Before You Swipe: Best Practices in Accepting Credit, Debit and Pre-Paid Card Payments

Sean Christy, Sutherland
Robyn Miller, Pro Bono Partnership of Atlanta

March 22, 2012

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 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 organization.
  - ✓ 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*
- Host free monthly webinars on legal topics for nonprofits
  - ✓ To view upcoming webinars or workshops, visit the Workshops Page on our website

Agenda

- 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
- Charitable solicitation issues in accepting online donations

Risks and Liabilities Associated with Acceptance of Payment Card Payments

Payment Card Risks and Liabilities

- Primary risk is loss or theft of payment card data
  - ✓ Cardholder Data
    - Primary account number
    - Cardholder Name
    - Service Code
    - Expiration Date
  - ✓ Authentication Data
    - Magnetic stripe data
    - CAV2/CVC2/CVV2/CID (i.e., the 3-digit number in the signature block of Visa, MasterCard and Discover cards or the 4-digit number on the front of American Express cards)
    - PIN / PIN block

Payment Card Risks and Liabilities (cont.)

- Liability stems from:
  - ✓ Federal statutes and regulations
  - ✓ State statutes and regulations (e.g., notice laws)
  - ✓ PCI standards and payment card contracts
- Liability includes:
  - ✓ Fines and penalties
  - ✓ Cost of payment card reissuance
  - ✓ Legal costs and associated settlements and judgments
  - ✓ Lost opportunity

PRO BONO PARTNERSHIP/ATLANTA

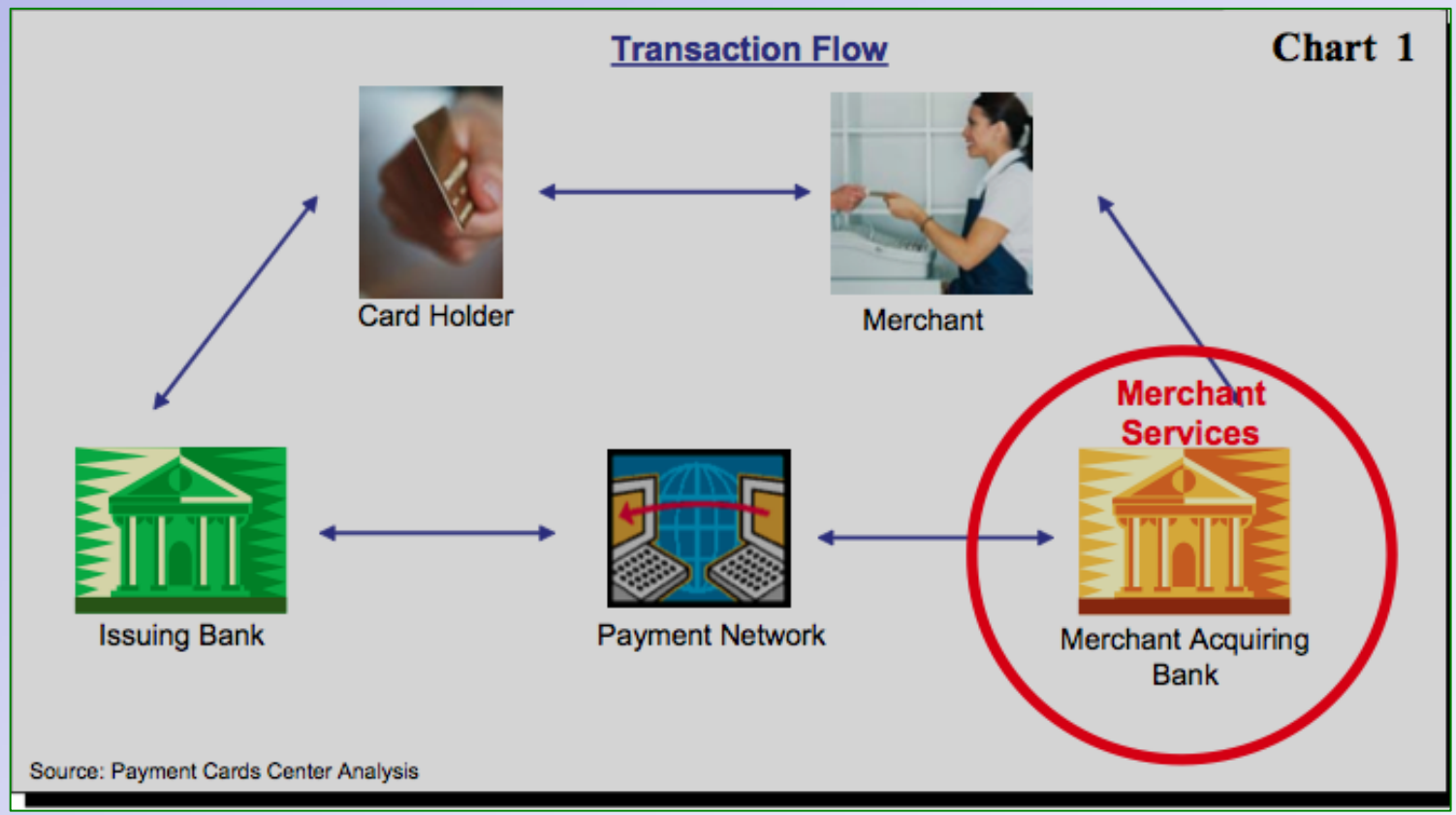
SUTHERLAND

Data Breach Cost Exposure

- $204 total average cost per record lost (most recent Ponemon Institute Survey)
  - ✓ $8 in detection and escalation costs
  - ✓ $15 in notification costs
  - ✓ $46 in defense and response costs
  - ✓ $135 in opportunity costs

Compliance Requirements Applicable to Payment Card Payments

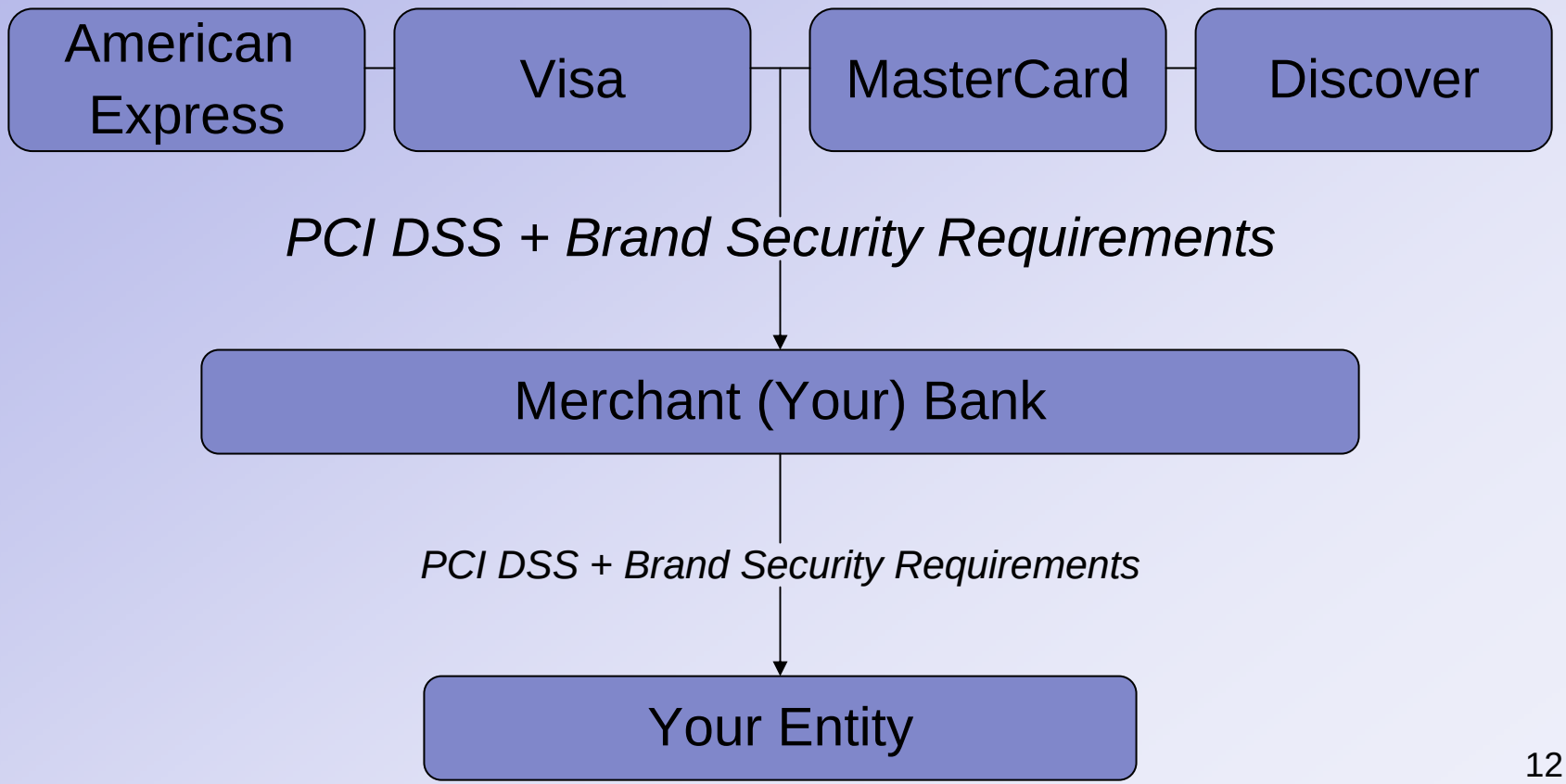
Payment Card Participants



Payment Card Regulators

- Self-regulating council comprised of the major payment card “brands” or “networks”:
  - ✓ American Express
  - ✓ Discover
  - ✓ Visa
  - ✓ MasterCard
  - ✓ JCB
- The council promulgates data security standards (the PCI DSS) for the protection of credit card data
- www.pcisecuritystandards.org

How the PCI DSS Apply to You



PRO BONO PARTNERSHIP/ATLANTA

SUTHERLAND

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 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

PRO BONO PARTNERSHIP/ATLANTA

SUTHERLAND

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 www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php)
  - ✓ 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

Online Direct Payment

Pros

+ Enables direct receipt of payment from donor constituents

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

Online 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

PRO BONO™ PARTNERSHIP/ATLANTA

SUTHERLAND

Some Payment Processing Scenarios

Fully Outsourced Processing (Indirect)

- No payments accepted by your entity
- All payments transacted with third party processor online
- No electronic records of cardholder or sensitive data retained by your entity
- SAQ A required of your entity

Imprint or Standalone Terminal (Direct)

- Cardholder data taken via imprint or POS terminal connected via dial-up (not to the Internet or other systems)
- No electronic records of cardholder or sensitive data retained by your entity
- SAQ B required of your entity

Virtual Terminal (Direct)

- Cardholder data received via mail, telephone or in person
- Cardholder data entered into third party's system via your entity's PC through a secure web interface
- No electronic records of cardholder or sensitive data retained by your entity
- SAQ C-VT required of your entity

Hybrid Model (Direct)

- Cardholder data entered into your entity's payment application that is connected to the Internet and/or
- Cardholder data transmitted to third party payment processor over Internet for back-end processing
- No electronic records of cardholder or sensitive data retained by your entity
- SAQ C and network scans required of your entity

PRO BONO PARTNERSHIP/ATLANTA

SUTHERLAND

Some Third Party Processor Scenarios

Fully Outsourced Processing (Indirect)

Data Exposure	Your Compliance Obligations	Online Payments Possible	Direct Payments Possible
Low	Low	Yes	Only through PC with access to third party

Imprint or Standalone Terminal (Direct but not Online)

Data Exposure	Your Compliance Obligations	Online Payments Possible	Direct Payments Possible
Low	Low	No	Yes

Virtual Terminal (Direct)

Data Exposure	Your Compliance Obligations	Online Payments Possible	Direct Payments Possible
Moderate	Moderate	No	Yes

Hybrid Model (Direct)

Data Exposure	Your Compliance Obligations	Online Payments Possible	Direct Payments Possible
High	High	Yes	Yes

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 for online payments 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

Charitable Solicitation Issues in Accepting Online Donations

Charitable Solicitation

- Regulated by each state individually
  - ✓ Overseen by Attorney General & Charity Officials
- Laws protecting the general public from fraud
- Often state laws contain specific acts that are prohibited & have penalties for violations
- Example: Georgia (O.C.G.A. § 43-17-12)
  - ✓ No untrue, false or misleading statements to Sec. of State
  - ✓ No using name, symbol of similar charity to confuse, mislead to acquire donations
  - ✓ No identification of sponsors who are not in fact sponsors of the organization
  - ✓ No statement of a false percentage of gross revenues going to the charity
  - ✓ Not providing proper information to a potential donor
  - ✓ Not having written agreement with charity that soliciting on its behalf
  - ✓ No device or schemes to defraud

Charitable Solicitation Registration

- Nonprofit organizations are often required to register to solicit for charitable contributions from the general public
- Varies state by state
  - ✓ Registration generally requires providing identifying information about the nonprofit and its operations
    - Information about executives, officers, directors of the nonprofit
    - Paid solicitors, Professional fundraisers
    - Financial information
  - ✓ Fee (average range from $0 to $200)
  - ✓ Registration required prior to conducting solicitation activities

Who Must Register?

- Who:
  - ✓ Varies state by state
  - ✓ Usually any nonprofit organization that solicits in the state for contributions*
  - ✓ Exceptions/Exclusions
    - Religious Organizations
    - In some states
      - Income thresholds
      - Certain types of organizations

*May also include paid solicitors, professional fundraisers and others.

Where Must a Nonprofit Register?

General Question to Ask

"Has my organization purposefully directed a charitable solicitation to a resident of State X?"

If yes, then usually the organization must register in State X.

Where is Registration Necessary?

- Where:
  - ✓ Requirements vary state by state
  - ✓ States in which organizations conduct charitable solicitation:
    - Nonprofit is physically “present” in the state (e.g., has an office, owns real estate, conducts program activities, fundraising events, door-to-door requests);
    - Nonprofit raises funds in the state (e.g., letters, phone calls, or advertising requesting support)
    - Online activities…..
      - Many state statutes don’t specifically address these activities

Internet or Online Solicitation

- Key Question:
  - ✓ How do state courts obtain jurisdiction over nonprofits participating in online solicitation activities?
    - How much contact must the organization have with the state and its citizens?
    - Each state establishes its own thresholds
- Common online activities:
  - ✓ Website
  - ✓ Email - Specific solicitation or donate now button at bottom of emails
  - ✓ Advertising online
  - ✓ Social Media

Charleston Principles - Internet Solicitation

- NASCO Board – Advisory Guidelines
- General Principles - Sufficient Contacts in state – must register
- Website - Charitable Solicitation Registration
  - ✓ Interactive website & either
    - Specifically target persons physically located in state (knew or reasonably should have known person a resident of the state) or
    - Receives contributions from state on a repeated & ongoing basis or substantial basis through its website
  - ✓ Definition of interactive website
    - Make contribution or purchase a product or service in connection with charitable solicitation by electronically completing the transaction
    - Use of linked or redirected sites to process transaction

Charleston Principles - Internet Solicitation (cont.)

- Website - Charitable Solicitation Registration (cont.)
  - ✓ Non-interactive website
    - That either invites further offline activity to complete donation or establishes other contacts with state (e.g. emails promoting website) and
    - Receives contributions from state on a repeated & ongoing basis or substantial basis

Charleston Principles - Internet Solicitation (cont.)

- Internet Solicitation by Others – Website & Advertising
  - ✓ Commercial co-venturers ("cause marketing") and professional fundraisers'websites must follow same principles
    - Charities benefitting from such interactive websites may need to register as though the site was its own interactive website
    - Commercial co-venturers and professional fundraisers must register as required by state laws
    - Examples:
      - Solicitation of donations for Charity A by another entity on its website
      - Sale of product for which 10% of proceeds goes to Charity A
  - ✓ Exceptions:
    - ISP that merely processes process online transactions
    - Admin., supportive, and technical service providers who do not solicit
    - Similar companies that do NOT receive compensation based on amount of funds raised

Charleston Principles - Internet Solicitation (cont.)

- Email Solicitation
  - ✓ Soliciting via email = soliciting via telephone or direct mail IF
  - ✓ Knew or reasonably should have known person a resident of the state
- Not Addressed in the Charleston Principles: Social Media
  - ✓ Facebook – an interactive webpage
  - ✓ Twitter?
- Still murky waters as each state still does its own thing – so check http://www.multistatefiling.org

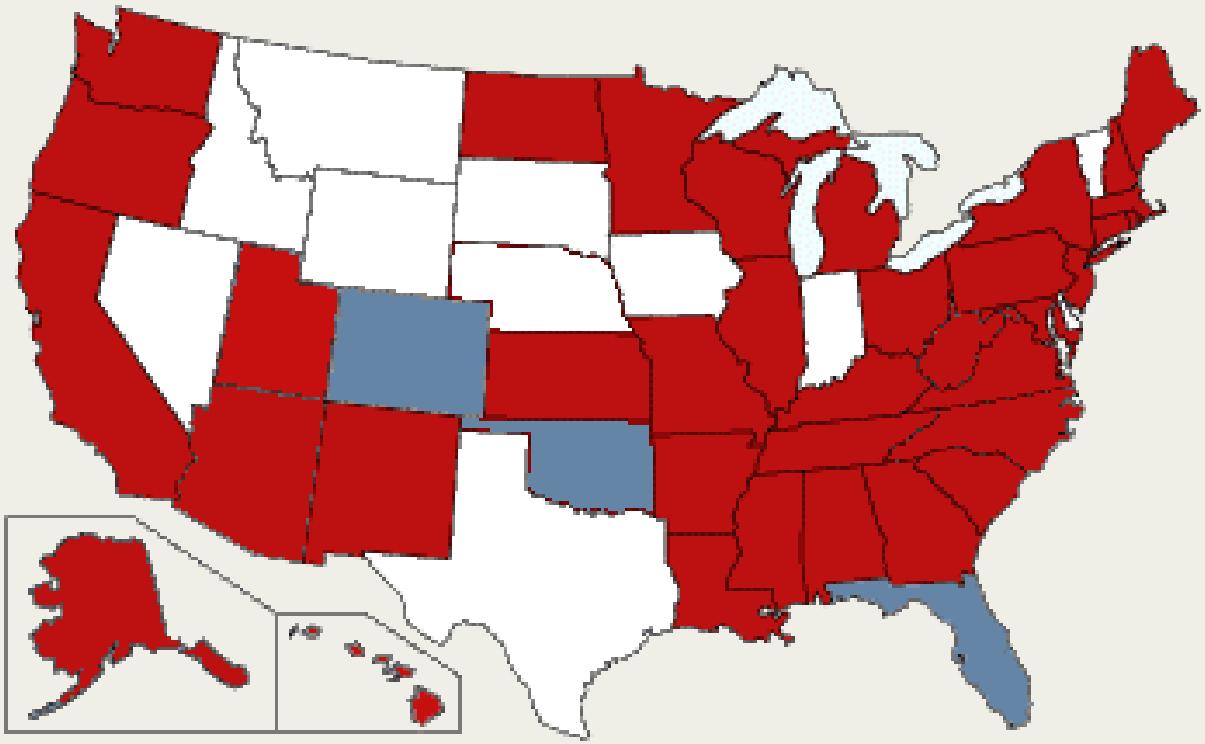
Registering in Multiple States: Unified Registration Statement

- Unified Registration Statement
  - ✓ Multistate filing form
    - http://www.multistatefiling.org
  - ✓ Alternative to filing each individual form
  - ✓ Some states require additional information –
    - – Included in multistate filing information

PRO BONO PARTNERSHIP/ATLANTA

SUTHERLAND

Charity Registration in the States



States that accept the common form
States that require charities to register but don't accept the common form
States that do not require registration

Source: Multi-State Filer Program

Map by Jasmine Stewart, Courtesy of the Chronicle of Philanthropy

For More Information:

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

Phone: 404-407-5088

Fax: 404-853-8806

Info@pbpatl.org

www.pbpatl.org

Appendix

PRO BONO PARTNERSHIP/ATLANTA

SUTHERLAND

Visa Compliance Validation Requirements

Level / Tier [1]	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region [2]	• Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") or internal auditor if signed by officer of the company • Quarterly network scan by Approved Scan Vendor ("ASV") • Attestation of Compliance Form
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	• Annual Self-Assessment Questionnaire ("SAQ") • Quarterly network scan by ASV • Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	• Annual SAQ • Quarterly network scan by ASV • Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	• Annual SAQ recommended • Quarterly network scan by ASV if applicable • Compliance validation requirements set by acquirer

PRO BONO PARTNERSHIP/ATLANTA

SUTHERLAND

Data Storage Limitations

	Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication Data [1]	Full Magnetic Stripe Data [2]	No	Cannot store per Requirement 3.2
	CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
	PIN/PIN Block	No	Cannot store per Requirement 3.2