Who is KirkpatrickPrice?

KirkpatrickPrice is a licensed CPA firm, providing assurance services to over 250 clients in more than 40 states, Canada, Asia and Europe. The firm, since its inception, has offered GLBA assessment services to organizations seeking to strengthen their privacy and security controls through compliance consulting, audits, and tests.
Welcome

Joseph Kirkpatrick is a certified specialist in data security, IT governance, and regulatory compliance. He has provided GLBA advice and security assessments for more than 14 years, performing over 300 audits worldwide.

- Certified in the Governance of Enterprise IT (CGEIT)
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Qualified Security Assessor (QSA)
The federal regulation that requires organizations to institute certain measures to protect the privacy and security of consumer information—Regulation P has been updated through the Dodd-Frank Act and rulemaking authority transferred to the Consumer Financial Protection Bureau—The Credit Union, Bank, and Thrift Regulatory Relief Act of 2008 excluded Privacy Notification requirements for Debt Buyers.
Overview

• Privacy
• Security

What’s the difference?
What started it all

- Financial Services Modernization—1999
Privacy and Security Requirements

Financial Institutions implemented these changes quickly. Enforcement came from the FDIC, OCC, OTS, NCUA, and State Regulatory Agencies.
Not Just for Banks

• This law also applied to NON-TRADITIONAL Financial Institutions—but no one knew it!
  – Promulgated by the Federal Trade Commission in 2002
November 16, 2004—"As part of a nationwide compliance sweep, the Federal Trade Commission has charged two mortgage companies with violating the agency’s Gramm-Leach-Bliley (GLB) Safeguards Rule by not having reasonable protections for customers’ sensitive personal and financial information."
In 2006, the FTC continued educating the business community about challenges with Information Security.
Enforcement Actions

• 2002—Microsoft
• 2004—Auto dealerships and mortgage companies
• 2005—Superior Mortgage, Nations Title Agency, and BJ’s Wholesale
• 2006—DSW Inc. and ChoicePoint
• 2008—Life is Good, Goal Financial, and Premier Capital Lending
Enforcement Actions

• 2009—James B. Nutter & Co.
• 2011—3 credit report resellers
• 2012—HTC America
• 2012—EPN a debt collector
• 2012—Franklin’s Budget Car Sales
• 2012—PLS Financial Services
Nonpublic Personal Information

- Social Security Number
- Credit Card Number
- Account Number
Privacy Requirements—Regulation P

- Notification about privacy policies and consumer rights
- Initial privacy notice when establishing a customer relationship
- Annual privacy notice to consumers
- Establish the type of information to be included in notices
- Opt out notices and opt out methods
- Revised privacy notices
Privacy Requirements—Regulation P

- Establish limits on disclosure to nonaffiliated third parties
- Establish limits on redisclosure and reuse of information
- Limits on sharing account number for use in marketing purposes
- Establish an exception to opt out requirements for service providers and joint marketing
- Establish an exception for processing and servicing transactions
Privacy Policy Example
XIII. Privacy

Except as otherwise expressly provided for in these Terms, your use of the Website is subject to Privacy Policy, which is expressly incorporated into these Terms and Conditions. Your continued use of the Website constitutes your express agreement to not only these Terms and Conditions but those enumerated in the incorporated Privacy Policy.
Privacy Policy Example

III. User Submissions to the Website

Any communication which you post or submit to the Website is considered to be non-confidential and in the public domain. By posting communications to the Website, you automatically grant a royalty-free, perpetual, irrevocable, worldwide, non-exclusive license to use, reproduce, modify, publish, edit, translate, distribute, perform, and display the communication alone or as part of other works in any form, media, or technology whether now known or hereafter developed, and to sublicense such rights through multiple tiers of sublicensees.
Safeguard Rule Objectives

• Ensure the security and confidentiality of customer information
• Protect against any anticipated threats or hazards to the security or integrity of such information
• Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer
Written Information Security Program

Appropriate to the organization’s:

• Size and complexity

• Nature and scope of its activities

• Sensitivity of the customer information
Components of the Information Security Program

• Approved and overseen by the board of directors
• Proper training given to employees
• An employee or employees are designated to coordinate the safeguards
• Identify and assess the risks to customer information
Components of the Information Security Program

- Implement controls to safeguard and monitor risk
- Oversee service providers
- Evaluate the program every year and make adjustments to the controls
Action Items

- Do you have a privacy policy?
- Do you have a written information security program?
Thank you for attending our Webinar

Q & A

For further information contact:
Todd Stephenson
t.stephenson@kirkpatrickprice.com
800.977.3154 Ext. 202
CFPB Readiness Series: Understanding UDAAP

Under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), *all covered persons or service providers are legally required to refrain from committing unfair, deceptive, or abusive acts or practices (collectively, UDAAPs) in violation of the Act*. What are you doing to prevent, detect and correct issues in your organization that might be in violation?