Fox Rothschild LLP
ATTORNEYS AT LAW

Updated Federal Regulations Contractors Must Know – Cybersecurity, Ethics & Compliance, SBA All-Small Program & More

Reggie Jones, Mark McCreary, Doug Hibshman, & Nick Solosky

AGC Federal Contractors Conference – May 1, 2017

Fox Rothschild LLP

- 800+ Attorney, Full Service firm
- 22 Offices – Coast-to-Coast
- DC Office - Government Contracts, Construction, Infrastructure, & Government Investigations Practices
- Represent Small, Medium, and Large Contractors, subcontractors, suppliers, owners, sureties, developers in all Federal and State contracting matters
- Bid Protests, Contract Claims, Litigation & ADR, False Claims Act, FCPA, Transactional Work, and Other Federal Compliance Advice

Introducing Today's Panel

- **Reggie Jones**
  - Fox Rothschild, LLP – DC Office Managing Partner
  - Chair, Federal Government Contracts & Procurement Practice Group
- **Mark McCreary**
  - Chief Privacy Officer
- **Doug Hibshman**
  - Partner, Federal Government Contracts & Procurement Practice Group
- **Nick Solosky**
  - Partner, Federal Government Contracts & Procurement Practice Group

Today's Outline

1. **New Federal Cybersecurity Requirements**
   - Unpacking the New FAR and DFARS Requirements
   - Ethics & Compliance Implications
   - Handling Classified Information
2. **Need to Know Regulations for the New Administration**
   - Buy American, Hire American
   - "Blacklisting" Rule
3. **SBA's "All Small" Mentor Protégé Program**

Why We Are Here

- The **Fraud Enforcement and Recovery Act of 2009 (FERA)** lowered the legal standard to prove fraud.

- The **American Reinvestment and Recovery Act (ARRA)** increased funding for staffing at the various Offices of the Inspector General; Subsequent National Defense Authorization Acts have maintained that spending.

Why We Are Here

- In 2011, the GAO investigated six federal agencies' suspension and debarment procedures and found that they weren't enforcing the rules. According to a 2014 GAO follow-up report, **the number of suspensions and debarments nearly tripled between 2011 and 2014**.

- On September 9, 2015, Deputy Attorney General, Sally Quillian Yates issued a memorandum (**The Yates Memo**) that directed Department of Justice attorneys to focus on individuals and not just their employers. According to the Yates Memo, **"[o]ne of the most effective ways to combat corporate misconduct is by seeking accountability from the individuals who perpetrated the wrongdoing."**

What Areas Are the Most Susceptible to Investigation and Enforcement?

- In the **construction industry**, the government's focus has been on pursuing alleged violations of the Small Business Administration (SBA) regulations (including the U.S. Department of Transportation's Disadvantaged Business Enterprise (DBE) program), Buy American Act, Davis-Bacon Act, and Certified Cost or Pricing Data issues.
- **Why?**
  - Unlike large defense contractors, construction contractors often don't have large compliance staffs.
  - There is often a disconnect between the bidding and proposal process and the ultimate design and construction of the project.

Why We Are Here

- **Today's Reality: Hyper Enforcement**
  - **False Claims Act, Suspension & Debarment, & More**
- The **Construction Industry** is an **Easy Target**
  - Disparity Between Enforcement and Compliance Capabilities
- **Bi-Partisan Political Support** for **Enforcement**
  - Total recoveries since FY 2009 is **$26.4 Billion**
- **Risk of Unintentional False Claims is High**
- **Regular Ethics & Compliance Training is the Best Protection**

Basic Ethics & Compliance Requirements

- **Implement an Ethics and Compliance Program!**
- **FAR 52.203-13** Requires Contractors to:
  - Implement a **Contractor Code of Business Ethics and Conduct**.
  - Establish a **Business Ethics Awareness and Compliance Program**.
  - Establish an **Internal Control System**.
  - Inform the Office of Inspector General and Contracting Officer of "**Credible Evidence**" of any Violation.

The Next Big Enforcement Area

Cybersecurity and Classified Information

FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)

- **Final Rule** Issued May 2016 (3+ years after interim rule first published)
    - Effective as of **June 15, 2016**
- Published by **DoD**, **GSA**, and **NASA**
  – But will apply to virtually all future Federal contracts
- Compliance Now **Mandatory** for All Contracts Including **Cybersecurity Clause**

FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)

- New subpart (4.19) and contract clause (52.204-21) to the Federal Acquisition Regulation (FAR)
- Basic Safeguarding of Covered Contractor Information Systems

"**For the basic safeguarding of contractor information systems that process, store, or transmit Federal contract information**."

FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)

- Intent of the Rule is to establish **basic** safeguarding measures as part of the contractor's "**routine**" business practice.
- Basic Jumping Off Point for Contractor Compliance
  - Think in terms of your **Business Ethics and Compliance Program**
- Does **Not** Impact Other Federal Safeguarding Requirements:
  - **DFARS 252.204-7012** (Safeguarding Covered Defense Information and Cyber Incident Reporting) (2016)
  - Requirements Relating to **Classified** or **Controlled Unclassified Information**

FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)

- The Rule imposes **15** "**basic" security controls** for contractors
- The Rule applies to "**covered contractor information systems**" (contractor systems that process, store, or transmit "Federal contract information")
- **Federal contract information** means information provided by **or** generated for the Government under a contract to develop or deliver a product or service for the Government, but does not include: (1) publicly available information, or (2) basic transactional information (like information required to process contractor payment applications)

The 15 Security Controls

1. Limit access to **authorized users**.
2. **Limit information system access** to the types of transactions and functions that authorized users are permitted to execute.
3. **Verify controls** on connections to external information systems.
4. **Impose controls** on information that is posted or processed on publicly accessible information systems
5. **Identify information system users and processes** acting on behalf of users or devices

The 15 Security Controls

6. **Authenticate or verify the identities of users, processes, and devices** before allowing access to an information system

7. **Sanitize or destroy** information system media containing Federal contract information before disposal, release, or reuse.

8. **Limit physical access** to information systems, equipment, and operating environments to authorized individuals.

9. **Escort visitors and monitor visitor activity**, maintain audit logs of physical access, control and manage physical access devices.

The 15 Security Controls

- 10. **Monitor, control, and protect organizational communications** at external boundaries and key internal boundaries of information systems.
- 11. **Implement sub networks** for publically accessible system components that are physically or logically separated from internal networks.
- 12. Identify, report, and correct information and information **system flaws** in a timely manner.
- 13. Provide protection from **malicious code** at appropriate locations within organizational information systems.

The 15 Security Controls

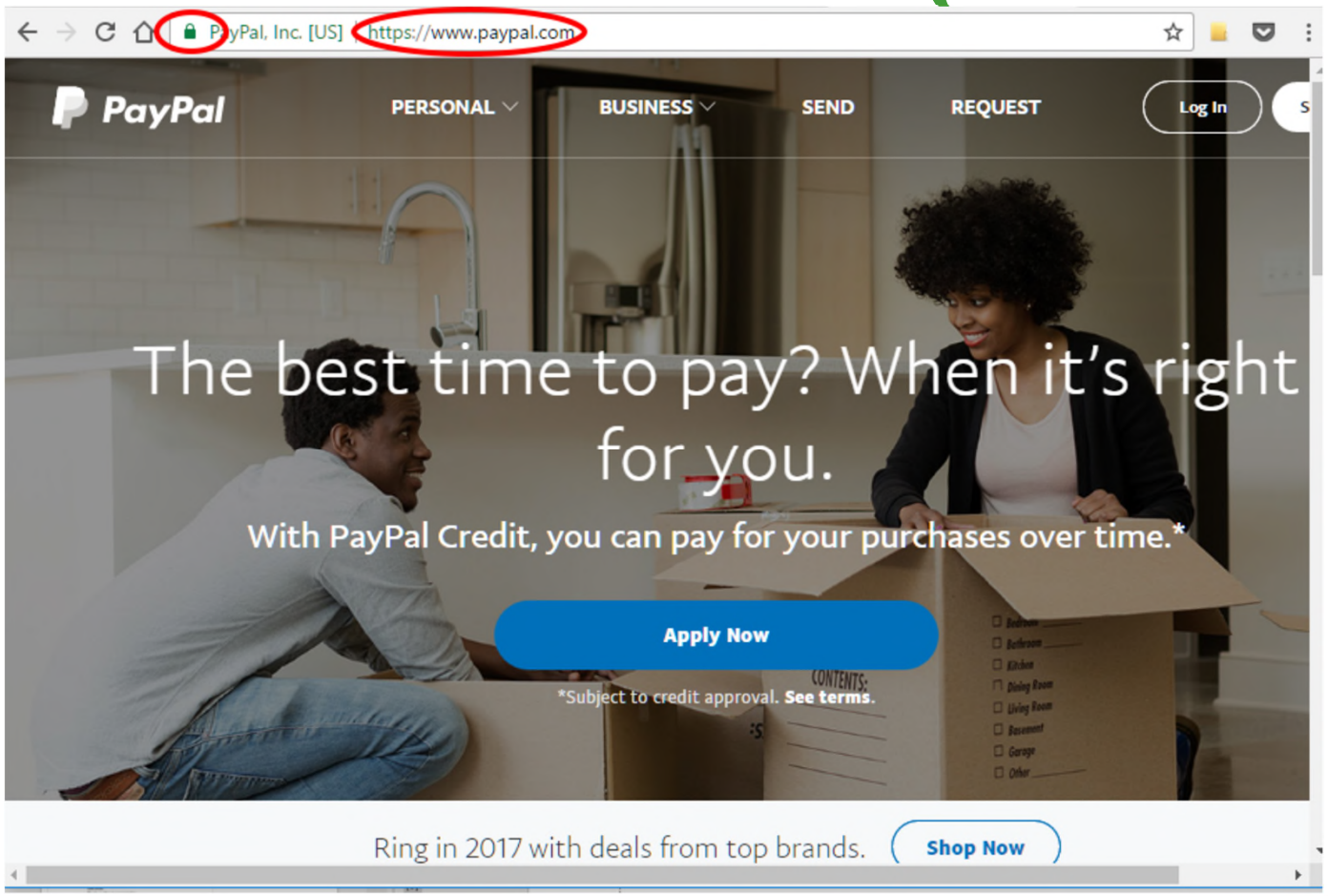
- 14. Update **malicious code protection** mechanisms when new releases are available.
- 15. Perform **periodic scans** of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. FAR 52.204-21(b).

Use of Public Wireless Connection

Public Wi-Fi

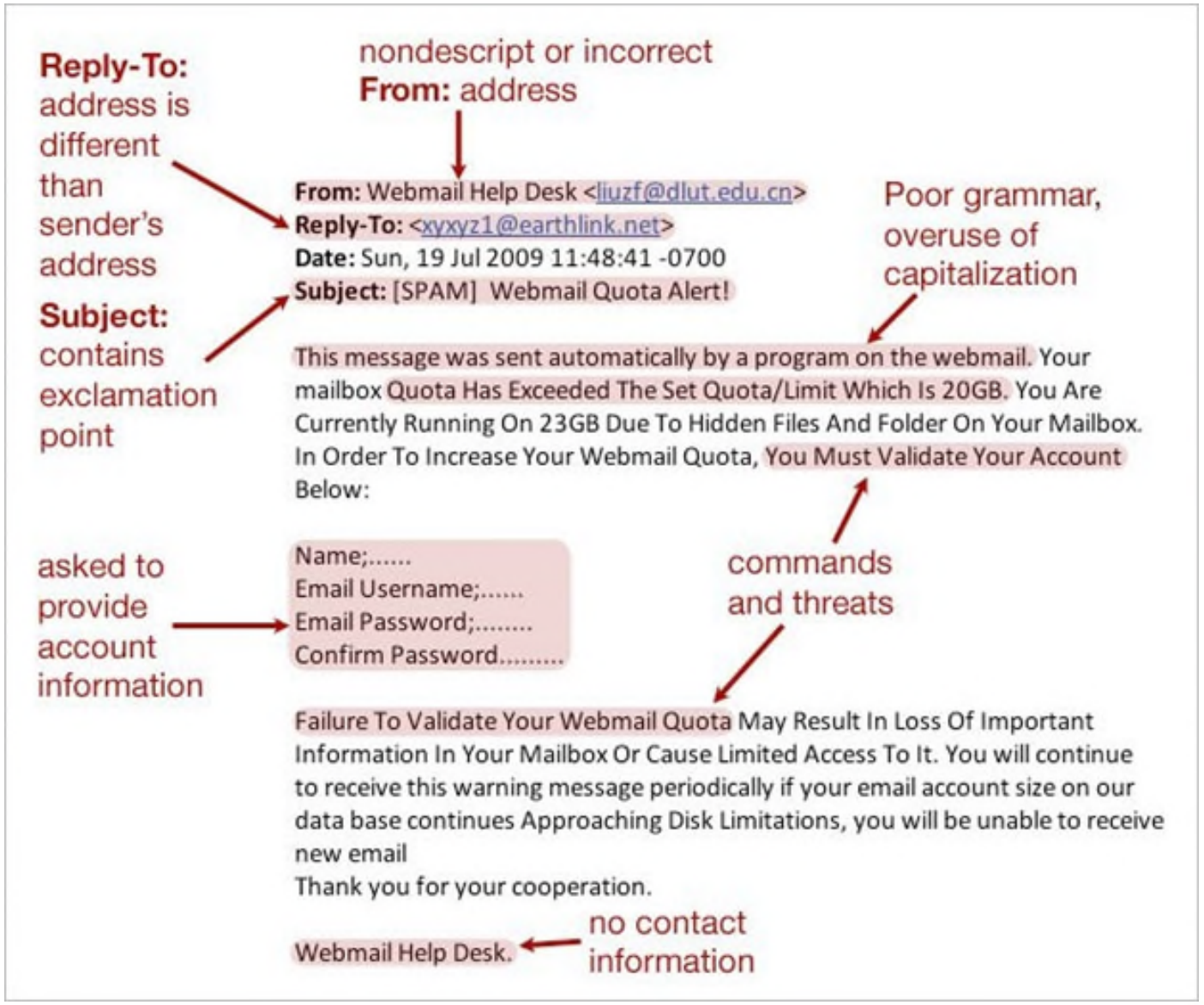
- Not all public Wi-Fi locations are secure, and your browsing maybe intercepted from your computer
- Even if encrypted connection back to work, unencrypted websites are still risky

Use of Public Wireless Connection (continued)



Common Threats Companies Face

Phishing – Spoofed Emails



Fox Rothschild LLP
ATTORNEYS AT LAW

Common Threats Companies Face (continued)

Phishing – Spoofed Emails

From: PayPal [service@paypals.co.uk] Spelling error

To: customer@paypal.co.uk Generic email

Cc:

Subject: PayPal Primary Email Address Change

Dear customer, Not personalized

The primary email for your PayPal account

If you did not authorise this change, plea

https://www.paypal.com/uk/cgi-bin/?cmd= emailchange

Domain is incorrect; it should be .co.uk not .com/uk

http://pr.atwola.com/promoclk/100001269x1115550333x1077361411/aol?redir=http://hedwigsfloridahome.co.uk/reds.htm?cgi-bin?webscr?cmd=_login-run&dispatch=5885d80a13c0db1fa798f5a5f5ae42e779d4b5655493f61722cd6b76ea2739e

Click to follow link

Link location does not match the text

Yours sincerely,
PayPal

For more information on protecting yourself from fraud, please review the Security Tips in our Security Centre.

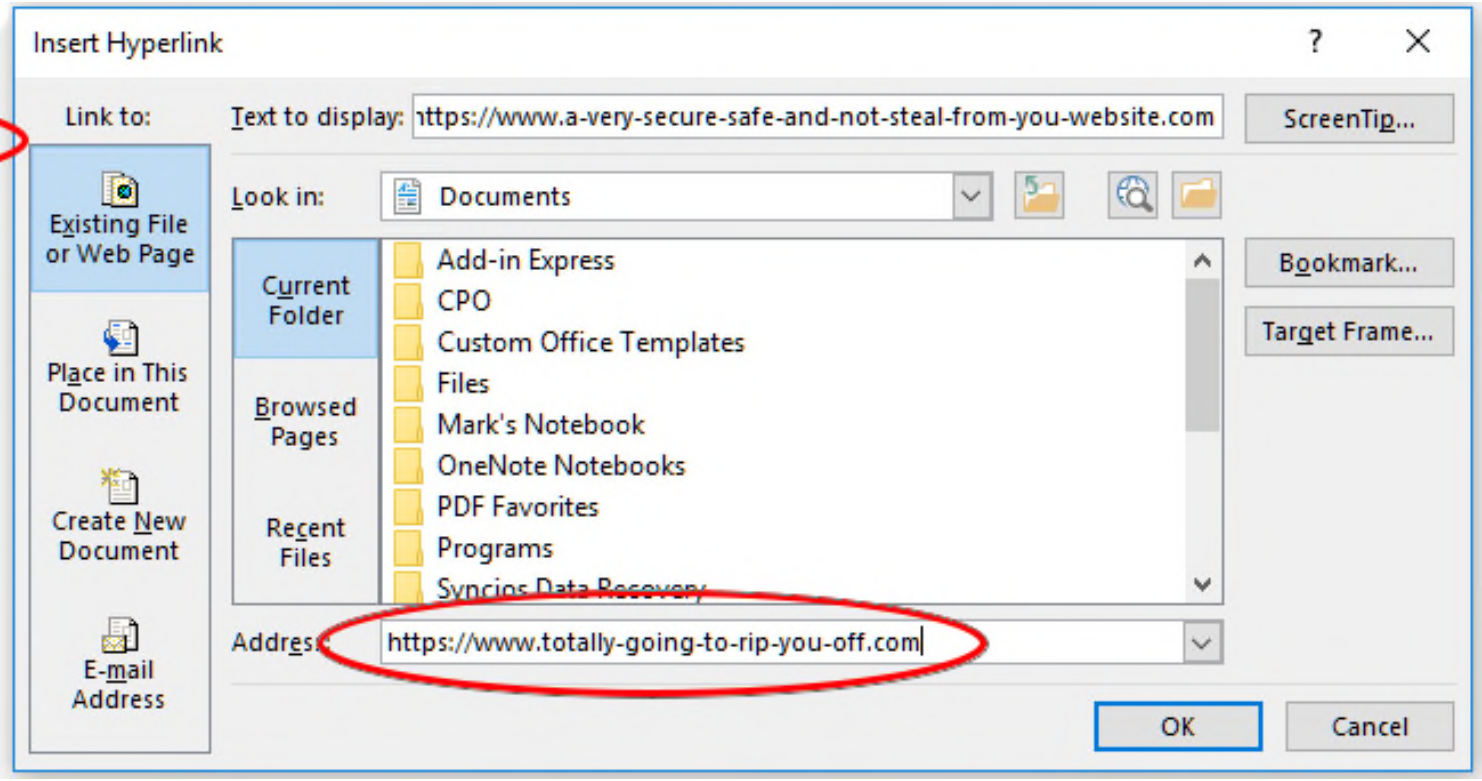
Fox Rothschild LLP
ATTORNEYS AT LAW

Common Threats Companies Face (continued)

Phishing – Spoofed Emails

https://www.a-very-secure-safe-and-not-steal-from-you-website.com

Mark McCreary, CIPP/US
Partner and Chief Privacy Officer
Fox Rothschild LLP
2000 Market Street, Twentieth Floor
Philadelphia, PA 19103-3222
(215) 299-2010 - Direct
(610) 457-7600 - Mobile
mmccreary@foxrothschild.com



Fox Rothschild LLP
ATTORNEYS AT LAW

Common Threats Companies Face (continued)

Phishing – Spoofed Emails

https://www.totally-going-to-rip-you-off.com/
Ctrl+Click to follow link

https://www.a-very-secure-safe-and-not-steal-from-you-website.com

Mark McCreary, CIPP/US
Partner and Chief Privacy Officer
Fox Rothschild LLP
2000 Market Street, Twentieth Floor
Philadelphia, PA 19103-3222
(215) 299-2010 - Direct
(610) 457-7600 - Mobile
mmccreary@foxrothschild.com

Common Threats We Face (continued)

Phishing – Check/Payroll Requests

From: Mark Silow <msilow@foxrothschild.com>
Date: April 8, 2016 at 12:07:26 PM EDT
To: <jdurling@foxrothschild.com>
Subject: Payroll
Reply-To: Mark Silow <ceo1554@aol.com>

Jean

I need you to send me a copy of our 2015 payroll

Thanks

Mark Silow

From: Edward Gillespie [mailto:egillespie@foxrothschild.com]
Sent: Tuesday, April 12, 2016 2:28 PM
To: Parker, Yvette
Subject: URGENT

Hello Yvette,

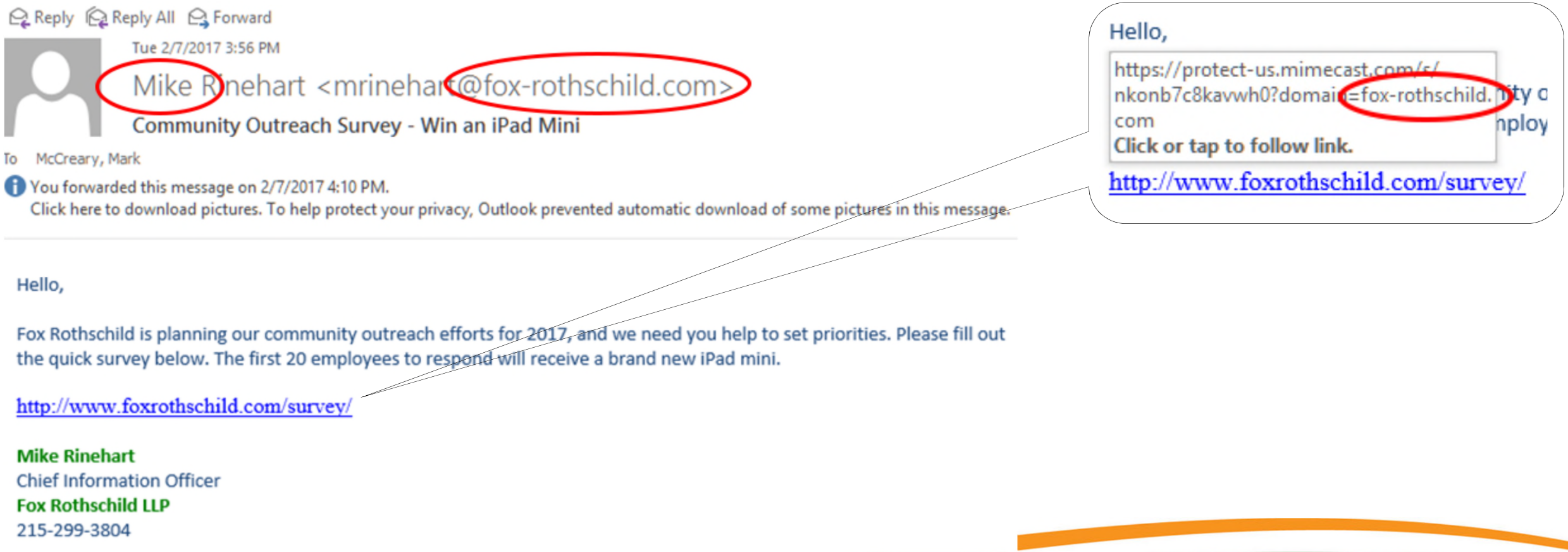
Could you please send me pdf copies of all employees 2015 W2s? I need to make a quick review and please copy: (corporateinfo@groupmail.com)

Thanks,
Edward

Sent from my iPhone

Common Threats We Face (continued)

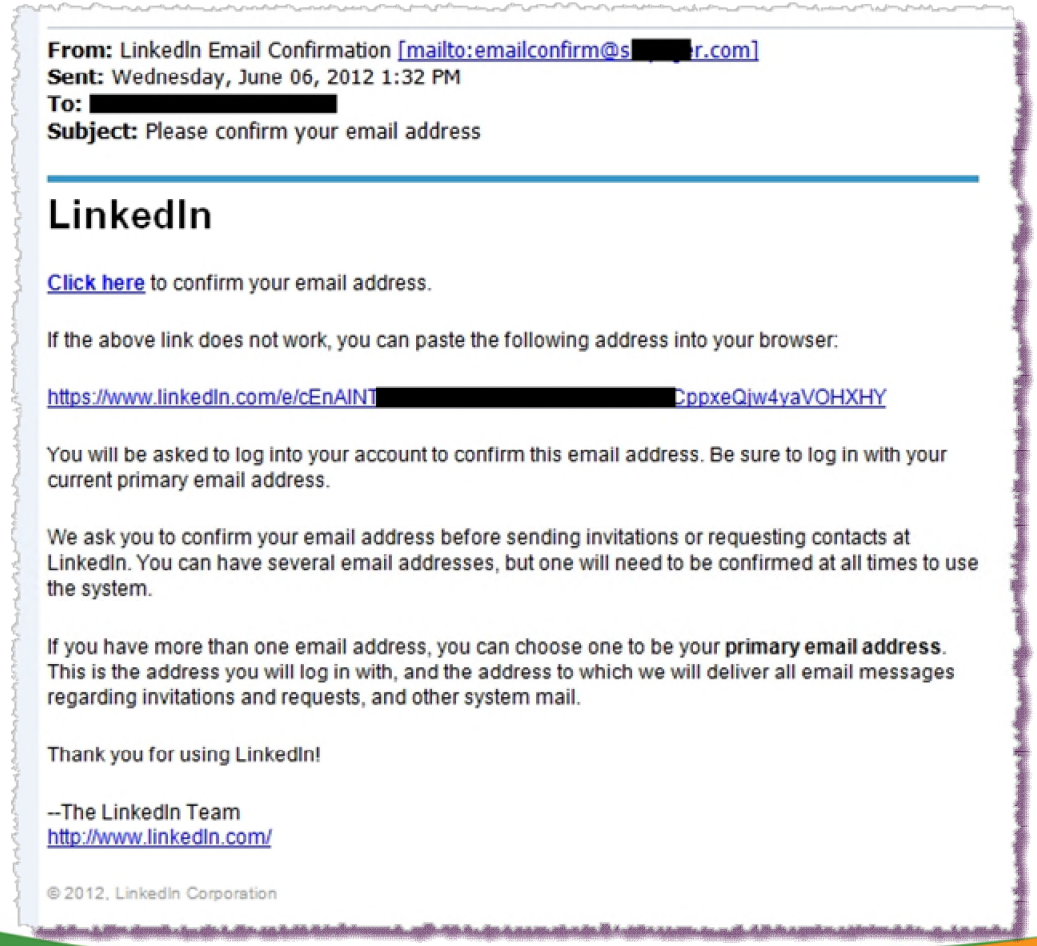
Phishing – Spoofed Emails



Fox Rothschild LLP
ATTORNEYS AT LAW

Common Threats We Face (continued)

Phishing – Username/password



From: LinkedIn Email Confirmation [mailto:emailconfirm@s[redacted]r.com]
Sent: Wednesday, June 06, 2012 1:32 PM
To: [redacted]
Subject: Please confirm your email address

LinkedIn

Click here to confirm your email address.

If the above link does not work, you can paste the following address into your browser:

https://www.linkedin.com/e/cEnAlNT[redacted]CppxeQjw4yaVOHXHY

You will be asked to log into your account to confirm this email address. Be sure to log in with your current primary email address.

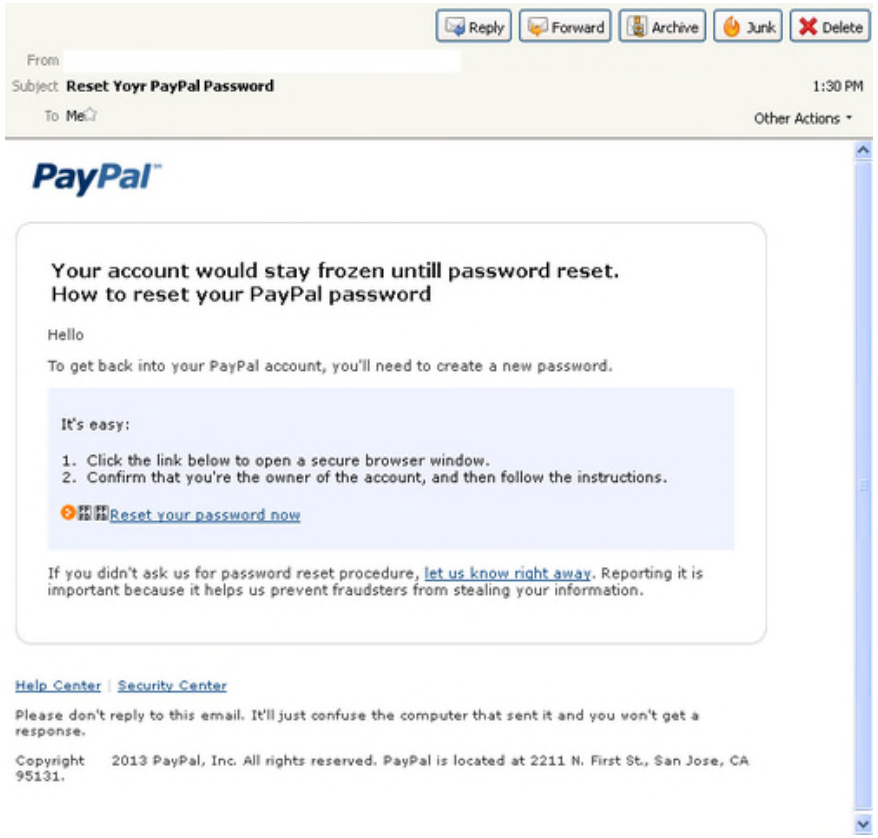
We ask you to confirm your email address before sending invitations or requesting contacts at LinkedIn. You can have several email addresses, but one will need to be confirmed at all times to use the system.

If you have more than one email address, you can choose one to be your **primary email address**. This is the address you will log in with, and the address to which we will deliver all email messages regarding invitations and requests, and other system mail.

Thank you for using LinkedIn!

--The LinkedIn Team
http://www.linkedin.com/

© 2012, LinkedIn Corporation



Reply | Forward | Archive | Junk | Delete

From
Subject **Reset Yoyr PayPal Password** 1:30 PM
To Me Other Actions

PayPal

Your account would stay frozen untill password reset.
How to reset your PayPal password

Hello

To get back into your PayPal account, you'll need to create a new password.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm that you're the owner of the account, and then follow the instructions.

Reset your password now

If you didn't ask us for password reset procedure, let us know right away. Reporting it is important because it helps us prevent fraudsters from stealing your information.

Help Center | Security Center

Please don't reply to this email. It'll just confuse the computer that sent it and you won't get a response.

Copyright 2013 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

Fox Rothschild LLP
ATTORNEYS AT LAW

Common Threats We Face (continued)

Ransomware

- Occurs when software is downloaded and executed
- Most variants have no “cure,” either pay the ransom, restore from backup, or start fresh
- On a network environment it will encrypt anything it can find, possibly making it to server environments

Common Threats We Face (continued)

Ransomware

Common Threats We Face (continued)

Ransomware

Fox Rothschild LLP
ATTORNEYS AT LAW

Firm Efforts and Policies (continued)

Secure Destruction

- Use the boxes to destroy paper with client information
- IS can assist with secure destruction of hard drives and flash drives

Secure Shredding Bin
Dimensions: 42" H X 25" W X 26" D
Max. Capacity: 210 lbs. (est.)

Security Console
Dimensions: 40" H X 19" W X 19" D
Max. Capacity: 70 lbs. (est.)

Mini Security Console
Dimensions: 27" H X 19" W X 19" D
Max. Capacity: 40 lbs. (est.)

DFARS 252.204-7012 (Safeguarding Covered Defense Information & Cyber Incident Reporting)

- Final Rule Issued October 2016
- “Covered contractor information system” means an unclassified info. system that is owned, or operated by or for, a contractor and that processes stores, or transmits covered defense info.
- “Covered defense information” means unclassified controlled technical information … as described in the Controlled Unclassified Information (CUI) registry (which is online).

DFARS 252.204-7012 (Safeguarding Covered Defense Information & Cyber Incident Reporting)

- Requires **"rapid reporting"** (i.e., 72 hours) of "cyber incidents" which result in a compromise or an actual or potentially adverse effect….
- Another DFARS, 252.239-7010, applies to Cloud Computing.
- **Requires compliance with NIST 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) by not later than December 31, 2017**.
- NIST = Department of Commerce's National Institute of Standards and Technology.

Comparison Guide

- Comparison to **DFARS Cybersecurity Provisions**
  - Many contractors will be subject to **both** the Final Rule and the DFARS Rule.
- DFARS requires far more extensive security controls and reporting requirements than the FAR clause.
  - Cyber Incident Reporting
  - Post-Incident Investigation (90 day preservation period from reporting to give DoD time to determine whether it wants to investigate and to give access to additional information and equipment)

Comparison Guide

- FAR Rule is more **limited and basic**
  - Steps a **reasonable** business should be taking irrespective of requirements
  - DFARS mandates “enhanced safeguarding,” by comparison

- FAR Rule does **not** include mandatory cyber-incident reporting, incident response, or data collection
  - No forensic analysis requirement
  - Reporting and data collection elements of the DFARS cited as most troubling for DoD contractors

- FAR Rule does **not** include NIST 800-171 requirements
  - Standard covering most government systems and the DFARS

Comparison Guide

- FAR Rule does **not** address Cloud computing
- FAR Rule does **not** include COTS element
  - Although some commercial item requirements do apply
- **More rules are coming . . .**

Federal Information Protections

Types of Federal Information Protections

Classified Information

- Confidential
- Secret
- Top Secret
  - SCI
  - Yankee White

Highest Protection

Unclassified

- Federal Contract Information
- Covered Defense Information
- FOUO
- Sensitive, but Unclassified
- Controlled Unclassified

Protected

Open Source

- Publicly available
- Website information
- Press releases
- Court filings

No Protections

Classified Information

Three levels of classified information

- Top Secret – Grave Damage
- Secret – Serious Damage
- Confidential - Damage
- Based on amount of damage to national security that would be caused by unauthorized disclosure
- To access, must have:
  - Security clearance – determination individual can access at that level
  - "Need to Know" – determination individual can access specific information
- Key facts:
  - Must be sponsored for clearance
  - DoD framework - DSS / OPM runs process
  - Facilities Clearance
  - Can lose clearance / Penalties for violations

Unclassified / Open Source Information

- **Unclassified Information**
- Requires safeguarding or dissemination controls
  - Marked or otherwise identified sensitive information and provided by DoD
  - Collected, provided, or stored in support of contract
- Not free to disseminate to anyone
- To access, must have:
  - "Need to Know" – determination individual can access specific information
  - No clearance required
- **Open Source Information**
  - Available to anybody
  - No clearance or "need to know" required
  - Can disseminate freely

Penalties for Failing to Comply with Cyber Security Requirements

Fox Rothschild LLP
ATTORNEYS AT LAW

Broad Penalties Addressed for Noncompliance

- Two kinds:
  - Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and
  - Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause
- United States as claimant:
  - False Claims Act
  - Suspension and Debarment
  - Breach of Contract / Default Termination
- Third party as claimant
  - Qui tam case – whistleblower
  - Various breach of contract or tort claims

False Claims Act – Once is Never Enough

Civil False Claims Act - 31 U.S.C. §§ 3729 *et seq.*

- Key government anti-fraud weapon - $5,000 - $11,000 per violation
- Prohibits submitting false documents or information to government
- **Three types of False Claims**
  - Direct False Claim
    - Knowingly presenting or causing to be presented a false claim
  - False Statement
    - Knowingly making, using or causing to be made or used a false record / statement material
  - Reverse FC
    - Knowingly concealing or decreasing an obligation to pay money to Government

False Claims Act – Once is Never Enough

- Elements of a False Claim
  - A "**Claim**" is any request for money or property submitted to government
    - Multiple requests = multiple false claims
  - Claim Must be submitted "**Knowingly**" to government
    - Know of falsity
    - Acts in deliberate ignorance of truth/falsity
    - Acts in reckless disregard of truth/falsity
  - Don't need intent to defraud government – irrelevant
  - No such thing as innocent mistake

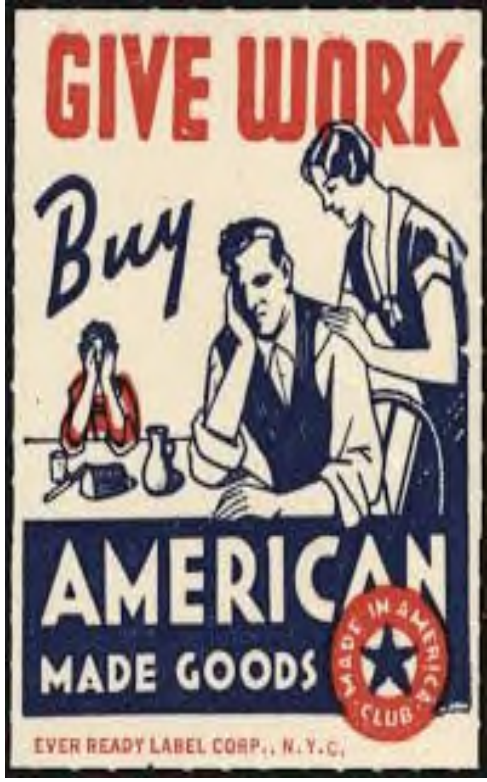
Predicting the Direction for the New Administration

Fox Rothschild LLP
ATTORNEYS AT LAW

Highlights of Proposed Actions

- **Increased Defense Spending**
  - $54 billion increase (proposed) for cyber, personnel, ships, special operations, etc.
- **Investment in Infrastructure**
  - $1 trillion in infrastructure investment over 10 years (proposed)
- **Regulatory Reform**
  - Two for One Reduction on Existing Regulations
- **Tax Reform**
  - Lower corporate rate to 15%

Buy American, Hire American



- **Executive Order** Signed April 19, 2017
- No changes to existing law – policy change only
- Requires all federal agencies to:
  - Hire American – “rigorously enforce” laws on hiring foreign workers
    - Suggest reforms to use H-1B Visas for “most skilled workers”
  - Buy American – “scrupulously monitor and enforce Buy American Laws”
    - Assess all practices on BAA
    - “Maximum utilization of goods, products, materials” produced in US
    - Minimize use of waivers for BAA for public interest

Fair Pay, Safe Workplaces - REPEALED

- Obama Executive Order from 2014 – "Blacklisting" Order
  - Required self-disclosure of labor law violations from past 3 years
  - Crackdown on repeat offenders – no contract
  - Paycheck data on hours worked, OT, pay, deductions, etc.
  - Banned forced arbitration clauses for discrimination claims
- **Eliminated** on March 27, 2017
  - Viewed as not pro-business
  - Improperly excluded contractors from competing for minor violations

SBA “All Small” Program

- **Major Policy Shift** by the Small Business Administration
  - **Vastly expands** access to set-aside contracts previously reserved for performance **only by small businesses.**
- **All** Government Contractors – **Small and Large** – need to create a **game plan** for how to take advantage of this shifting landscape
- **Application Period Open** (and has been since October 2016)

SBA "All Small" Program

- Small Business Protégés may Joint Venture with Large Business Mentors – **Without Fear of Affiliation**.
  - Including small business set-aside contracts
  - Protégé must qualify as small for the procurement.
- Previously, this **Shield** from Affiliation was Reserved Only for the **8(a) Mentor Protégé Program**.
- Now, **all** small businesses Have the Opportunity to Form SBA Approved Mentor-Protégé Teams with Larger Businesses.
  - **HubZone, Women-Owned Small Business (WOSB and EDWOSB), and Service-Disabled Veteran Owned Small Business (SDVOSB)**

Mentor-Protégé Agreement & Joint Venture Regulation Update

- **Written Mentor-Protégé Agreement** is **Required**
  - Must address how assistance provided will help the protégé firm meet its goals as defined in its **business plan**
- The SBA **must approve** the joint venture **in advance**
  - JV Agreement must satisfy the requirements of **another** new SBA regulation (13 C.F.R. 125.8)
- SBA also **overhauls** Mentor-Protégé JV Requirements
  - Certifications & Reports trigger **FCA warning**

SBA “All Small” Program

- **The Unknown**: Translation from on-paper to in-practice
- We anticipate that small businesses (including SDVOSBs, HUBZones, and WOSBs) will face **heavily increased competition** on set-aside contracts from peers now backed by the support and assistance of a large business
- **Strategic Considerations**:
    - Access to Set-Aside Programs
    - Left Out in the Cold without a Dance Partner?

**Reggie Jones, Mark McCreary,
Doug Hibshman, & Nick Solosky**

Fox Rothschild LLP
ATTORNEYS AT LAW

www.FoxRothschild.com

202-461-3101

Fox Rothschild LLP
ATTORNEYS AT LAW