Card Compromise Assistance Plan

This Card Compromise Assistance Plan ("CCAP") Agreement (the "**Agreement**") sets forth the terms and conditions by which **Global Payments** will assist **Merchant** for certain losses related to a data security **incident. Global Payments'** obligations to **Merchant** under this **Agreement** do not constitute the issuance of a policy, certificate, or contract of insurance between **Global Payments** and **Merchant**. **Global Payments** has chosen to obtain insurance, from a licensed insurance broker, to support **Global Payments'** contractual obligations to **Merchant** under this **Agreement**. Words and phrases that appear in boldface are defined as above or in Clause III or elsewhere in this CCAP. In the event of any conflict between this CCAP and any other written agreement between **Global Payments** and **Merchant** (including but not limited to the Merchant Card Processing Agreement), the terms of this **Agreement** shall control only with respect to matters addressed in this **Agreement**. Both **Global Payments** and **Merchant** agree that this **Agreement** is offered solely by **Global Payments**; and not Member Bank. Member Bank does not have any liability or responsibility under this **Agreement**.

I. COVERAGE

Global Payments will either reimburse or pay on behalf of **Merchant** those **expenses** contractually due to **claimants** as a result of an **incident**; provided always that the **incident** is **discovered** during the **coverage period**. In no event shall **Global Payments** be obligated for **expenses** after the applicable Limits of Liability have been exhausted by payment of **expenses**.

II. LIMIT OF LIABILITY

1. **Global Payments**' liability for all **expenses** arising from an **incident** shall be limited to the lesser of: actual expenses; or the "Each Incident" Limit of Liability as set forth herein. **Global Payments**' liability shall be further limited as delineated in paragraphs 2 thru 5 below.

2. Any "Per **MID**" Limit of Liability appearing herein is the total limit of **Global Payments**' liability under this Agreement for all **expense** arising from a single **MID**.

3. Any "Per **Merchant**" Limit of Liability appearing herein is the total limit of the **Global Payments**' liability under this policy for all **expense** arising from **Merchant**; regardless of the number of **MID's** or **merchant agreements**.

4. A "Per **Merchant** Hardware and Software Upgrade" Sub-Limit of Liability, as appearing herein, shall be part of and not in addition to the "Per **Merchant**" Limit of Liability.

5. A "Per **Merchant** EMV System" Sub-Limit of Liability, as appearing herein, shall be part of and not in addition to the "Per **Merchant**" Limit of Liability. In the event that a **Merchant** with EMV enabled and functional terminals or POS system in place at the **Merchant** location is held financially liable by the **card association** for a failure of the EMV cards (also referred to as smart cards, chip cards or IC cards), EMV enabled and functional terminals or POS system that results in a card present, counterfeit fraud card loss, the policy will provide an "Per **MID** EMV System" Sub-Limit of Liability. This financial liability must be due to counterfeit EMV cards (and not a lost or stolen EMV card. Each claim or loss must be documented by the proper **card association** reason codes (eg. Mastercard uses reason code 70). Such claims may be presented **Global Payments** at any time. However, claim payments will be aggregated and paid by **Global Payments** to Merchant on an annual basis in settlement for all such claims during each annual policy period. **Global Payments** will only make payment to Merchant. This reimbursement does not apply to: (a.) any **Merchant** without EMV enabled and functional terminals or POS systems in place at the **Merchant** location, (b.) any transaction(s) not processed through EMV enabled and functional terminals or POS systems in place at the **merchant** location; or (c.) any card not-present transactions no matter how those transactions are processed.

III. EXCLUSIONS

Global Payments shall not be obligated to pay, and this the reimbursements under this Agreement do not apply to, any **claim**, **demand** or **expenses** arising from or in connection with:

1. an **incident** known or discovered outside the term of this Agreement or reported **coverage period**.

2. an **incident discovered** before the effective date of the **merchant agreement**, or after the termination of such **merchant agreement**.

3. a **failure of security** specifically known to **Global Payments** or **Merchant** to exist on or before the **coverage period** that gives rise to an **incident**. This exclusion does not apply to network equipment, operating systems, or software applications in the possession of the **Merchant** and/or any third party vendors.

4. an **incident** caused by or resulting, directly or indirectly, from an act, error or omission of **Global Payments**, including, without limitation, the disclosure of any **cardholder information** by **Global Payments** or any entity to whom **Global Payments** provides **cardholder information**.

5. any fraudulent, illegal, dishonest or criminal act committed by, at the direction of, or with the direct knowledge of any director or officer of **Global Payments**.

6. any **incident** at **Merchant** which has experienced a prior **incident** unless **Merchant** was recertified to an eligible **PCI Compliance Level** as defined herein by a **qualified security assessor** prior to the current **incident**.

7. any costs or **expenses** incurred or required for **Merchant** to become PCI compliant in the first instance, prior to the occurrence of an **incident**.

8. any breach, damage, cost, penalty or fine incurred, assessed, transferred or charged back by any **card network**, card issuer, **acquiring bank**, **ISO** or **processor** for noncompliance with accepted **PCI Data Security Standards** other than an **expense** or **card replacement cost** arising from an **incident**.

9. any governmental or regulatory action, investigation, litigation or settlement seeking damages, contributions, restitution or injunctive relief or reimbursement of costs or **expenses** associated therefrom.

10. any third party action, investigation, litigation or settlement seeking damages, contributions, restitution or injunctive relief or reimbursement of costs or **expenses** associated therefrom other than an **expense** contractually created by the **merchant agreement** and arising from an **incident**.

11. war (whether or not declared), civil war, insurrection, rebellion, revolution, usurp of power, governmental intervention, or act of terrorism.

12. any software not within the control of **Merchant**. However, this exclusion is not intended to limit coverage for **expenses** arising from the use by third parties of software, virus, Trojan or malware to obtain fraudulent access to data on the **Merchant's** computer systems or to collect data in transit to or from the **Merchant's** computer systems.

13. any **incident** that occurs in any computer system in which multiple merchants with no legal relationship to one another have hosted accounts or share a common database, operating system or software applications.

14. an **incident** without: (a.) a formal written notification by the **card network** (including case number) to either the **acquiring bank**, **ISO** or **Merchant** of an incident; and (b.) a contractually enforceable **demand** by the **card network** for **expense** reimbursement due to an **incident**. This exclusion does apply to **hardware and software upgrades** that are required in order to avoid a **PCI Assessment**.

15. any **chargeback** of a consumer transaction made or processed by **Merchant**.

16. Amounts or charges incurred by **Merchant** unrelated to an **incident**, including but not limited to: employee compensation and benefits; overhead administrative or general expenses.

17. any transaction against a cardholder's account unless:

a. the transaction is a fraudulent or illegal use of a compromised **card** number; and

b. the card number is compromised as a direct result of an incident; and

c. a fine or **compliance case** is assessed by the **card network** for such transactions as a result of an **incident**; and

d. the resulting fine or **compliance case** is specifically covered by this Agreement as a **PCI Assessment** or **related cost**.

IV. DEFINITIONS

When used in this policy:

1. "**acquiring bank**" means a financial institution that accepts or acquires payment transactions from a **card** issued by itself or another financial institution.

2. "**ADCR**" means the Account Data Compromise Recovery process as established by the **card network**.

3. "**card**" means credit cards, debit cards, stored value cards, and pre-funded cards.

4. "**card network**" means any of the following associations or entities formed to administer and promote cards: MasterCard International, Inc., VISA U.S.A., Inc., VISA International, Inc., Discover Financial Services, American Express, JCB International Credit Card Company, Ltd. or any of the following Debit Provider Networks: Exchange/Accel, Interlink, Maestro, NYCE, Plus, PrestoLink, Shazam and STAR.

5. "**card replacement cost**" means any written **demand** received from the **card network** for payment of the monetary costs required to reproduce and distribute **cards** as a direct result of an **incident**.

6. "**chargeback**" means the procedure by which **Merchant's** sales draft or other indicator of a card transaction (or disputed portion thereof) is returned to **Merchant**, the liability for which is **Merchant's** responsibility. **Chargeback** does not include **compliance case** liability.

7. "**claim**" means a contractual **demand** for monetary reimbursement of **expenses** as a result of an **incident**.

8. "**claimant**" means either a:

   a. **card network** or **acquiring bank** assessing **PCI Assessments**, **related costs** and/or **card replacement cost**; or

   b. **qualified security assessor** incurring and seeking reimbursement for authorized **mandatory audit** fees;

   making **demand** for **expense** payment as a result of an **incident**. **Claimant** shall also include such party that has contractually assumed the right of **claimant** by payment of such **expenses**.

9. "**compliance case**" (or PCI-DSS Compliance Case) means a determination by a **card network**, following a written allegation by an issuing bank, that:

   a. an **incident** violated a specific operating rule of the **card network**; and

   b. the situation giving rise to the allegation is not covered by a **chargeback** right; and

   c. the issuing bank suffered a financial loss as the result of the **incident**.

10. "**coverage period**" means the term this CCAP Agreement is in effect.

11. "**data compromise**" means the exposure of **card** information that compromises the security, confidentiality, or integrity of personally identifiable information due to a **failure of security** at the **Merchant** level.

12. "**date of discovery**", "**discovered**" or "**discovery**" means the date appearing on the first formal written notification by the **card network** (including case number) to either **Global Payments, acquiring bank, processor, ISO** or **Merchant** of an **incident** or a request by the **card network** for a **mandatory audit**.

13. "**demand**" means any written request for payment of contractually recoverable **expenses**.

14. "**EMV"** means Europay, Mastercard and Visa, a global standard managed by EMVCo. for cards equipped with computer chips and the technology used to authenticate chipcard transactions.

15. "**expenses**" means **PCI Assessments**, **related costs**, **mandatory audit** fees, **card replacement cost** and/or **hardware and software upgrades** contractually assessed by the **card network** as a result of an **incident** and for which **Global Payments** is contractually liable. **Expense** does not include:

   a. any other economic damage, legal expenses, punitive or exemplary damages, legal or regulatory fines or penalties;

b. that portion of any award or judgment caused by the trebling or multiplication of actual damages under federal or state law;

c. the cost to restore consumer identities or monitor or verify the creditworthiness, credit accuracy or damage to credit of any consumer (including but not limited to fraud victim assistance, paying for any credit bureau report);

d. the costs to notify consumers of an actual **incident**; or

e. interchange fees, **chargeback** expenses or the amount of any transaction returned to the **acquiring bank, processor** or **Merchant**; or

f. fraudulent card charges not specifically assessed as a fine by the **card network**.

16. "**failure of security**" means:

a. the actual failure and inability of the security of computer system to mitigate loss from or prevent computer data infiltration; physical theft of hardware or firmware controlled by the **Merchant** (or components thereof) on which electronic data is stored, or through which electronic data passes, from a premises occupied and controlled by the **Merchant**. **Failure of security** shall also include such actual failure and inability above, resulting from the theft of a password or access code by non-electronic means; or

b. physical loss of information (including loss of receipts, employee theft and stolen databases).

17. "**hardware and software upgrade**" means software or hardware product upgrades necessary to confirm compliance with **PCI Data Security Standards** and avoid a **PCI Assessment** from being issued as the result of an **incident**.

18. "**incident**" means one or more actions, inactions, errors, omissions, unauthorized accesses, intrusions, breaches of security and/or breaches of duty at the **Merchant** level resulting in a **failure in security** at the **Merchant** level and ensuing **data compromise** as identified in and evidenced by a notification issued by the **card network**. Regardless of the number of unauthorized accesses, intrusions, security breaches or **data compromise** events, all activities at a **Merchant** resulting from common intruders (or conspiracy of intruders) or unauthorized software installations shall be considered a single **incident**. Continuous or repeated actions or exposure to substantially the same general harmful condition, injury or damage at **Merchant** shall also be considered a single **incident**. A **data compromise** that involves either (a.) multiple intrusions into the **Merchan**t's computer system that are enabled by the insertion of a worm, virus, key logger, trojan, or other device or (b.) the repeated use of a stolen or compromised password or access code at **Merchant** shall be considered a single incident. All **expenses** arising from the same **incident** or chain of related **incidents** at **Merchant** shall be considered a single **incident**.

19. "**ISO**" means registered Independent Sales Organization or merchant service provider.

20. "**mandatory audit**" means a forensic accounting and/or information technology examination of the **Merchant** required by the **card network** or **acquiring bank** that has been triggered by one or more cardholders indicating potential or actual fraudulent activities that the **card network** has cause to believe occurred due to a **data compromise**. **Mandatory audits** must be initiated by the **card network** or **acquiring bank** in writing and must be conducted by a **qualified security assessor**. The **mandatory audit** requires the **qualified security assessor** to examine the operations of the **Merchant** in order to either locate the source of the problem or to determine if non-compliance of the **PCI Data Security Standards** actually occurred.

21. "**Merchan**t" means the legal entity (including affiliates and subsidiaries) listed as a party to the **merchant agreement** with **Global Payments**.

22. "**merchant agreement**" means the Merchant Card Processing Agreement between **Merchant** and **Global Payments**.

23. "**MID**" means a merchant identification number.

24. "**PCI**" means Payment Card Industry.

25. "**PCI Assessment**" means any written demand against the **Merchant, Global Payments** or **acquiring bank** by the **card network** for monetary assessments or fines due to the **Merchant's** non-compliance with accepted **PCI Data Security Standards** resulting in an **incident** at the **Merchant** level.

26. "**PCI Compliance Level**" means the Payment Card Industry compliance level assigned by the **card network** based, in part, upon annual transaction volume. PCI Compliance Levels are currently designated 1 through 4.

27. "**PCI Data Security Standards**" means generally accepted and published Payment Card Industry standards for data security (DSS).

28. "**POS**" means point of sale.

29. "**Processor**" means an **acquiring bank** or **PCI** compliant system vendor approved by the **acquiring bank** to provide **card** processing services.

30. "**qualified security assessor**" shall mean a security assessor that has been certified as such by the **PCI** Security Standards Council.

31. "**related costs**" means any other costs in the process leading up to the **PCI Assessment** as demanded in writing by the **card network** and for which **Global Payments** is contractually liable as a result of an **incident**. **Related costs** includes

a. **compliance case** costs of the **card** issuer associated with the monitoring of at risk **card** accounts filed under the rules of the **card networks**; and

b. **ADCR** financial liability assessed by the **card network** for the uncollectible amount of any transaction against a **card** holder's account incurred directly as a result of fraudulent or illegal use of a compromised **card** number.

32. "**Global Payments**" means TSYS Merchant Solutions, LLC d/b/a Global Payments, or the applicable affiliate company of TSYS Merchant Solutions, LLC d/b/a Global Payments.

V. CONDITIONS

1. **Duties in the Event of Claim:**

a. As soon as practicable after the **date of discovery**, **Merchant** shall provide a written Notice of **Claim** to **Global Payments.** Such Notice of **Claim** shall include:

i. the circumstances by which the **incident** was **discovered**, including but not limited to, a copy of the first formal written notification by the **card network** (including case number) to **merchant** of an **incident** at the **merchant** level or a request for a **mandatory audit,** if applicable;

ii. **expenses** which may result or have resulted from the **incident**;

iii. evidence and description of the **incident** giving rise to the **claim**;

iv. any **demand**, notification letters, **mandatory audit** reports, fee and **expense** invoices and other documents pertinent to the **claim** that are in the possession of or obtainable by the **Merchant**.

b. **Global Payments** shall have the right to review all relevant documentation related to all **claims**, including correspondences and forensic reports, except to the extent such documentation is protected by attorney-client privilege or attorney-client work product doctrine.

c. To report claims to **Global Payments**, utilize the notice address provided for under the **merchant agreement.**

d. **Merchant** shall cooperate reasonably with **Global Payments** in the investigation and settlement of all **claims**, including but not limited to:

i. enforcing any contractual right to contest or mitigate any **expense**; and

ii. assisting in making statements; in the conduct of suits; and in enforcing any right of contribution or indemnity against others.

If **Global Payments** both prejudiced and damaged by the failure of the **Merchant** to comply with any of these duties, **Global Payments** may, at its discretion, deny liability for such **claim**. Should the **Merchant** be unable or unwilling to comply with any of the duties required herein, any successive party contractually liable for the **expenses** may assume such duties to comply with the terms and conditions of this Agreement.

e. Payment by any party of **expenses** shall not automatically bind **Global Payments** with respect to reimbursement of any **claim**.

f. As a condition precedent to reimbursement, the initial reporting of a **claim** to **Global Payments** must be no later than sixty (60) days after the end of the the term of this **Agreement.**

2. **Reimbursement**

a. Upon receipt of a Notice of **Claim**, **Global Payments** shall commence investigation and request all items, statements and information that **Global Payments** reasonably believes will be required. Additional requests may be made if, during the investigation of the **claim**, such additional requests are necessary.

b. Within thirty (30) days of receipt of all items, statements and information required by **Global Payments** to verify the **claim** and determine coverage (including but not limited to any **mandatory audit** results), **Global Payments** shall notify **Merchant** of **Global Payments'** acceptance or rejection of the **claim**. If **Global Payments** rejects the **claim**, in whole or in part, **Global Payments** shall state the reasons for the rejection. The parties may accept such rejection, exercise their rights under the policy, or submit an amended Notice of **Claim**. An amended Notice of **Claim** must be submitted within thirty (30) days of **Global Payments'** rejection and contain such additional information as necessary for **Global Payments** to reevaluate the reasons for rejection.

c. Payment of the **claim** shall be made within thirty (30) days after **Global Payments** reaches agreement with the **Merchant**, or the entry of a judgment against **Global Payments**. **Global Payments** will make payment to or on behalf of the **Merchant.**

d. **Global Payments** shall have the right to investigate, contest, defend, appeal and/or settle any **expense** (other than **mandatory audit expense**) assessed or otherwise brought by any party as it deems expedient. **Global Payments** shall have the right, but not the obligation, to defend the **Merchant** against any legal action initiated by a **claimant** to recover **expenses.**

e. **Global Payments** shall have the right to require any party receiving payment other than the **claimant** to execute a written release from liability acknowledging:

i. that payment by **Global Payments** to such party is in satisfaction of liability to the **claimant** under this **Agreemen**t; and

ii. such party has either paid such **expense** or contractually warrants to **Global Payments** that payments received from **Global Payments** will be property disbursed to the **claimant** or such successor in interest to the claim proceeds.

3. **Subrogation:** In the event of any payment of **expenses** under this policy, **Global Payments** shall be subrogated to all rights of recovery of such **expenses** as determined in a final adjudication in the underlying action. The **Merchant** shall execute and deliver instruments and papers and do whatever else is necessary to secure such rights. The **Merchant** shall not do anything after a **claim** to prejudice such rights without first obtaining the written consent of **Global Payments**. **Global Payments** shall not exercise any right of recovery against the **Merchant** in respect of any **claim** reimbursed under this **Agreement** unless such **claim** was the direct result of fraudulent, illegal, dishonest or criminal acts of **Merchant**.

4. **Assignment:** Unless specifically allowed in this policy, no right, duty or benefit may be assigned or transferred without the prior written consent of **Global Payments**.

5. **Action Against Global Payments:** No person or organization shall have any right to join **Global Payments** as a party to any action against the **Merchant** or any other party to determine the **Merchant's** liability, nor shall **Global Payments** be impleaded by the **Merchant** or any other party.

6. **Changes in Policy Terms:** No rights, terms or conditions of this policy may be waived, changed, altered, modified or deleted without the written agreement of **Global Payments**.

7. **Cancellation / Non-Renewal**: This Agreement may be canceled by either party at any time by written notice.

8. **Inspection of Records:** The **Merchant** shall keep record of all information relative to this **Agreement**. **Global Payments** may examine such records at any time during the **Agreement** and within two (2) years after the end of the **Agreement** as far as it relates to the subject matter of this **Agreement**. By **Global Payments'** right to examine or making an examination, **Global Payments** makes no representation that the **Merchant** or such records are in compliance with any law, rule or regulation.

9. **Schedule of Limits.**

Eligible Merchants: All PCI Compliance Level 3 and 4 merchants (not levied a previous PCI Assessment unless reinstated upon completion of PCI certification) reported for coverage under the policy. Coverage does not extend to Level 1 and 2 merchants unless specifically authorized by **Global Payments** in writing.

PCI Compliance	**"Per MID" Limit**	**"Per Merchant" Limit**	**"Each Incident" Limit**
Level 2 *	$100,000	$500,000	$500,000
Level 3	$100,000	$500,000	$500,000
Level 4	$100,000	$500,000	$500,000

“Per Merchant Hardware and Software Upgrade” Sub-Limit: $25,000

“Per Merchant EMV System” Sub-Limit: $10,000