THE TWENTY-SECOND NATIONAL

HIPAA SUMMIT

FEBRUARY 5 – 7, 2014, WASHINGTON, DC

CYBER ATTACKS AND HIPAA COMPLIANCE: PREPARED?

China. Target. Coke…

What next? Who?

Ali Pabrai

ecfirst

Agenda

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

- **Challenge**: *Learning* from:
  - Shanghai attacks
  - Target breach
  - Coke compromised
- **Checklist**: Establishing a *credible* Program
  - Plan
  - Policy
  - Controls

ecfirst

Unit 61398 in Shanghai

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

Critical Background Summary

Mandiant, a US-based computer security firm, reported:

- APT1, an organization in China focused on cyber espionage
- Mandiant traced the hacking activities of APT1 to the site of 12-storey building in the Pudong area of Shanghai
  - It said that Unit 61398 of the PLA "is also located in precisely the same area" and that the actors had similar "missions, capabilities and resources"
- Staffed by hundreds, possibly thousands, of proficient English speakers with advanced computer security and networking skills
- Hacked into 141 companies across 20 industries, 87% based in English-speaking countries, and is able to steal from dozens of networks simultaneously
- Stolen hundreds of terabytes of information including blueprints, business plans, pricing documents, user credentials, emails and contact lists

Stayed inside hacked networks for an average of 356 days, with the longest lasting 1,764 days

ecfirst

Target breach

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

The Wall Street Journal/The New York Times, Dec 2013-Jan 2014

- POS malware compromises cash registers that monitor card authorization process
- RAM-scrapping malware steals unencrypted data from memory
- Stolen information copied to a compromised internal system & transmitted outside
- Before a transaction can be authorized, card data is momentarily decrypted & stored in memory (RAM)
- 110 million impacted
- Senior Target executives, including CFO, are witnesses in federal committee hearings

Demand for hackers with POS malware expertise fast rising

ecfirst

breach bottom-line

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

Malware

- Eastern European/Russian hackers wrote the malicious program known as BlackPOS
- BlackPOS is a specialized piece of malware designed to be installed on POS devices
- It records all data from credit & debit cards swiped through the infected system

How was it done?

Step 1: Compromised Target Web server & then got the malware BlackPOS into POS devices

Step 2: Installed on POS devices & recorded all data from credit & debit cards swiped through the infected system

Step 3: Information temporarily stored on a compromised system; then trasmitted outside

ecfirst

Neiman marcus breach

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

The New York Times (Jan 27, 2014)

- Breach was deeper than previously reported
- Hackers invaded systems for several months
- 1.1 million cardholders impacted
- POS malware installed on NM stores appeared to be same malware that infiltrated Target
- NM data stolen from July 16 thru Oct 20, 2013
- NM not aware of breach until mid-Dec 2013

Bottom-line Fact:

50% of Fortune 1000 firms each year experience a breach of 1,000 to 100,000 confidential records, including those of employees

Ponemon Institute (The New York Times, Jan 27, 2014)

ecfirst

Coke compromised

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

The New York Times (Jan 27, 2014)

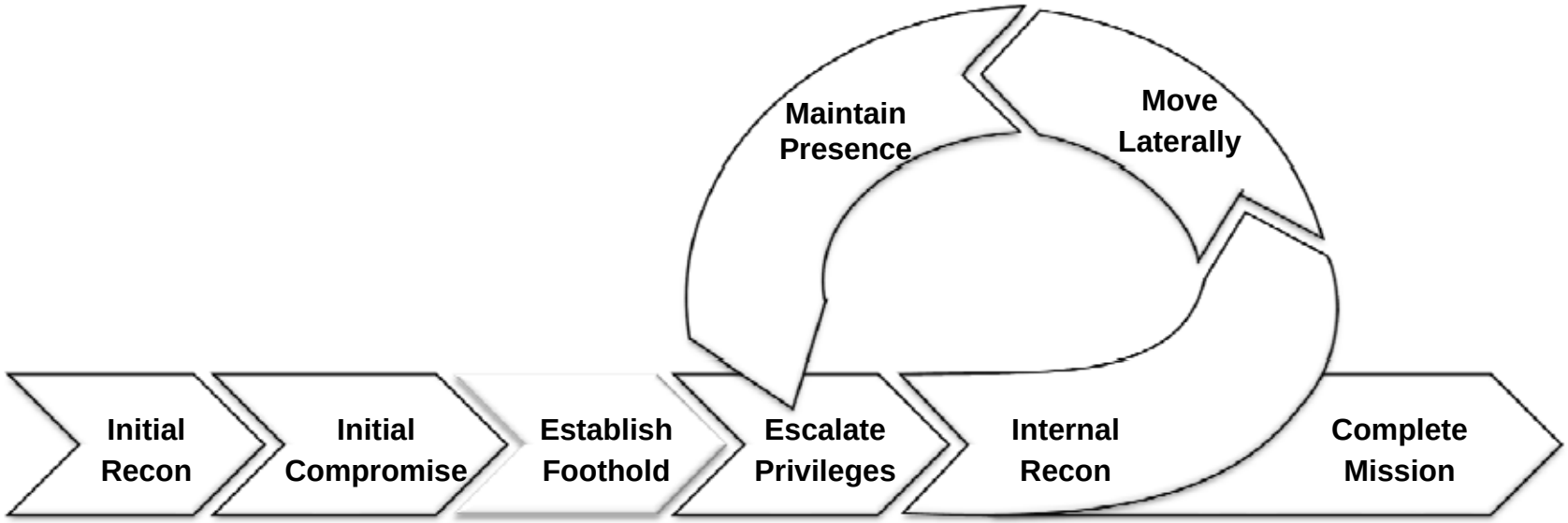
- PII on 70,000 workforce members compromised (including contractors, vendors)
- Data not encrypted stolen by a former worker responsible for maintaining & disposing of company equipment
- Recovered 55 company laptops in Nov/Dec 2013, stolen over 6 years
- *Breach discovered* Dec 10, 2013
- Senior executive leaves Dec 12, 2013
- *Breach disclosed* Jan 23, 2014
- Coke assesses over 200,000 files on recovered computers to determine whose PII had been breached
- Stolen computers belonged to employees who worked in HR & had access to HR records

Insider threats must be within scope of risk analysis

ecfirst

Chinese attack lifecycle

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT



ecfirst

Chinese attack malware tools

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

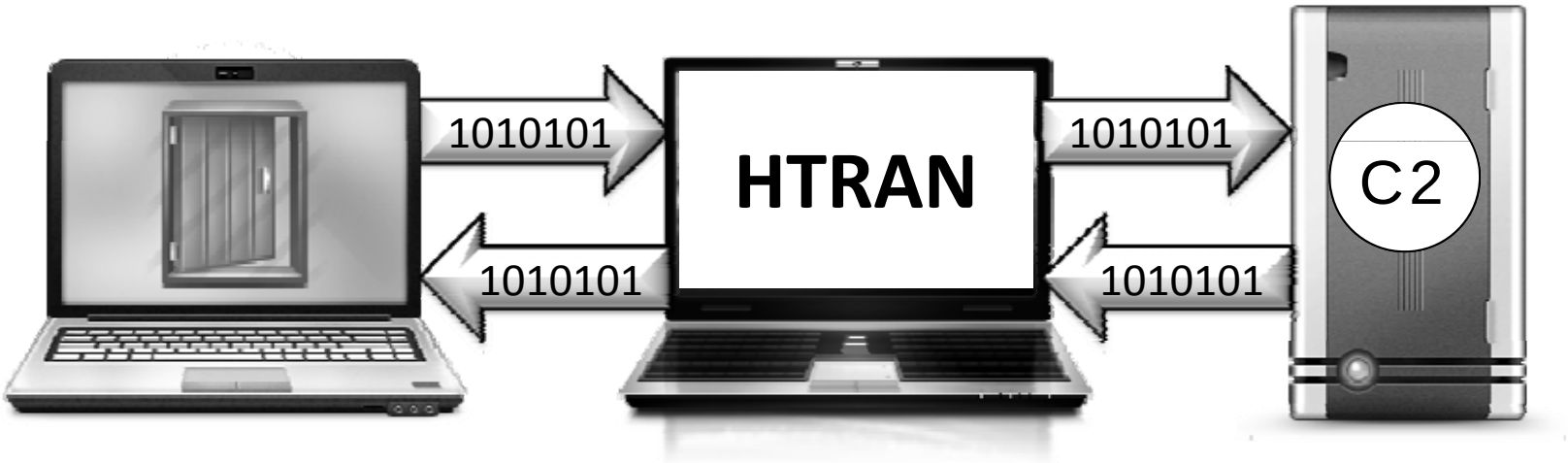
- APT1 developed specialized malware tools, organized into malware families
- Each tool behaves differently, once deployed
- Malware families evolve with time, and have specific backdoor capabilities, that are enhanced
- Partial examples of Chinese malware attack function categories include:
  - Capture keystroke
  - Capture mouse stroke
  - Change directories
  - Create processes
  - Create/modify files
  - Download/execute files from a specified address
  - Establish connection
  - Kill processes
  - List processes
  - Log off currently logged-in user
  - Open listening port
  - Set sleep interval
  - Route network traffic

Emblem of the People's Liberation Army

ecfirst

backdoors

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

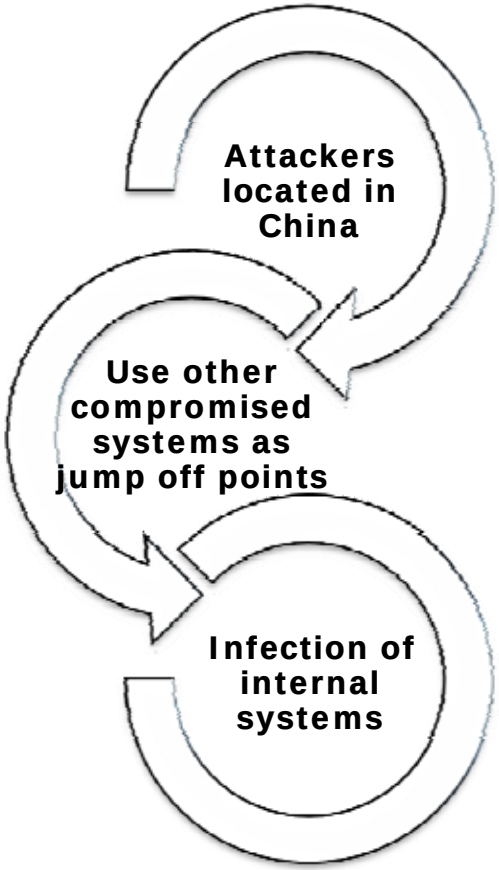


The HTRAN tool resides on APT1 hop points and acts as a middle-man

ecfirst

Anatomy of an attack

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT



- Customized emails sent to internal employees
- Contain malware leading to an initial infection

Spear-phishing attack

Backdoor Installation

- Provides continuous unrestricted access
- Compromised systems used as "pivot" points to attack other internal systems

- Custom code to search for "interesting" data
- Outbound connections are often not monitored, leading to data loss

Data Exfiltration

ecfirst

Successful attacks!

- **Coca Cola**: Code in a malicious email, sent to an executive, allowed **hackers to operate undetected**, logging commercially sensitive information

- **Apple**: Breach occurred when some employees visited a developer website that exploited a vulnerability in the Java browser plug-in, **installing malware on Mac computers**

- **Google**: Subjected to a "sophisticated cyber attack originating from China"; email accounts of human rights activists were hacked

- **NASA**: Victim of 47 cyber attacks traced to IP addresses in China; accessed computers at JPL, which controls NASA's robots in space; **hackers accessed sensitive accounts**; could create, delete & modify systems & accounts and upload hacking software

- **Lockheed Martin**: Hackers broke into Lockheed Martin computers & took large amounts of data on the Joint Strike Fighter, the most advanced warplane in the world

- **NYT**: Attacks bore hallmarks of previous Chinese hacks, including being routed through the same university computers

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

Compliance & Security Controls

"Cyber threat to our nation is one of the most serious economic and national security challenge we face."
President Obama

ecfirst

Security Controls Implemented

Your current state?

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

Key Security Controls	
Implemented	Missing
Firewall *(Sonic Firewall TZ210)*	Two-factor authentication
IDS *(Dell SecureWorks)*	DLP
Antivirus protection *(Webroot)*	Secure text messaging
Data transfer *(SFTP, HTTPS)*	USB & portable device encryption
Remote access *(VPN, Citrix)*	MDM
Asset management *(Dell KACE)*	
Laptop encryption *(TrueCrypt at the Bios Level; Windows OS & File Vault on Mac OS)*	
Email encryption *(Voltage)*	

ecfirst

Firewalls: First Line of DefenSe!

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

- It starts with the firewall configuration standard
  - Is there a formal process for approving and testing all external network connections and changes to the firewall configuration?
  - Does a current network diagram with all connections, including any wireless networks?
  - What are the requirements for a firewall at each Internet connection and between any DMZ and the internal network zone?
  - Is there a documented list of services and ports necessary for business?
  - What is the justification and documentation for any risky protocols allowed (for example, FTP), which includes reason for use of protocol and security features implemented?
  - Is there a formal review of firewall and router rule sets? At what frequency? Who is responsible? Who is accountable?
  - What are your configuration standards for communication devices such as routers, switches, access points, and others?
- **Key** - disable all unnecessary and insecure services & protocols

ecfirst

Anti-virus: A Key Control!

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

- Many vulnerabilities & malicious viruses enter the network via employees' email activities
- Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software
- Deploy anti-virus software on all systems commonly affected by viruses (particularly end systems & servers)
- Ensure that anti-virus programs are capable of detecting, removing, & protecting against other forms of malicious software, including spyware & adware
- **Key**: Ensure that all anti-virus mechanisms are current, actively running, & capable of generating audit logs

ecfirst

Audit Control: Key for HITECH!

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

- Establish a process for linking all access to system components (especially privileged access)
- Implement automated audit trails for all system components to reconstruct the incident event
- Secure audit trails so they cannot be altered
  - Limit viewing of audit trails to those with a job-related need
  - Protect audit trail files from unauthorized modifications
  - Promptly back-up audit trail files to a centralized log server or media that is difficult to alter
- **Key**: Review logs for all system components at least **????**
- **Key**: Retain audit trail history for at least one year, with a minimum of three months online availability

ecfirst

Encryption: last line of defenSe!

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

- The use of an algorithmic process to transform data into a form in which there is a *low probability* of assigning meaning without the use of a confidential process or key

Compliance Mandates

- Encryption & Decryption (*Data @ Rest*)

  Implement a mechanism to encrypt & decrypt PII
- Encryption (*Data in Motion*)

  Implement mechanism to encrypt PII when deemed appropriate

The bottom-line: What is your enterprise standard for encryption?

ecfirst

Unsecured PII
Breach Notification Mandate

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

- Organizations must provide the required breach notification if the breach involved unsecured PII

- Unsecured PII that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or specified methodology

The bottom-line: Encrypt or destroy!

Document what PII you process, where!

ecfirst

ISO 27002 Updates

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

ISO 27002: 2005	ISO 27002: 2013
Security Policy	Information Security Policies
Organizing Information Security	Organization of Information Security
Asset Management	Human Resource Security
Human Resources Security	Asset Management
Physical & Environmental Security	Access Control
Communications & Operations Management	**Cryptography**
Access Control	Physical & Environmental Security
Information Systems Acquisition, Development & Maintenance	Operations Security
Information Security Incident Management	Communications Security
Business Continuity Management	System Acquisition, Development & Maintenance
Compliance	**Supplier Relationships**
	Information Security Incident Management
	Information Security Aspects of Business Continuity Management
	Compliance

Pci dss requirement 12.2

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

PCI DSS Requirements	Testing Procedures
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).
12.1.1 Addresses all PCI DSS requirements.	**12.1.1** Verify that the policy addresses all PCI DSS requirements.
12.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 & NIST SP 800-30).	**12.2.a** Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.
	12.2.b Review risk assessment documentation to verify that the risk assessment process is performed at least annually & upon significant changes.

NIST SP 800-30

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

ecfirst

Taoguang yanghui

THE TWENTY-SECOND NATIONAL HIPAA SUMMIT

"The true organization is so prepared for battle that battle has been rendered unnecessary."

"Much strategy prevails over little strategy, so those with no strategy cannot but be defeated (defenses penetrated). Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win."

Sun Tzu, The Art of War

Taoguang yanghui, is a Chinese saying, "*hiding capabilities & bidding one's time*"

ecfirst

Pabrai's Laws of Information Security
Is Your security, Kismet or Karma?

1. There is no such thing as a 100% secure environment
2. Security is only as strong as your weakest link
3. Security defenses must be integrated and include *robust* (passive) and *roving* (active) controls to ensure a *resilient* enterprise
4. Security *incidents* provide the foundation for security *intelligence*

Is Your Enterprise Security & Compliance Program?

Kismet – A Reactive Security Framework

Karma – A Proactive Security Framework

ecfirst

Next steps

1. Assign responsibility & authority
2. Conduct risk analysis, technical vulnerability assessment
3. Develop an enterprise security plan, policies & procedures
4. Assess your security controls & enhance capabilities
5. Ensure business associates comply continually
6. Deliver comprehensive training to workforce members
7. Evaluate

Treat security & compliance as a life-cycle, a process baked in

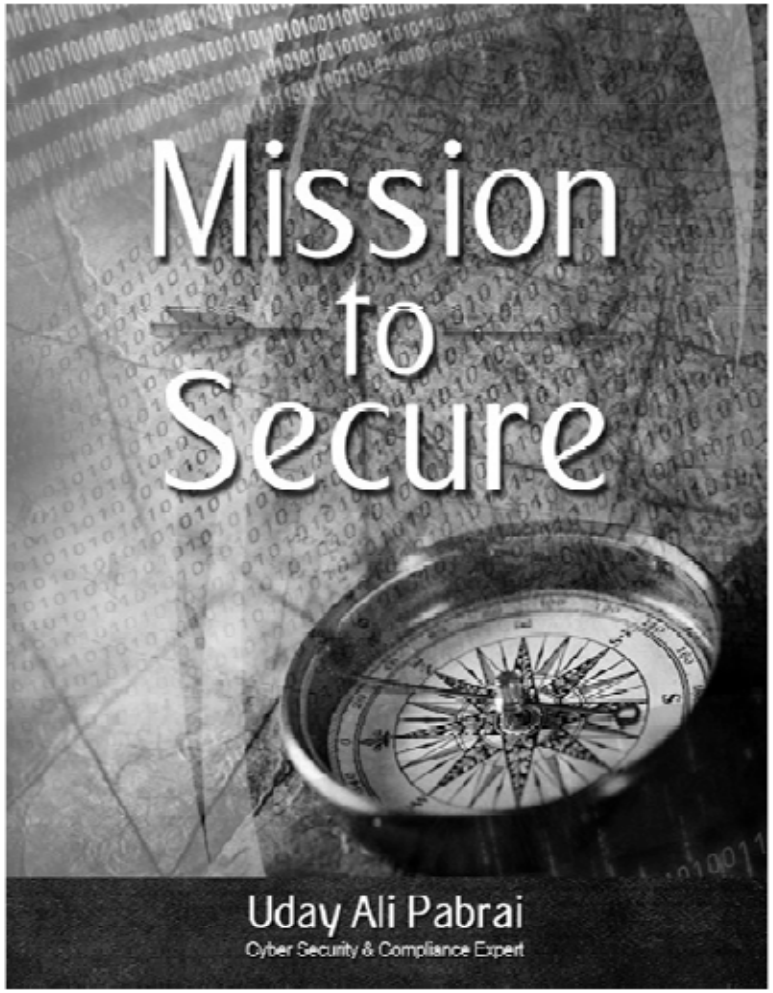
ecfirst

Questions?

Are we excited?

ecfirst

PDF Brief Now Available!
www.ecfirst.biz



- Cyber security
- Enterprise Security Plan
- Summary of HIPAA Fines & CAP
- Checklist for enterprise security
- Breach management
- Policy checklist

& a lot more

ecfirst

ecfirst
Compliance & Security

Over 2,100 clients served including **Microsoft, Cerner, HP, State of Utah, PNC Bank, IBM, Kaiser & hundreds of hospitals, government agencies, business associates in India, Philippines**

ecfirst

CHP Certified HIPAA Professional

HIPAA Academy

Manila, Philippines
May 13-14, 2014

Denver
May 13-14, 2014

Washington, D.C.
July 22-23, 2014

Las Vegas
Nov 18-19, 2014

From this training, you will learn the following about HIPAA:

- Step through all major sections of HIPAA, HITECH and the Omnibus Final Rule
- Review of the HITECH Act and how it effects all organizations with access to health information
- Examine the HIPAA Privacy and Security Rules; HIPAA Transactions Code Sets and Identifiers
- Review HIPAA compliance challenges; walk through best practices for addressing HIPAA/HITECH mandates
- Step through how to plan and prepare for HIPAA compliance

ecfirst

CSCS™
CERTIFIED SECURITY COMPLIANCE SPECIALIST

Manila, Philippines
May 15-16, 2014

Denver
May 15-16, 2014

Washington, D.C.
July 24-25, 2014

Las Vegas
Nov 20-21, 2014

From this compliance and security training program you will:

- Examine HITECH & the HIPAA Security Rule, including new Final Rule updates
- Learn about FISMA, NERC CSS, & GLBA
- Step through the core requirements of PCI DSS.
- Analyse the international security standard, ISO's 27001, ISO 27002, ISO 27799 & others.
- Examine California's SB 1386, SB 541, AB 1950, AB 1298, AB 211 & other U.S. State information security related regulations.
- Understand NIST security standards

ecfirst

Ali Pabrai
MSEE, CISSP (ISSAP, ISSMP)

Information Security & Compliance Expert

- Consults extensively with technology firms, government agencies and business associates
- Created *biz*SHIELD^{tm} – *an ecfirst Signature Methodology* - to address compliance and information security priorities
- Featured speaker at compliance and security conferences worldwide
- Presented at Microsoft, Kaiser, Intuit, E&Y, Federal & State Government agencies & many others
- Established the HIPAA Academy & CSCS Programs – gold standard for cyber security & compliance solutions
- Member InfraGard (FBI)
- Daily Compliance Tips: www.facebook.com/ecfirst
- www.facebook.com/Pabrai.

Did you get information of value from this brief?
"Like" ecfirst on

ecfirst

Thank you!

Pabrai@ecfirst.com
Cell: +1.949.528.5224