First Republic
It's a privilege to serve you®

Cybersecurity Top 10 Fraud Prevention Checklist

1. **Train your employees regularly.**
   Online security training should be a regular occurrence that includes all employees across the organization.
2. **Verbally validate payment instructions.**
   Implement an internal process to verbally verify new payment instructions or changes to existing payment instructions received via email. Administrative changes to add authorized users/signers should also be verbally verified.
3. **Use multifactor authentication.**
   Multifactor authentication is an authentication control in which a user is granted access to a website or application only after successfully presenting two or more authentication pieces: something you know (e.g., a password), something you have (e.g., a token) and something unique to you (e.g., fingerprints).
4. **Enforce secure password policies.**
   Configure your password policies to be as secure as possible based on industry standards. These include but are not limited to instituting minimum complexity requirements and account lockout policies and avoiding password reuse.
5. **Restrict privileges: Operate based on the principle of least privilege.**
   Give users only the permissions they need to do their jobs and nothing more.
6. **Keep your operating systems and applications up to date.**
   Ensure that both your operating system and applications are patched in a timely manner.
7. **Consider mobile device management software.**
   Utilize mobile device management software that allows your IT department to implement policies to protect company data on employee mobile devices.
8. **Regularly maintain backups and test them in mock-crisis scenarios.**
   Regularly back up critical data and test the access and response process via tabletop scenarios (e.g., a ransomware exercise).
9. **Create a documented incident response plan.**
   Prepare for future incidents by creating a response plan outlining how you would react and who would be involved.
10. **Conduct vendor due diligence.**
    Assess your vendor risk, especially vendors handling your critical data, and ensure that they have appropriate security measures and controls in place.

We're ready to help.

At First Republic, we offer complimentary cybersecurity services to proactively safeguard your accounts and improve your security posture. To learn more about and schedule these services, please contact InformationSecurity@firstrepublic.com.

492468B-01-0521