristics. Look for differences, not similarities.

Source: United States Secret Service

# How to detect counterfeit money

- Portrait - The genuine portrait appears lifelike and stands out distinctly from the background. The counterfeit portrait is usually lifeless and flat. Details merge into the background which is often too dark or mottled.
- Federal Reserve and Treasury Seals - On a genuine bill, the saw-tooth points of the Federal Reserve and Treasury seals are clear, distinct, and sharp. The counterfeit seals may have uneven, blunt, or broken saw-tooth points.
- Border - The fine lines in the border of a genuine bill are clear and unbroken. On the counterfeit, the lines in the outer margin and scrollwork may be blurred and indistinct.



Source: United States Secret Service

# Raised Notes

- Genuine paper currency is sometimes altered in an attempt to increase its face value. One common method is to glue numerals from higher denomination notes to the corners of lower denomination notes



Source: United States Secret Service

# If you receive a counterfeit

- Do not return it to the passer.
- Delay the passer if possible.
- Observe the passer's description, as well as that of any companions, and the license plate numbers of any vehicles used.
- Contact your local police department or [United States Secret Service field office](#). These numbers can be found on the inside front page of your local telephone directory.
- Write your initials and the date in the white border areas of the suspect note.
- Limit the handling of the note. Carefully place it in a protective covering, such as an envelope.
- Surrender the note or coin only to a properly identified police officer or a U.S. Secret Service special agent.

Source: United States Secret Service

# Additional resources

Please visit our website for further information:

[www.wellsfargo.com/fightfraud](http://www.wellsfargo.com/fightfraud)

# Questions