Best Practices in Accepting Payment Card Payments

Sean Christy – Partner, Bryan Cave
Tim Carlton – Associate, Bryan Cave

PRO BONO PARTNERSHIP/ATLANTA

BRYAN CAVE

Mission of Pro Bono Partnership of Atlanta:

To maximize the impact of pro bono engagement by connecting a network of attorneys with nonprofits in need of free business legal services.

PRO BONO PARTNERSHIP/ATLANTA

BRYAN CAVE

Pro Bono Partnership of Atlanta Eligibility & Other Information

- In order to be a client of Pro Bono Partnership of Atlanta, an organization must:
  - ✓ Be a 501(c)(3) nonprofit.
  - ✓ Be located in or serve the greater Atlanta area.
  - ✓ Serve low-income or disadvantaged individuals.
  - ✓ Be unable to afford legal services.
- *Visit us on the web at* www.pbpatl.org
- We host free monthly webinars on legal topics for nonprofits
  - ✓ To view upcoming webinars or workshops, visit the Workshops Page on our website
  - ✓ Join our mailing list by emailing rla@pbpatl.org

Legal Information:

✓ This webinar presents general guidelines for Georgia nonprofit organizations and should not be construed as legal advice. Always consult an attorney to address your particular situation.

Agenda

- Payment card background and terminology
- Risks and liabilities associated with acceptance of payment card (credit, debit and pre-paid card) payments
- Compliance requirements applicable to payment card payments (focus on PCI)
- Difference between acceptance of payments directly versus through a third party processor
- Ways in which a non-profit may limit its exposure

Payment Card Background and Terminology

PRO BONO PARTNERSHIP/ATLANTA

BRYAN CAVE

Players in the Payment Ecosystem

Acquiring Bank – The financial institution that does business with the merchant and enables the merchant to accept credit cards.

Cardholder – The person to whom a payment card is issued.

Issuing Bank – The financial institution that issues a payment card to the cardholder.

Merchant – A retailer or any other person or entity that accepts credit cards or debit cards pursuant to a Merchant Agreement.

Payment Facilitator – An entity that provides payment services to a Merchant on behalf of an Acquiring Bank (e.g., payment processors like First Data, Bank of America Merchant Services, or Square).

Payment Network – The electronic payment system providing authorization services and clearing and settlement services (e.g., Visa).

Point of Sale (POS) – The device placed at the Merchant's location designed to authorize and record each sale.

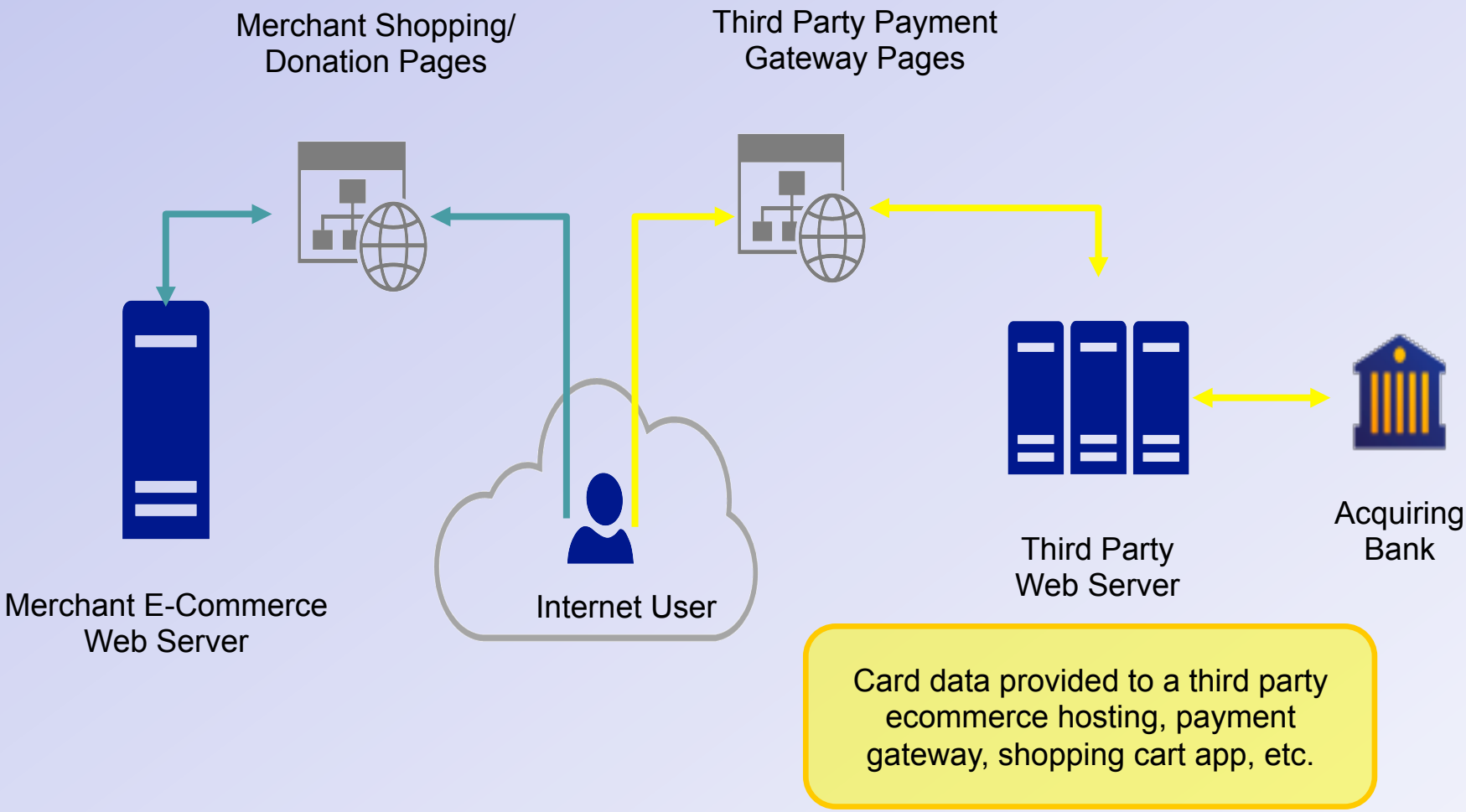
Point-of-Sale

1. The Cardholder data is entered into the Merchant's POS
2. The card data is sent to the Acquiring Bank
3. The Acquirer sends the card data to the Payment Network
4. The data is forwarded to the Issuing Bank, who verifies the card is legitimate and the account has appropriate credit.

5. If so, the Issuing Bank generates authorization number and routes this number back to the Payment Network. With this authorization, the Issuing Bank is agreeing to fund the purchase on the Cardholder's behalf.
6. The Payment Network forwards the authorization code back to the Acquiring Bank
7. The Acquiring Bank sends the authorization code back to the Merchant
8. The Merchant concludes the sale with the Cardholder

Note: In some circumstances, a Payment Facilitator may transmit the data between the Merchant and Acquiring Bank in Steps 2 and 7.

E-Commerce with Third Party Processor



Card data provided to a third party ecommerce hosting, payment gateway, shopping cart app, etc.

Risks and Liabilities Associated with Acceptance of Payment Card Payments

Fraud Liability

- Fraud liability - Card fraud losses may be borne by Merchants, Cardholders, or the Issuing Banks depending on how the fraud occurred
- Chargebacks
  - Cardholder files dispute for fraud
  - Issuing Bank makes investigation
  - Issuing Bank enters process with Merchant to decide who is responsible
  - If Issuing Bank determines Merchant cannot prove transaction was legitimate, Issuing Bank takes entire value of transaction plus a chargeback fee.
  - Card Not Present (CNP) transactions have much higher chargeback rates than Card Present (CP) transactions
  - But CP chargeback rates may increase due to EMV Chips

PRO BONO PARTNERSHIP/ATLANTA

BRYAN CAVE

EMV Chip

PRO BONO PARTNERSHIP/ATLANTA

BRYAN CAVE

Why Does EMV Matter?

- Liability for fraudulent transactions has changed
- On October 1, 2015, Payment Cards shifted their liability framework

Card Used	Terminal Available	Party Liable for Counterfeit Fraud
Mag stripe only	Mag stripe only	Issuer
Mag stripe only	EMV Chip	Issuer
EMV Chip	**Mag stripe only**	**Merchant**
EMV Chip	EMV Chip	Issuer

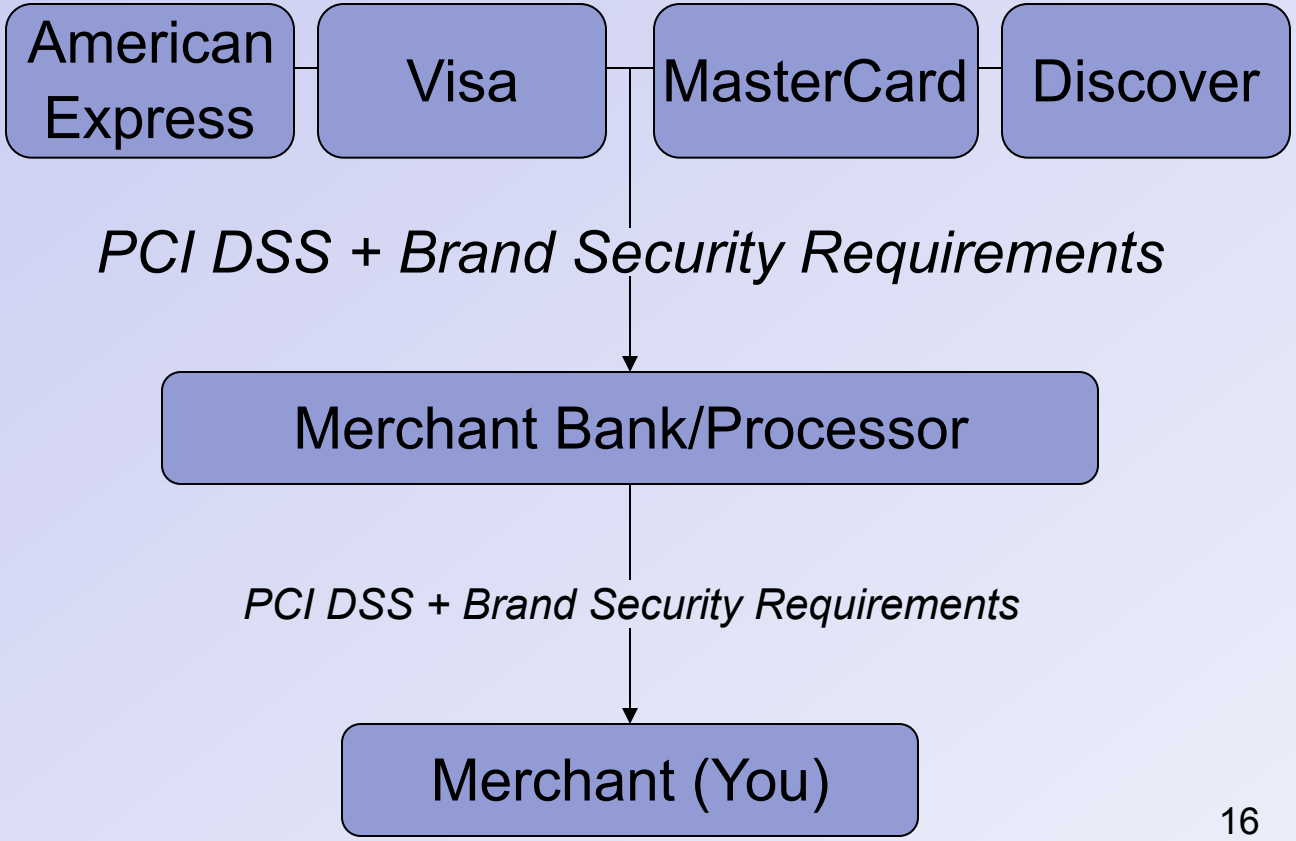
- The party with the least secure technology is liable for counterfeit fraud

Data Loss Liability

- $221 total average cost per record lost (most recent Ponemon Institute Survey)
  - ✓ $23 in detection and escalation costs
  - ✓ $19 in notification costs
  - ✓ $54 in defense and response costs
  - ✓ $125 in opportunity costs

Compliance Requirements Applicable to Payment Card Payments

The PCI DSS


American Express
Visa
MasterCard
Discover
PCI DSS + Brand Security Requirements
Merchant Bank/Processor
PCI DSS + Brand Security Requirements
Merchant (You)

PRO BONO PARTNERSHIP/ATLANTA

BRYAN CAVE

The PCI DSS

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Brand/Network Security Requirements

- Reflected in your Merchant Bank/Processor contract either directly or by reference to the applicable brand security standards and includes:
  - ✓ Compliance validation requirements and deadlines
    - Dictated by merchant classification
    - Self-Assessment Questionnaire (SAQ) and Network Scans almost always required if payments processed directly
  - ✓ Security incident response requirements
  - ✓ Fines and penalties for breaches and data loss

SAQs and Network Scans

- Self-Assessment Questionnaires (SAQ)
  - ✓ Essentially a self-reporting of compliance with the PCI DSS
  - ✓ Third party payment processors and service providers also provide assistance and input
- Network Scans
  - ✓ Must be performed by an approved scanning vendor (listed on PCI website)
  - ✓ Test your network, or that of your third party processor for security vulnerabilities that would violate the PCI DSS

Certain Key Requirements

- Storage of payment card data electronically should be avoided if possible
- If the primary account number is stored, it should be obfuscated
- Certain payment card data should never be stored
- If you contract with a third party to store payment card data, process transactions or operate and/or support your payment processing systems, you must contractually obligate the third party to comply with the PCI DSS and validate compliance

Direct Payment Acceptance versus Third Party Processors and Limiting Your Liability

Pros and Cons

Direct Payment

Pros

+ More information and systems control

Cons

- PCI DSS compliance requirements apply to your entity directly (security not likely a core competency)
- More PCI validation requirements apply to your entity
- Your entity carries higher risk of data loss and data breach

Indirect Payment

Pros

+ Many PCI compliance requirements shifted to third party processor (security a core competency)
+ PCI validation requirements minimized
+ Third party processor carries predominant risk of data loss and data breach

Cons

- Usually carries higher per transaction fee
- Branding / convenience factor for donor

Limiting Your Liability

- Regardless of how you accept payment card payments, develop, update and monitor compliance with a data security policy that incorporates the PCI DSS as they apply to your entity
- Do not store payment card data electronically if it can be avoided
- Never store sensitive authorization data
- Limit access to payment card data (electronic or paper) on a need-to-know basis and properly secure any stored data
- Secure your payment card systems

Limiting Your Liability (cont.)

- Regularly validate, and report as required, your compliance with applicable PCI requirements
- Use a fully outsourced payment card processor solution if possible to limit your exposure to payment card data and compliance risk
- Use lower risk terminal solutions to limit exposure for in-person transactions
- Engage counsel immediately if you or your provider suffers a data loss

PRO BONO PARTNERSHIP/ATLANTA

BRYAN CAVE

For More Information:

If you would like more information about the services of Pro Bono Partnership of Atlanta, contact us at:

www.pbpatl.org

info@pbpatl.org

404-407-5088