Client Data Security Report

Helen Resalvo
Global Payment System Risk

Disclaimer

Forward-Looking Statements

The materials, presentations and discussions during this meeting contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms "will," new," "continue," "could," "accelerate," and other similar references to the future. Examples of such forward-looking statements may include, but are not limited to, statements we make about our plans and goals regarding authentication, risk and fraud, the effect of developments in regulatory environment, and other developments in electronic payments.

By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance and (iii) are subject to risks, uncertainties, assumptions and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors, including the following:

- the impact of regulation, including its effect on issuer and retailer practices and product categories, and the adoption of similar and related laws and regulations elsewhere;
- developments in current or future disputes
- macroeconomic and industry factors such as: global economic, political, health and other conditions; competitive pressure on customer pricing and in the payments industry generally; material changes in our customers' performance compared to our estimates; and disintermediation from the payments value stream through government actions or bilateral agreements;
- systemic developments, such as: disruption of our transaction processing systems or the inability to process transactions efficiently; account data breaches involving card data stored by us or third parties; increased fraudulent and other illegal activity involving our cards; failure to maintain interoperability between our and Visa Europe's authorization and clearing and settlement systems; loss of organizational effectiveness or key employees; and
- the other factors discussed under the heading "Risk Factors" herein and in our most recent Annual Report on Form 10-K and our most recent Quarterly Reports on Form 10-Q.

You should not place undue reliance on such statements. Unless required to do so by law, we do not intend to update or revise any forward-looking statement, because of new information or future developments or otherwise.

Disclaimer

Notice

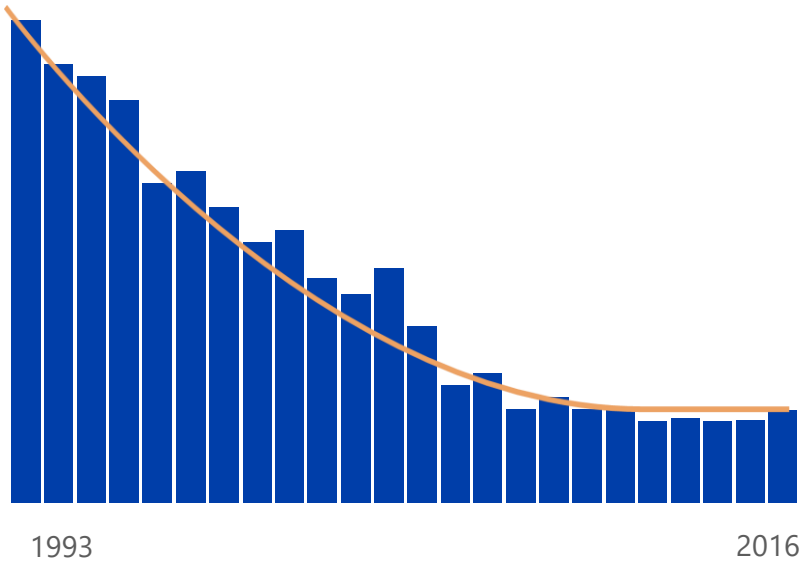
The information, recommendations or "best practices" contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or "best practices" may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance.

Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

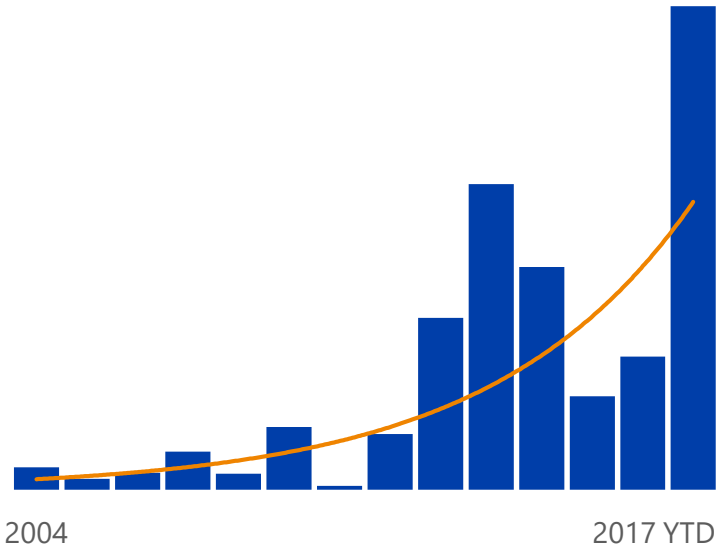
Payment Security: Where are we now?

Fraud remains near historic lows, but data losses continue to accelerate

Gross Fraud Rate



Personal Data Exposed



Improving Security

Focus on improving ecosystem security and ensuring consistent global program adoption and enforcement

- Fair, consistent enforcement across regions and programs

- Clear, consistent communication with clients

- Enforcement actions to be proportionate to risks
- Extensions and waivers considered in fair and consistent manner

- Enhanced value-add security communications and resources

Visa Account Information Security Program

Visa's Data Security Programs

▸ Merchant Risk Program	Defines data security compliance, validation and reporting requirements for merchants and acquirers
▸ Third Party Agent Program	Defines data security compliance, validation and registration requirements for third party agents handling data on behalf of Visa clients or merchants
▸ VisaNet Processor Risk Program	Defines data security compliance, validation and registration requirements for VisaNet processors (processors connected directly to Visa)
▸ PIN Security Program	Focuses on ensuring compliance of entities that process PIN data or perform key management activities on behalf of Visa clients
▸ Card Vendor Security Program	Defines data security compliance and validation requirements for vendors that provide payment card manufacturing or personalization services
▸ Access Control Server (ACS) Security Program	Defines data security and financial requirements for vendors supporting Verified by Visa/3D Secure services for Visa issuers

Data Security Reports

1 - Aging Report

What is it?	Who will receive it?	Frequency	Client Obligations
Report(s) listing all: • Third party agents (i.e., third party agents, VisaNet processors, and PIN agents) that are within 30-days of their revalidation date or overdue to revalidate against PCI DSS and/or PCI PIN. • NA & LAC Merchants that are 6 months from eligibility for non-compliance assessment.	The report will be sent via email to the Visa client contact who manages merchant compliance and agent registration contact in VOL (i.e., function #180 contact).	First week of every month	Provide the required documentation to demonstrate compliance for the entity, or a remediation plan by the Action Required Deadline.

Aging Report - Sample

Client Name
Client BID

Dear Visa Member:

The Visa Rules require Merchants and Agents handling cardholder data for your organization to comply with the Payment Card Industry Data Security Standard (PCI DSS) and to demonstrate PCI DSS compliance to Visa every 12 months (ID: 0008031 and 0002228). Agents are entities that act as a VisaNet Processor, a Third Party Agent, or both (ID: 0025920).

Merchants and Agents with Upcoming and Overdue PCI DSS Compliance Validation

Your organization is responsible for ensuring that the Merchants and Agents in the attached report submit their PCI DSS compliance validation to Visa on or before the stated deadline. Our records indicate that the following Merchants and Agents are not current with Visa's PCI DSS validation requirements.

Your organization may be liable for the following non-compliance assessments if the Merchant(s) or Agent(s) fail to address their non-compliance by the deadlines indicated (Action Required or Remediation Deadline).

Please refer to attached document for more information on the action required and consequences of non-compliance.

Please feel free to email to the addresses provided below if you have any questions or if you would like to discuss further.

Region(s)	Merchant Compliance	Agent Compliance
AP, CEMEA	vpssais@visa.com	pciagents@visa.com
Canada, US, LAC	cisp@visa.com	pcirocs@visa.com

Thank you for ensuring that your merchants and agents are taking the necessary steps to protect cardholder data.

Aging Report - Attachment

- One .csv attachment per program
- Each report will contain: the entity name, operating country, entity type, Business ID, compliance status, validation due date, remediation due date (if applicable), non-compliance assessment (NCA) amount, accumulated non-compliance assessment amount, and action required deadline.
  - The "non-compliance assessment amount" is the amount that will be assessed against the client if the action required deadline is missed.
  - The "accumulated non-compliance assessment amount" represents any NCA that has been suspended during the validation cycle of the merchant or third party agent.

	A	B	C	D	E	F	G	H	I	J
1	Name	Operating Country(s)	Entity Type(s)	BID	Compliance Status	Next Review Date	Remediation Due Date	Non-Compliance Assessment Amount	Accumulated NCA	Action Required Deadline
2	SAMPLE AGENT	UNITED STATES OF AMERICA	Third Party Agent	12345678	Not Compliant	6/30/2017	n/a	n/a	0	9/30/2017
3										

Data Security Reports

2 – Warning Notification

What is it?	Who will receive it?	Frequency	Client Obligations
In the event NCAs are applicable, Visa will provide a warning notification detailing all entities that are subject to NCA, the potential NCA amount, the action that must be taken to suspend or waive the NCA, and action required deadline.	The report will be sent via email to the Visa client contact who manages merchant compliance and agent registration contact in VOL (i.e., function #180 contact).	First week of every month	Provide the required documentation to demonstrate compliance for the entity, or a remediation plan by the action required deadline.

Warning Notification - Sample

Client Name
Client BID

Re: Account Information Security Program Non-Compliance Assessments

Dear Visa Client,

Account information security is essential to ensuring sustainable growth of the Visa payment network. According to the Visa Rule 'Account and Transaction Information Security Requirements' (ID: 0002228) (the 'Visa PCI DSS Rule'), Agents and Merchants, as defined in ID: 0025920 and 0024828, handling Visa cardholder data for your organization must comply with the Payment Card Industry Data Security Standard (PCI DSS).

Non-Compliance Assessment

Based on our records, the following entities are non-compliant with the Visa PCI DSS Rule and may result in your organization being liable for the following non-compliance assessments (ID: 0008193):

Business Name	Program	BID	Assessment Amount	Non Compliance Assessment Month
Sample Agent	Third Party Agent	12345678	$10,000.00	Sep 2017
Sample Merchant	Merchant Level 1	N/A	$5,000.00	Sep 2017

The non-compliance assessments totaling US$15,000.00 for September 2017 may appear in your monthly integrated billing statement. Please be reminded that non-compliance assessments may continue to be imposed until the entities either comply with the Visa PCI DSS Rule or have submitted to Visa a remediation plan that has been deemed acceptable by Visa.

In order to suspend or waive the non-compliance assessments, please provide the necessary remediation plans (e.g. Prioritized Approach) or validation documents (i.e. signed Attestation of Compliance, Report on Compliance) by 09/20/2017.

Please feel free to email to the addresses provided below if you have any questions or if you would like to discuss further.

Region(s)	Merchant Compliance	Agent Compliance
AP, CEMEA	vpssais@visa.com	pciagents@visa.com
US, Canada, LAC	cisp@visa.com	pcirocs@visa.com

Thank you for ensuring that your merchants and agents are taking the necessary steps to protect cardholder data.

Data Security Reports

3 – Final Notification

What is it?	Who will receive it?	Frequency	Client Obligations
A final notification will be sent after the deadline in the warning notification has passed. The final notification will provide the total amount for any NCAs that were assessed through the Global Member Billing Solution for the month. In addition, the final notification will include any decisions to waive or suspend NCAs for entities that were included in the warning notification in the prior month.	The report will be sent via email to the Visa client contact who manages merchant compliance and agent registration contact in VOL (i.e., function #180 contact).	Last week of every month	Provide the required documentation to demonstrate compliance for the entity, or a remediation plan in order to suspend or waive ongoing NCA.

Final Notification - Sample

Client Name
Client BID

Re: Account Information Security Program Non-Compliance Assessments

Dear Visa Client,

Account information security is essential to ensuring sustainable growth of the Visa payment network. According to the Visa Rule 'Account and Transaction Information Security Requirements' (ID: 0002228) (the 'Visa PCI DSS Rule'), Agents and Merchants, as defined in ID: 0025920 and 0024828, handling Visa cardholder data for your organization must comply with the Payment Card Industry Data Security Standard (PCI DSS).

Non-Compliance Assessment

Based on the September non-compliance notification previously sent, below is/are the final decisions:

Business Name	Program	BID	Assessment Amount	Non Compliance Assessment Month	Decision
Sample Agent	Third Party Agent	12345678	$10,000.00	Sep 2017	Suspend
Sample Merchant	Merchant Level 1	N/A	$5,000.00	Sep 2017	Assess

The non-compliance assessment totaling US$5,000.00 for September 2017 will appear in your monthly integrated billing statement. Please be reminded that non-compliance assessments will continue to be imposed until the non-compliance entities either comply with the Visa PCI DSS Rule or have submitted to Visa a remediation plan that has been deemed acceptable by Visa.

Please feel free to email to the addresses provided below if you have any questions or if you would like to discuss further.

Region(s)	Merchant Compliance	Agent Compliance
AP, CEMEA	vpssais@visa.com	pciagents@visa.com
Canada, US	cisp@visa.com	pcirocs@visa.com
LAC	cisp@visa.com	pcirocs@visa.com

Thank you for ensuring that your merchants and agents are taking the necessary steps to protect cardholder data.

Data Security Resources

Visa Data Security Websites
North America and LAC: www.visa.com/cisp
AP and CEMEA: www.visa.com/staysecureAPCEMEA

Data Security Questions
Merchant, North America and LAC @ cisp@visa.com
Merchant, AP and CEMEA @ vpssais@visa.com
TPA/VNP/PIN, North America and LAC @ pcirocs@visa.com
TPA/VNP/PIN, AP and CEMEA @ pciagents@visa.com

Visa Global Registry of Service Providers – www.visa.com/onthelist

Visa Business School – www.visabusinessschool.com

PCI Security Standards Council Website – www.pcissc.org

Q&A