Mitigate, Recognize and React to Identity Theft
Mitigate Fraud Risk

Have you assessed your risks and taken appropriate action to secure yourself, your business and organization?

- Private vs. Public Information
- Know your environment
- Practice Cleaning and Clear Outs
Home Security Checklist

- Always update your computer software; the operating system, internet browser, Adobe Acrobat, Flash, Java, antivirus, etc.
- Create strong passwords for your online accounts and never share them with anyone.
- Use different passwords for online banking than you use for social media sites or email.
- Shred any documents that contain your personal information, instead of putting them in the garbage.
- Whether you are on a cell phone or talking to another individual, be aware of your surroundings when discussing your personal information in public.
- Check your credit report at least once per year at Annualcreditreport.com - it’s free!
- If you have a wireless network at home, be sure that you use strong encryption, change any default passwords, and update any default security settings as appropriate.
Take Control

Ask questions and be aware of controls available through your bank, mobile applications and card programs.

- Lock misplaced cards
- Set transaction limits
- Block International transactions
- Use Alerts
How to detect malicious links

Phishing scams often succeed because end users don't know how to tell a valid link from a fake one. Phishers use fake links to fool people into clicking on what looks like a valid address that actually goes to a malicious website instead. **Identifying the Domain is the most effective method to detect phishing emails.**

**What do you need to know?**

The most important part of any web address (i.e. link) is the Domain. The domain is what comes right before the first single forward slash. When you hover your mouse over the link, always look for the actual domain. **Note:** Users with mobile devices should be aware that link hovering may not work. If the email is suspicious, wait to inspect it more closely from your PC and use the hovering technique.

```
http://support.amazon.com/onsale
```

If the part of the web address right before the first single forward slash (the Domain) is different than what you are expecting, the link could be malicious.

An example would be a web address of `http://support.amaz.on.com/onsale` where it may look like it goes to Amazon, but is actually going to the on.com domain. Always hover over a link to see the actual address. This technique also works on links within documents.

[People's United Bank](http://www.people'sunited.com)®

*What know-how can do®*
Phishing Warning Signs

1. Emails sent from public email address
2. Unsolicited attachment
3. Generic greetings
4. Spelling mistakes
5. Links to unrecognized sites or slightly misspelled sites
6. Threat or enticements that create a sense of urgency
7. Toll free numbers in suspicious emails that don’t match known numbers
Victim of Identity Theft

TAKE ACTION IMMEDIATELY!

• Use the ID Theft Affidavit at www.ftc.gov/idtheft
  – Review recovery steps
  – Create a Personal Recovery Plan
• Contact your creditors and Follow up in writing
• Call where the fraud occurred
• File a complaint with the Federal Trade Commission
• Ask for verification that disputed accounts have been closed and fraudulent debts discharged
• File a police report
Security is the **shared** responsibility of your business and bank.

It takes a multi-layered approach from both.
Best Practice to protect your business

- Perform a risk assessment
- Establish company security policies and procedures
- Protect computer and mobile device endpoints (patch, anti-virus, etc.)
- Limit access and closely monitor accounts
- Train and test employees (awareness)
- Use a dedicated PC for high risk business functions (i.e. online banking)
- Use fraud detection and prevention tools for your bank accounts – ACH/Check Positive Pay
- Consider commercial fraud insurance
Protect – Best Practices in Fraud Prevention

Services available from your bank.

- Positive Pay
- Alerts Features
- ACH Blocks/Filters
- Services and Features offered by your Bank
- Wire Procedures
- Segregate Accounts
- Out of Channel Approvals
Detect – develop and implement the appropriate activities

<table>
<thead>
<tr>
<th>Daily</th>
<th>Review bank accounts daily</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconcile</td>
<td>Reconcile all bank accounts</td>
</tr>
<tr>
<td>Audit</td>
<td>Regularly review online banking usage</td>
</tr>
<tr>
<td>Dedicated</td>
<td>Have a PC that is only utilized for banking</td>
</tr>
<tr>
<td>Rotate</td>
<td>Cross-train staff and rotate responsibilities</td>
</tr>
<tr>
<td>Beware</td>
<td>Prepare for 3-day weekends &amp; sudden changes in business practices</td>
</tr>
</tbody>
</table>
Lucie Hannigan, SVP
Treasury Management
(207)828-3145
Lucie.Hannigan@peoples.com

Janet Butland, VP
Market Manager
(207)828-3036
Janet.butland@peoples.com