ILLINOIS COMMUNITY COLLEGE
CFO CONFERENCE 2014

ELECTRONIC PAYMENTS, SECURITY AND PAYMENT INDUSTRY UPDATES
This presentation was prepared exclusively for the benefit and internal use of the J.P. Morgan client or potential client to whom it is directly delivered and/or addressed (including subsidiaries and affiliates, the “Company”) in order to assist the Company in evaluating, on a preliminary basis, the feasibility of a possible transaction or transactions or other business relationship 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.

To the extent that the information in this presentation is based upon any management forecasts or other information supplied to us by or on behalf of the Company, it reflects such information as well as 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. J.P. Morgan makes no representations as to the actual value which may be received in connection with a transaction nor 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 (if applicable) of the transactions contemplated hereby and all materials of any kind (including opinions or other tax analyses) that are provided to the Company 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.

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.

Chase, JPMorgan and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, “JPMC”) and if and as used herein may include as applicable employees or officers of any or all of such entities irrespective of the marketing name used. Products and services may be provided by commercial bank affiliates, securities affiliates or other JPMC affiliates or entities. In particular, securities brokerage services other than those which can be provided by commercial bank affiliates under applicable law will be provided by registered broker/dealer affiliates such as J.P. Morgan Securities LLC or J.P. Morgan Institutional Investments Inc. or by such other affiliates as may be appropriate to provide such services under applicable law. Such securities are not deposits or other obligations of any such commercial bank, are not guaranteed by any such commercial bank and are not insured by the Federal Deposit Insurance Corporation. Not all products and services are available in all geographic areas. Eligibility for particular products and services is subject to final determination by JPMC and its affiliates/subsidiaries.

This presentation does not constitute a commitment by any JPMC entity to extend or arrange credit or to provide any other services.
Objectives

After attending this session, you will better understand

- The Landscape of Electronic Payments today
- The latest technology available to help reduce fraud and PCI Scope
- Best Practices to decrease risk without compromising constituent satisfaction
### Payments Landscape

<table>
<thead>
<tr>
<th>Overview</th>
<th>Payment Points</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complex Set-up</td>
<td>Point-of-Service</td>
<td>Convenience</td>
</tr>
<tr>
<td>Multiple Merchant Codes</td>
<td>Online</td>
<td>Customer Service</td>
</tr>
<tr>
<td>Varied Equipment types</td>
<td>Mobile payments</td>
<td>Compliance</td>
</tr>
<tr>
<td>Multiple gateways</td>
<td>Third Party (Taxes)</td>
<td>Costs</td>
</tr>
<tr>
<td>Multiple partners</td>
<td>Kiosk</td>
<td></td>
</tr>
<tr>
<td>Back-Office</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Innovation
- End to End Encryption (E2EE)
- EMV – Chip card readers
- Hosted Pay Page
- Kiosks

### Cost Containment
- Look for a partner
- Get the proper pricing structure
- Keep staff productivity in mind
- Mitigate Risk/Fraud

### Continue to Learn
- Ask for Training
- Keep up on trends
- Understand your statements
- Achieve and Maintain PCI compliance
3 C’s of Card Acceptance

- **Control Your Cost**
  - Fees and Productivity

- **Make it Convenient**
  - Students, Donors and Staff

- **Achieve and Maintain Compliance**
  - Your Organization and Service Providers
- **Discount with Billback**
  A target qualification rate is established and any transaction that does not qualify at that rate is assessed a “surcharge” or “billback” fee.

- **Tiered**
  This can be 3, 6 or 9 different rates or tiers based on card type (debit credit, rewards) and how the card is accepted (swipe or keyed)

- **Interchange Pass Through or Cost Plus**
  This is a direct pass through of the cost of Interchange, plus the processor’s fee(s).
COST – Interchange Pass Through Overview

- **Over 250 categories – determined by the Card Brands, based on industry, card type and processing method**

- **Components**
  - **Interchange** - consists of a percentage and a per item fee (as applicable). These fees are based on card type and the method in which the card was accepted. (i.e. debit, credit, business, purchasing – swiped, key entered).
  - **Assessments** - a percentage of the transaction’s dollar amount passed through to the Card Brands. The current fee is 0.11% for Visa (aka Auth & Settle) and 0.13% MasterCard (aka NABU) for consumer credit and commercial transactions over $1,000, 0.11% for all debit transactions and consumer credit and commercial transactions under $1,000.
  - **Access Fee** - a per transaction fee paid to Card Brands for network access to process transactions. ($0.0195 Visa and $0.0185 MasterCard)
COST – Other considerations

As a merchant, other than pricing method these things can affect cost:

- **Volume**
- **Average Payment**
- **Merchant Category Code**
  - MCC code is based on the product and/or service you provide within your different payment channels
  
  **Possible Codes for Colleges**
  
  8398 CharitableSocialServices*
  
  8220 Colleges and Universities

  * Indicates specialty category and rates by Card Brand available

- **Account Set-up**
  - Address verification
  - Card Present vs. Card Not Present
  - Convenience Fee vs. Non-Convenience Fee
  - Level I, II or III Data
  - Surcharge Pass Through
CONVENIENCE – Payment Applications

Face to Face Payments
- Terminals, software (integrated/non-integrated) or mobile applications

Website Payments
- Hosted or managed (internally or externally)

Phone/IVR
- Internal or External service provider

Mailed/Phoned In
- Lockbox or onsite

Kiosks
- Onsite or offsite public locations
## Compliance – types of compliance

<table>
<thead>
<tr>
<th>Type of Compliance</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>
## COMPLIANCE - Threats outpacing most organizations

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

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
COMPLIANCE - What is “PCI Compliance”

- 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
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
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
COMPLIANCE – 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

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?
COMPLIANCE – Common Data Security needs and challenges

<table>
<thead>
<tr>
<th>Cost</th>
<th>Complexity</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>“I need to protect my organization from the cost of a data breach”</td>
<td>“I need to reduce PCI compliance scope and complexity.”</td>
<td>“I have to provide a seamless student experience.”</td>
</tr>
<tr>
<td>- Cost to maintain PCI compliance</td>
<td>- Merchants don’t want to be in the security business</td>
<td>- Disjointed patient experience</td>
</tr>
<tr>
<td>- Payment brand fines</td>
<td>- Maintaining compliance is complicated and cumbersome</td>
<td>- Security fears</td>
</tr>
<tr>
<td>- Investigation and legal fees</td>
<td>- Heavy impacts on IT departments</td>
<td>- Shopping cart abandonment</td>
</tr>
<tr>
<td>- Customer churn</td>
<td></td>
<td>- Brand confusion</td>
</tr>
<tr>
<td>- Lost employee productivity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## COMPLIANCE – How the challenge is met

<table>
<thead>
<tr>
<th>Value</th>
<th>Simplicity</th>
<th>Empowerment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remove data from payment network</strong></td>
<td><strong>Reduce PCI scope and complexity</strong></td>
<td><strong>Positive patient experience</strong></td>
</tr>
</tbody>
</table>
| ■ Removing payment data from your network may  
  ■ Reduce risk of exposure  
  ■ Prevent loss of student confidence  
  ■ Minimize scope and cost of PCI compliance  
  ■ Reduce the likelihood of fines | ■ When payment data never has to enter the network  
  ■ Scope is reduced  
  ■ Complexity is reduced  
  ■ Less time needed to manage compliance  
  ■ IT burden is minimized | ■ Seamless checkout  
  ■ Full branding control  
  ■ Reduces patient security concerns  
  ■ Minimizes shopping cart abandonment |

Note: Merchants will still have to meet some PCI requirements
<table>
<thead>
<tr>
<th>Retail</th>
<th>Ecommerce</th>
<th>Mobile</th>
</tr>
</thead>
</table>
COMPLIANCE AND CONVENIENCE – Multiple protection layers

- Encrypt card data as it enters the POS, payment page or mobile device
- “Token” response masks card data
- Merchant retains full brand control
- Seamless 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
**COMPLIANCE AND CONVENIENCE – Available solutions**

<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 = 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
COMPLIANCE AND CONVENIENCE – Available Solutions E2EE and HPP

End to End Encryption

E2EE is the encryption of card data at the point of entry until it reaches the processor’s secure systems where it’s decrypted. It gives card acceptors security for card holder data taken via card swipe/key-entry at the point of purchase (both online and retail settings). E2EE has been available for a few years but was only utilized by online acceptors but with slow adoption. This has now moved into the card present environment and is leaping forward.

The benefit: Advantages relate to reducing or meeting PCI Compliance Standards.

Hosted Pay Page

HPP is a secure payment portal embedded into a webpage. Instead of being hosted and information collected on the clients webpage, the payer is directed to the secure web site of the service provider where the transaction data is tokenized. It still looks and feels like the merchant’s site to give the payer a feeling of security.

The benefit: Advantages relate to reducing scope or meeting PCI compliance standards.
**Surcharging participation**

Effective January 27, 2013 merchant may pass through a surcharge at the point of sale – card present or not-present environment

- You must check to see if your state allows it (10 do not)
- Consumer or Commercial Credit cards ONLY
- Either brand-level surcharging or product-level surcharging
- You may not charge more than YOUR cost of acceptance (capped at 4%)  
- Level playing field requirements
- Disclosure of surcharging has to be displayed
- Must provide acquirer and payment brands notice at least thirty days prior to surcharging

**The benefit:** Reduced cost of acceptance

**Consider:** Affect on those you serve.

**Note:** Technology has to catch up, other states are joining in to prohibit it
Surcharging participation

- What’s the difference between a convenience fee and a surcharge?
  - A Convenience Fee is a fee for the convenience of paying for goods/services in a payment method that is outside the normal payment channel of the card acceptor.
  - Surcharging is the passing through the cost of accepting a credit or commercial card for payment at any point of sale.
### Key Take-a-ways

<table>
<thead>
<tr>
<th>Category</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>
PCI Resources

Websites
- [http://www.chasepaymentech.com/datasecurity](http://www.chasepaymentech.com/datasecurity)
- [http://www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)
- [http://www.trustwave.com](http://www.trustwave.com)
- [https://sdp.mastercardintl.com](https://sdp.mastercardintl.com)

PABP
- Payment Applications Site
- Payment Application Best Practices document
- Validated Payment Applications list
Questions?

Jeanie Griffin, Director Government, Non-Profit and Healthcare
Chase Paymentech
Office: 630.554.2984
Jeanie.Giffin@chasepaymentech.com