This presentation was prepared exclusively for the benefit and internal use of the J.P. Morgan client to whom it is directly addressed and delivered (including such client’s subsidiaries, the “Company”) in order to assist the Company in evaluating, on a preliminary basis, the feasibility of a possible transaction or transactions and does not carry any right of publication or disclosure, in whole or in part, to any other party. This presentation is for discussion purposes only and is incomplete without reference to, and should be viewed solely in conjunction with, the oral briefing provided by J.P. Morgan. Neither this presentation nor any of its contents may be disclosed or used for any other purpose without the prior written consent of J.P. Morgan.

The information in this presentation is based upon any management forecasts supplied to us and reflects prevailing conditions and our views as of this date, all of which are accordingly subject to change. J.P. Morgan’s opinions and estimates constitute J.P. Morgan’s judgment and should be regarded as indicative, preliminary and for illustrative purposes only. In preparing this presentation, we have relied upon and assumed, without independent verification, the accuracy and completeness of all information available from public sources or which was provided to us by or on behalf of the Company or which was otherwise reviewed by us. In addition, our analyses are not and do not purport to be appraisals of the assets, stock, or business of the Company or any other entity. J.P. Morgan makes no representations as to the actual value which may be received in connection with a transaction or the legal, tax or accounting effects of consummating a transaction. Unless expressly contemplated hereby, the information in this presentation does not take into account the effects of a possible transaction or transactions involving an actual or potential change of control, which may have significant valuation and other effects.

Notwithstanding anything herein to the contrary, the Company and each of its employees, representatives or other agents may disclose to any and all persons, without limitation of any kind, the U.S. federal and state income tax treatment and the U.S. federal and state income tax structure of the transactions contemplated hereby and all materials of any kind (including opinions or other tax analyses) that are provided to the Company relating to such tax treatment and tax structure insofar as such treatment and/or structure relates to a U.S. federal or state income tax strategy provided to the Company by J.P. Morgan. J.P. Morgan's policies on data privacy can be found at http://www.jpmorgan.com/pages/privacy.

J.P. Morgan’s policies prohibit employees from offering, directly or indirectly, a favorable research rating or specific price target, or offering to change a rating or price target, to a subject company as consideration or inducement for the receipt of business or for compensation. J.P. Morgan also prohibits its research analysts from being compensated for involvement in investment banking transactions except to the extent that such participation is intended to benefit investors.

**IRS Circular 230 Disclosure:** JPMorgan Chase & Co. and its affiliates do not provide tax advice. Accordingly, any discussion of U.S. tax matters included herein (including any attachments) is not intended or written to be used, and cannot be used, in connection with the promotion, marketing or recommendation by anyone not affiliated with JPMorgan Chase & Co. of any of the matters addressed herein or for the purpose of avoiding U.S. tax-related penalties.

J.P. Morgan is a marketing name for investment banking businesses of JPMorgan Chase & Co. and its subsidiaries worldwide. Securities, syndicated loan arranging, financial advisory and other investment banking activities are performed by a combination of J.P. Morgan Securities LLC, J.P. Morgan Limited, J.P. Morgan Securities plc and the appropriately licensed subsidiaries of JPMorgan Chase & Co. in EMEA and Asia-Pacific, and lending, derivatives and other commercial banking activities are performed by JPMorgan Chase Bank, N.A. J.P. Morgan deal team members may be employees of any of the foregoing entities.

This presentation does not constitute a commitment by any J.P. Morgan entity to underwrite, subscribe for or place any securities or to extend or arrange credit or to provide any other services.
After attending this session, you will better understand

- PCI compliance and data security
- The latest technology available to help reduce fraud
- How to increase card acceptance among patients without compromising patient satisfaction
- How to introduce card payments into the patient registration process
## Threats outpacing most organizations

<table>
<thead>
<tr>
<th>9x</th>
<th>The number of cyber attacks in the U.S. has increased ninefold in the last six years¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>58.4</td>
<td>In 2013, there were an estimated 58.4 million unique new strains of malware deployed²</td>
</tr>
<tr>
<td>619</td>
<td>619 breaches reported in 2013; an increase of 31% from 2012³</td>
</tr>
<tr>
<td>863,860,240</td>
<td>Records that were breached in 4,214 data breaches between 2005 and 2013⁴</td>
</tr>
<tr>
<td>89%</td>
<td>Percentage of companies NOT fully compliant with all 12 PCI standard requirements in 2013⁵</td>
</tr>
</tbody>
</table>

Sources:
1. Redwood Capital Market Analysis—Feb 2014
2. Aite Group, Cyberthreats: Multiplying Like Tribbles, October 2013
3. ITRC Breach Report 2013
4. Privacy Rights Clearinghouse
5. Verizon 2014 PCI Compliance Report
PCI in brief

- Data security standards created and maintained by the Payment Card Industry Security Standards Council (PCI SSC)
- Applies to any system that stores, processes or transmits card data
- 12 requirements addressing operational and technical areas
- Specific technology guidelines for encryption and tokenization

Organizations often need to combine multiple technologies to secure data and meet PCI requirements
The prioritized approach

- Six milestones
  1. If you don’t need it, don’t store it
  2. Secure the perimeter
  3. Secure applications
  4. Monitor and control access to your systems
  5. Protect stored cardholder data
  6. Finalize remaining compliance efforts, and ensure all controls are in place

- Tools and guidance on the PCI SSC Web site
### What is “Compliance”

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic compliance</td>
<td>The act of complying; The state of being compliant; The tendency of conforming with or agreeing to the wishes of others</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>A situation in which an agency fully meets the requirements of laws, rules and regulations and court cases (SOX, HIPAA, GLBA, etc.)</td>
</tr>
<tr>
<td>Professional compliance</td>
<td>Acting according to certain accepted standards “their financial statements are in conformity with generally accepted accounting practices” (GAAP, Professional Code of Conduct)</td>
</tr>
<tr>
<td>Internal compliance</td>
<td>The ability to reasonably ensure conformity and adherence to organization policies, plans, procedures, laws, regulations, and contracts</td>
</tr>
<tr>
<td>PCI compliance</td>
<td>Compliance to the Payment Card Industry, Visa and MasterCard regulatory bylaws, specifically cardholder information security (PCI DSS, PA-DSS, SDP, CISP, etc)</td>
</tr>
</tbody>
</table>
What is “Information security”

- Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction

- An all encompassing term that refers to the security of the information systems that are used and the data that is processed

- The securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organization

- Preservation of the confidentiality, integrity and availability of information

- Situation in which information security risks are under control

- The implementation of programs and practices that protect the integrity and safety of computer programs and information
Why NOT compliance?

New “compliance” mandates are potentially endless

- Government regulation
- Industry standards
- Company policies

Achieving compliance is easier than maintaining compliance

- Becoming compliant is a project
- Maintaining compliance is a culture change
Why information security?

A single, comprehensive set of enterprise information security polices, standards, baselines, and procedures

- Simplifies culture change
- Simplifies compliance mandate responses by
  - Cataloging existing controls
  - Speeding gap analysis
  - Limiting expense and churn caused by new mandates

Reduces “compliance” to a single core competency: Security
Security is a business decision

- Assess the risks
- Identify the mitigation options
- Determine how much risk
  - The business is comfortable accepting
  - The business is ALLOWED to accept?
- Recognize the constraints
- Acquire and apply resources
Business decisions

The drivers for storing, processing, and transmitting cardholder data are BUSINESS drivers

The business has to ask (or be asked)

- Do legacy cardholder data business processes make sense in the post PCI world in light of
  - The expenditures we will be called upon to make?
  - The processes we will have to implement?
  - The effort we will have to exert?
  - The discipline we will have to maintain?
  - To become and remain compliant?
If the answers are “No”

The organization has to

- Reengineer Processes
  - Evaluate acceptance processes and technologies
  - Identify significant post deposit events and their timing
  - Adjust data capture, processing, storage and retrieval policies

- Reduce cardholder data storage
  - Rely on the Acquirer
  - Implement tokenization
  - Examine outsourcing options
IT and information security can THEN

- Consolidate data and systems
- Segment the network
- Implement the controls
- Close the gaps
Omni channel protection

Encrypt – Tokenize – Protect – Mask
Multiple layers of protection

- Encrypt card data as it enters the POS, payment page or mobile device
- “Token” response masks card data
- Merchant retains full brand control
- Seamless patient checkout
- Hackers are less likely to access card data
- Reduces some PCI compliance scope
- Financial reports mask card data

Merchants choose option to best fit their business model and infrastructure
## Solutions available

<table>
<thead>
<tr>
<th>Data protection</th>
<th>Fraud management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Fraud Tools</td>
</tr>
<tr>
<td>Tokenization</td>
<td>Fraud Filters</td>
</tr>
<tr>
<td>Hosted Pay Page</td>
<td>EMV terminals</td>
</tr>
<tr>
<td>Account Number Masking</td>
<td></td>
</tr>
</tbody>
</table>
EMV discussion

EMV = Europay MasterCard Visa, a set of card authentication standards

- Prevents counterfeit fraud
- Prevents skimming
- Chip instead of Mag Stripe
- Not a security solution
- Does not encrypt data
# Key takeaways

<table>
<thead>
<tr>
<th>Topic</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI</td>
<td>Basic security measures but not all that is needed</td>
</tr>
<tr>
<td>Data protection</td>
<td>Any time the card data is exposed, in transit or at rest, it is at risk</td>
</tr>
<tr>
<td></td>
<td>Layered protection is the only answer</td>
</tr>
<tr>
<td>Fraud management</td>
<td>Different from data protection</td>
</tr>
<tr>
<td></td>
<td>More risk in CNP space than card present</td>
</tr>
<tr>
<td></td>
<td>Geolocation, proxy piercing, device fingerprinting</td>
</tr>
<tr>
<td>Regulation and compliance</td>
<td>The next chapter EMV/Chip and PIN</td>
</tr>
</tbody>
</table>
Speaker contact information

Matthew Rozen
Treasury Management Strategic Solutions
O: 480-577-6509
Matthew.c.rozen@jpmorgan.com