UNITED BANK

Fraud Prevention Checklist

1. Establish a multi-level approval process and an extended release time for all wire transfers, for example:
   - Institute a time delay for all wire transfers over a certain amount
   - Entities on both sides of the transaction should utilize digital signatures

2. Implement technical controls to help prevent phishing attacks. Recommended controls include:
   - Email filtering
   - Two-factor authentication – simply requiring a username and password isn't always enough
   - Keep the reins tight on network boundaries and access
   - Automated password and user ID monitoring – which requires periodic updating of your usernames and passwords

3. Establish a comprehensive security policy and plan and review it regularly

4. Implement best practices and procedures
   - Study, train and enforce security and risk policies
   - Encourage executive management buy-in and keep them informed of data breaches and reporting
   - Purchase domain names that are variations of your organization's name
   - Periodically test the plan and make changes as needed
   - Create intrusion system rules that flag emails with extensions that look like a company email. For example, while an e-mail from 123_company.com can be legitimate, the system would flag a similar-looking, fraudulent e-mail from 123-company.com
   - Have a contingency plan