COMPANY

Data Breach
Incident Response Plan

Document Revision History

Version Number	Date	Changed By	Description
1.0	12/5/2014	Name	Description

Table of Contents

1. Purpose of Data Breach Incident Response Plan.

This Data Breach Incident Response Plan is intended to provide guidance for COMPANY officials to take appropriate action when confidential information maintained by COMPANY is acquired by, accessed by, or disclosed to any unauthorized individual. The Plan is intended to reduce the risk of harm (including the risks of payment card fraud and identity theft) to individuals whose information COMPANY maintains, to prevent loss of public confidence in COMPANY, and to safeguard COMPANY's information assets.

2. Incident Response Team.

The Incident Response Team, under the supervision of Vice President of Marketing, is responsible for implementing the Plan. The mission of the Incident Response Team is to provide timely and effective responses to any disclosure of confidential information maintained by COMPANY to unauthorized persons.

The Incident Response Team has been authorized to take appropriate steps necessary to contain, to mitigate, and to resolve incidents that include the disclosure of confidential information maintained by COMPANY. The Team is responsible for managing the investigation of data breach incidents, for reporting the Team's findings to appropriate management members, and for taking additional action as needed.

The Incident Response Team is responsible for maintaining the accuracy of this Plan and for modifying it as necessary to reflect current COMPANY processes and any new legal requirements. The Team will meet at least once each quarter to review the Plan and to assess COMPANY's ability to implement the Plan.

3. Types of Confidential Data Maintained by COMPANY.

COMPANY may create or store the following types of confidential information:

- Payment card data, which includes account numbers, expiration dates, cardholder names, and cardholder addresses.
- "Personally Identifiable Information" of COMPANY customers, which means for purposes of this Plan:
    - A customer's first name or first initial and last name in combination with any of the following:
        - The customer's Social Security Number,
        - The customer's Driver's License or Identification Card number,
        - The customer's financial account number (bank account, credit card, or debit card number),
        - The customer's home address or e-mail address; or
        - The customer's medical or health information.

- COMPANY's confidential financial information.
- COMPANY's trade secret information, including but not limited to the source code of computer programs developed by or for COMPANY.

4. Definition of "Data Breach"

A "data breach" includes

- The acquisition of any of the confidential information described in section 3 by a person or entity not authorized to have the information, regardless of method by which the information is acquired;
- The disclosure of any of the confidential information described in section 3 to a person or entity not authorized to review the information, regardless of how the information is disclosed; and
- The unauthorized access to any of the confidential information described in section 3 that could compromise the security, confidentiality, or integrity of the information, regardless of how the unauthorized access to the information occurs.

5. Incident Response Team Members.

The Incident Response Team includes the following members:

- Vice President of Information Technology;
- Vice President of Marketing; and
- Executive Director, Finance

If the investigation of a data breach suggests that an action or failure to act by a COMPANY employee caused or contributed to the breach, Team members will consult with Director of Human Resources, to ensure that COMPANY takes appropriate actions regarding the employee.

6. Levels of Data Breaches.

For purposes of this Plan, a Level 1 data breach includes:

- The disclosure of, or unauthorized access to, COMPANY financial information.
- The disclosure of, or unauthorized access to, 100 or more individuals' payment card data or personal information.

Level 2 data breaches include all other data breaches.

Responses to Level 1 and Level 2 data breaches will be managed by the Vice

President of Marketing. Management of the response to Level 2 data breaches may be delegated by the Vice President of Marketing to another manager of his or her choice. The person to whom the management of the response to Level 2 data breach has been delegated will report as appropriate to the Vice President of Marketing.

7. Known and Suspected Data Breaches Should Be Reported.

All known or suspected data breaches should be reported to the Vice President of Information Technology. The Vice President of Information Technology will screen the incident as quickly as possible:

- To determine whether the reported breach is an actual breach or not;
- For electronic breaches, to determine if there is an ongoing intrusion and if so, to take all necessary steps to cut-off any continued access to compromised servers or other computers by unauthorized persons;
- For a confirmed data breach, to determine whether the breach is a Level 1 or Level 2 breach;
- To convene a meeting of the Incident Response Team, including the Vice President of Marketing, for all breaches.

8. Incident Response Team Members' Roles and Responsibilities.

8.1 Actions the Team Should Take and Team Member Responsible.

The Incident Response Team should take the following steps as quickly as possible under the supervision of the Vice President of Marketing for Level 1 breaches and under the supervision of the Vice President of Marketing or his or her delegatee for Level 2 breaches:

8.1.1 Notify COMPANY officials.

For all Level 1 breaches, the Vice President of Marketing will notify COMPANY's President of the breach and should update the President on an hourly basis. The President will notify the Chairman of the COMPANY Board of Directors and the Vice President of Marketing will notify COMPANY's general counsel. If it is known or suspected that a COMPANY employee caused or contributed to causing the breach, the Vice President of Marketing will notify the Human Resources Director.

For Level 2 breaches, the Vice President of Marketing or his or her delegatee will notify COMPANY's President of the breach and will update the President at least every 6 hours. The Vice President of Marketing will determine whether to notify other COMPANY officials and, if so, when to do so. If a COMPANY employee caused or contributed to a Level 2 breach, or is suspected to have done so, the Vice President of Marketing or his or her delegatee will notify the Human Resources Director.

8.1.2 If the breach involves electronic data --

For both Level 1 and 2 breaches that involve electronic information, the Vice President of Information Technology will ensure that no actions are taken that will compromise potentially relevant computer log files, configuration information, or other pertinent evidence.

8.1.3 Image electronic evidence and investigate the breach.

The Vice President of Information Technology, together with his staff and forensic investigators, if they are requested to assist as described in sections 8.1.4.1 or 8.1.4.2 below, should image any potentially relevant computer log files, configuration information, and other data. Files should be retained for use as evidence in any criminal prosecution or civil litigation. When such files and other information have been imaged, the investigation, under the Vice President of Information Technology's supervision, should attempt to determine how the breach occurred.

8.1.4 Notify payment card entities and other payment processors.

If a data breach potentially affects any payment card data or other payment processor's data (such as related to "Bill Me Later," PayPal, electronic check processors, banks that process wire payments, ACH, or similar payment processors), the Executive Director, Finance should notify the designated individuals at VISA, MasterCard, Federal Express, other payment card entities, or payment processors whose data were acquired, accessed, or disclosed and will supervise providing required or requested information to payment card entities or other payment processors. Instructions for notifying payment card entities are included in Appendix 2. If COMPANY's merchant bank or banks require or request that COMPANY provide certain information, the Executive Director, Finance will provide that information as well. Prior to providing any information to persons not employed by COMPANY, the Executive Director, Finance will work with other Team members and with COMPANY's attorneys to ensure that the information should be provided and is accurate.

8.1.4.1 Cooperate with any forensic investigators designated by a payment card entity.

If any payment card entity determines that a forensic investigator designated by the payment card entity should investigate the breach, the Senior Manager, Payments 7 Fraud will coordinate with the payment card entity to provide access to the forensic investigator designated by the payment card entity. The Executive Director, Finance will take appropriate action to assist the forensic investigator to complete any report to the payment card entity that the entity requires the investigator to complete.

8.1.4.2 Determine whether to use a COMPANY-designated forensic investigator if one is not required by any payment card entity.

If no payment card entity requires a forensic investigator to investigate the breach, the Vice President of Information Technology will determine whether a forensic investigator chosen by COMPANY should nonetheless be asked to investigate the breach. If such an investigator is hired, the Vice President of Information Technology will supervise the investigator. If electronic data were acquired or accessed by unauthorized persons or were disclosed, the investigation should determine how the pertinent computer or server was penetrated, by whom or from what IP address, when the intrusion occurred, and what data were copied or exported. The individuals conducting the investigation should carefully document their investigation and complete a report as soon as possible. If a forensic investigator chosen by COMPANY is asked to assist, the Vice President of Information Technology will determine whether the investigator's report should be made to COMPANY's attorneys or directly to the Team.

8.1.5 Take additional corrective actions as necessary.

If the investigation of a data breach shows that inadequate computer network security, substandard software patch maintenance, poor physical security, deficiencies in any intrusion detection and response systems, or any other correctable cause or causes contributed to the breach, the Vice President of Information Technology will ensure that corrective action is taken as soon as possible. If the breach involved electronic data, corrective actions should not be taken until potentially relevant data are imaged as described in section 8.1.3.

8.1.6 Decide whether to notify law enforcement.

As soon as possible after information regarding a data breach is available to the Team, the Team will discuss whether law enforcement should be notified of the breach. The Team will solicit input from COMPANY's attorneys and President regarding this decision. For Level 1 breaches, the Vice President of Marketing will be responsible for making the final decision about whether to notify law enforcement, after discussing the matter with whomever he determines is appropriate, and for notifying appropriate law enforcement officials if the decision is made to do so. For Level 2 breaches, the Vice President of Marketing or his or her delegatee will be responsible for the final decision and for notifying appropriate law enforcement officials if the decision is made to do so.

8.1.7 Notify insurers.

When sufficient information regarding a breach has been determined, Executive Director, Finance will work with COMPANY's attorneys to submit a claim to each insurance carrier that has issued coverage to COMPANY that arguably covers damages that may be related to the breach.

8.1.8 Determine whether customers or employees must be or will be notified.

After the Team learns what information has been acquired, accessed, or disclosed, the Team should solicit input from COMPANY's attorneys regarding whether applicable state, federal, or other countries' data breach notice laws require that potentially affected customers or employees must be notified of the breach. For example, if COMPANY stores unencrypted personal information of a COMPANY customer who is a Nevada resident and the information is reasonably believed to have been acquired by an unauthorized person, Nevada law requires COMPANY to notify the customer. In those instances where notice is not mandatory, (1) for Level 1 breaches, the Team will recommend to the Vice President of Marketing whether to notify customers or employees and the Vice President of Marketing will decide whether to do so, and (2) for Level 2 breaches, the Team the will make a similar recommendation to the Vice President of Marketing or to his or her delegatee, and the Vice President of Marketing or his or her delegatee will decide whether COMPANY should provide such notices after consulting with whomever he or she decides is appropriate.

8.1.9 Notify public agencies and credit reporting agencies as required by law.

If a data breach discloses personal information of more than 1000 residents of the state of Indiana, the Executive Director, Finance will, as required by Indiana law, shall disclose to all credit reporting agencies that (a) compile and maintain files on consumers on a nationwide basis, and (b) assemble or evaluate public record information and credit account information from persons who furnish such information regularly in the ordinary course of business, and (c) do so for the purpose of furnishing consumer reports to third parties bearing on a consumer's creditworthiness, credit standing, or credit capacity, information necessary to assist credit reporting agencies prevent fraud.

If a data breach discloses personal information of a resident of the commonwealth of Massachusetts, the Executive Director, Finance will, as required by Massachusetts law, notify the Massachusetts Attorney General and the Massachusetts Director of Consumer Affairs and Business Regulation of the nature of the breach, the number of residents of the commonwealth of Massachusetts potentially affected by the incident as of the date notices were sent to such residents, and the steps COMPANY has taken or plans to take regarding the incident.

If a data breach discloses personal information of a resident of the State of New Hampshire, the Executive Director, Finance will, as required by New Hampshire law, notify the New Hampshire Attorney General of the breach, the anticipated date that notices will be sent to New Hampshire residents regarding the breach, and the approximate number of residents of New Hampshire who will be notified.

If a data breach discloses personal information of a resident of the State of New York, the Executive Director, Finance will, as required by New York law, notify the Attorney General of the State of New York, the New York State Consumer Protection

Board, and the New York State Office of Cyber Security & Critical Infrastructure Coordination of the breach, the approximate number of New York residents potentially affected by the breach, and of the timing, content, and distribution of the notices to New York residents. If more than 5,000 residents of New York will be notified of a breach, the Executive Director, Finance will request from the New York Attorney General the list of consumer reporting agencies that must be notified of the breach and will send notices to those consumer reporting agencies.

If a data breach discloses personal information of more than 1000 residents of the state of North Carolina, the Executive Director, Finance will, as required by North Carolina law, notify the following agencies of the breach and of the timing, content, and distribution of the notices to North Carolina residents: (1) the Consumer Protection Division of the North Carolina Attorney General's Office, and (2) all credit reporting agencies that (a) compile and maintain files on consumers on a nationwide basis, and (b) assemble or evaluate public record information and credit account information from persons who furnish such information regularly in the ordinary course of business, and (c) do so for the purpose of furnishing consumer reports to third parties bearing on a consumer's creditworthiness, credit standing, or credit capacity.

If a data breach discloses personal information of a resident of Norway, the Executive Director, Finance will, as required by Norwegian law, notify the Norwegian Data Inspectorate of the breach and its potential effect on Norwegian residents.

The addresses of these agencies are stated in Appendix 3. Forms of letters for notifying these agencies are included in Appendix 7.

8.1.10 Determine what to tell COMPANY managers and employees, then distribute the information.

When the Team has received sufficient information regarding a breach, the Vice President of Marketing will coordinate a discussion among Team members about what information to share with other company managers and employees. When the Team has reached a consensus, if the decision is to provide certain information to company managers and employees, the Vice President of Marketing will supervise the drafting of a proposed notice to such individuals and will send the recommended notice to the President or delegate, as appropriate depending on the level of data breach. The memos should ask or direct employees not to speak to the media or others outside the company about the data breach and to direct all inquiries to the Vice President of Marketing. Once the content of such internal notices has been decided, the Vice President of Marketing will supervise the distribution of the notices to COMPANY managers and employees.

8.1.11 Prepare COMPANY to respond to inquiries from the media, customers, and employees regarding the breach.

The Vice President of Marketing will coordinate a discussion among Team members to determine what information to provide to media, to customers, and to employees in response to their inquiries. After receiving recommendations from Team

members, the Vice President of Marketing will be responsible for drafting or working with COMPANY's public relations firm to draft press releases, telephone call response scripts, and any website disclosures about the breach. For Level 1 breaches, the Vice President of Marketing will also designate an individual who will be assigned to monitor information on the Internet, especially on blogs, to identify and to respond to any misinformation regarding the breach before it is further circulated on the web or by the mainstream media.

8.1.12 Notify Potentially Affected Customers or Employees.

If notice to potentially affected customers or employees is legally required or if COMPANY management determines to notify such individuals if notice is not required, the Vice President of Marketing will coordinate the distribution of such notices. If a large number of such notices need to be sent, the Vice President of Marketing will work with the Team to select a vendor and to determine the services the vendor should provide. The Vice President of Marketing or delegate will decide whether or not to hire a vendor for both Level 1 and 2 breaches. If a vendor is hired, the Vice President of Marketing will supervise the vendor's performance of its services. The Vice President of Marketing, working with COMPANY's attorneys and with its public relations professionals (if he chooses to consult the public relations firm), and with any vendor chosen to assist in sending notices, will be responsible for providing the content of notices sent to individuals.

8.1.13 Respond to inquiries from the media and the public.

The Vice President of Marketing or his designee will provide responses to inquiries from the media, from employees, and from individuals in the public after receiving approval for the planned responses through the Vice President of Marketing or delegate, as appropriate. Either the Vice President of Marketing or his designee will be the spokesperson for COMPANY regarding the data breach. Responses to such inquiries should be appropriate for at least four potential audiences: the person who is inquiring, the public at large who may learn about the COMPANY response to the breach through such statements, and the judge and possibly a jury who may decide any legal claims brought against COMPANY regarding the data breach.

8.1.14 Retain records related to the breach.

For both Level 1 and Level 2 data breaches, the Vice President of Information Technology will send a written directive to all company personnel and contractors involved in the breach or in responding to the breach to retain all paper and electronic records related to the incident until further notice. The Vice President of Information Technology will send periodic reminders to the same individuals to retain such records and will work with COMPANY's attorneys to determine whether to suspend any automated electronic information purging practices, such as any periodic deletion of e-mail messages and any periodic over-writing of back-up media, to preserve potentially relevant records. After consulting with COMPANY attorneys, the Vice President of Information Technology will notify the company personnel and contractors who retained such documents when the documents may be discarded.

8.2 Summary of Required Actions by Each Team Member.

Team Member	Level 1 Breach	Level 2 Breach
Vice President of Marketing	Manage Incident Response Team	Same or delegate responsibility to do so
	Notify COMPANY President, update President hourly, notify general counsel of breach	Notify COMPANY President or delegate that responsibility; update President at least every 6 hours
	Decide whether to notify law enforcement and do so if determined appropriate	Same or delegate that responsibility
	Decide whether to send non-mandatory notices	Same or delegate that responsibility
	Provide recommendation to President on decision of whether to hire vendor to assist with sending notices, to provide credit monitoring and other services, or to do both	Same
	If COMPANY employee was involved or suspected, notify Human Resources	Same or delegate that responsibility
	Coordinate discussion of what to tell COMPANY managers and employees about the breach; supervise drafting and distributing such notices	Same
	Coordinate discussion of what to tell the media, COMPANY customers and the public about the breach; supervise drafting press releases, other public statements, and notices to customers	Same
	Supervise responses to inquires from the media, customers, and individual members of the public about the breach; serve as spokesperson for COMPANY regarding the breach or designate someone to do so.	Same
	Coordinate sending notices to customers; make recommendation to the President regarding whether to hire a vendor to assist sending	Same

Team Member	Level 1 Breach	Level 2 Breach
	such notices, to provide credit monitoring and other services, or both; supervise vendor if President decides a vendor should be hired	
	Supervise development of (1) answers to FAQs to post on COMPANY website and (2) call center scripts	
	Supervise monitoring of information on the Internet related to the breach	
Vice President of Information Technology	Evaluate reports of known and suspected breaches	Same
	Determine whether there has been a breach and, if so, whether it is a Level 1 or 2 breach	Same
	Notify the Vice President of Marketing of breach	Same
	Convene meeting of Incident Response Team	Same
	For breaches involving electronic data, ensure that potential server logs and other pertinent data are preserved	Same
	Determine whether to hire forensic investigator when not required by payment card entity or other payment processor, and if such an investigator is hired, supervise the investigator's work	Same
	Determine whether any investigator's report should be to Team or VDC attorneys	Same
	Ensure that corrective actions are taken to prevent a similar breach	Same
	Send written notices to all employees and any vendors involved in responding to the breach directing them to retain all documents, including electronic documents, related to the breach;	Same

Team Member	Level 1 Breach	Level 2 Breach
	determine whether to suspend automatic deletion or overwriting of electronic information about the breach, and if so, implement that decision and periodically ensure that documents are being retained	
Executive Director, Finance	If payment card data or other payment processor's data are accessed or disclosed, notify payment card entities or payment processors of breach and provide required information to them	Same
	If payment card entity, other payment processor, or merchant bank requires that its forensic investigators investigate the breach, assist such investigators and provide required information to them.	Same
	Work with COMPANY attorneys to submit claims to insurers	Same
	Notify agencies required by Indiana, Massachusetts, New Hampshire, New York, and North Carolina laws if breach discloses personal information of residents of those states; notify Norwegian Directorate if breach discloses personal information of residents of that country	Same

Appendix 1 – Incident Response CHECKLIST

	TASK	RESPONSIBILITY
☐	Terminate on-going attack	IT
☐	Notify VP-IT and Incident Response Team	IT
☐	Determine who will coordinate responses	Incident Response Team
☐	Image potentially relevant data	IT
☐	Investigate the intrusion	IT
☐	Take additional corrective actions if needed	IT
☐	Decide whether to notify law enforcement	Incident Response Team
☐	Notify payment processor, card associations, and any other payment vendors affected	Finance
☐	Determine whether to notify potentially affected customers and whether to offer them assistance	Incident Response Team
☐	Decide what to tell company managers and employees about the incident	Incident Response Team
☐	Prepare to respond to media, customer, and employee inquires	MKTG
☐	Notify insurers	Finance
☐	Notify company managers and employees	HR
☐	Notify potentially affected customers if required or if management chooses to do so	MKTG
☐	Respond to inquires	MKTG
☐	Retain all records related to the incident for potential litigation	ALL

Appendix 2 – Data Breach Incident Response Team
(as of DATE)

NAME
VP – IT
Work:
Cell:
Email: name@COMPANY

NAME
VP – Marketing
Work:
Cell:
Email: name@COMPANY

NAME
Executive Director, Finance
Work:
Cell:
Email: NAME@COMPANY

Conference Bridge

Data Breach Central Location
<fileserver> or <URL>

Appendix 3 – Data Breach QUICK ACTION LIST

If you do not read any other part of this CRISIS MANAGEMENT binder, at the very least, **PLEASE FOLLOW THESE "MUSTS":**

1. **Do NOT comment, speculate or assume anything**
   Remember - Nothing is "off the record"

2. ***GO!*** **Immediately take action by calling one of the following until someone is reached:**

NAME
VP – IT
Work:
Cell:
Email: name@COMPANY

NAME
VP – Marketing
Work:
Cell:
Email: name@COMPANY

NAME
Executive Director, Finance
Work:
Cell:
Email: NAME@COMPANY

Communication Procedures

In a time of crisis, it's especially important to understand how news travels, even by word-of-mouth. The slightest misinformation can find its way into national and international news if someone is not careful. With internet, satellite, cell phone and fax, all news is international news the minute it happens. Due to the rapidity with which news can now spread in this high-tech information age, it is essential that news be disseminated accurately, efficiently and completely.

Contact Immediately

NAME
VP – Marketing
Work:
Cell:
Email: name@COMPANY

NAME
Public Relations
Work:
Cell:
Email: name@COMPANY

Following are the key questions that need to be addressed

1. What happened and why did it happen?
2. How was it discovered and has it ever happened before?
3. Who was responsible and what is being done about it?
4. How does it affect our clients, customers, stakeholders, and employees?

Guidelines to Follow

- SPEAK WITH ONE VOICE - actions must be prioritized to seize control of the situation so that it does not seize control of you.
- TELL THE TRUTH – be simple and straight-forward. Organizations that tell the truth fare far better than those who try to cover up the facts.
- TAKE RESPONSIBILITY – Do not deny or be defensive.
- CONTROL AND CENTRALIZE COMMUNICATIONS (ALLOCATE APPROPRIATE SPOKESPEOPLE) – eliminates public confusion and different versions of the crisis in the media
- COMMUNICATE WITH STAKEHOLDERS AS OPENLY AS POSSIBLE AS SOON AS POSSIBLE – could include acknowledging problem; publicly take responsibility to further investigate, and offering assistance to all affected.

Communicating with the Media

The corporation is to provide appropriate communications to all media, external parties, and internal parties. All staff media inquiries should be referred to **NAME**. Below are some media communication guidelines, which will help should you find yourself in an unavoidable situation where you are required to speak directly to the media:

- TELL THE TRUTH – If you do not know the answer to a question, say so, and promise to get back with the information as soon as possible. It is better to provide accurate information at a later time than to speculate.
- BE WELL PREPARED – Review the facts, press releases, and previous company statements so that you can clearly articulate the issues and the company's actions.
- Assume everything is ON THE RECORD – Do not say anything that you don't want to be repeated. Anything that you say is fair game for journalists and you may ASSUME you will see it appear in print somewhere.
- LOG EVERYTHING – Keep a detailed record of calls in and out to be able to track public and media response.
- Repeat key themes and messages throughout the interview – Focus on the key messages and themes that the company wants to communicate. Be positive and stay in control of the story.
- Think of journalists as intermediaries, not your audience – Do not get lured into a debate or take their questions personally. They are doing their job; your job is to not let them slant your story.
- Do not let reporters put words in your mouth – If a reporter says, "So in other words..." or "What you are trying to say is..." think carefully before you respond. Use your own words.
- You do not have to answer every question – If a reporter asks for proprietary information, simply explain that you cannot disclose such information.
- Respect deadlines, but do not be driven by them. Don't feel pressured to make a statement on the spot to accommodate a reporter. Note his or her questions and call back with a prepared response in a timely manner.
- Stay within your area of knowledge and authority. Don't discuss issues you don't know about.
- Politely correct false assumptions or erroneous facts. If a reporter's question is based on false information, don't answer the question until you have pointed out the factual error.
- Offer "third-party" sources. Offer names and phone numbers of industry experts, employees, governmental officials, etc., who can be called to support your key messages
- Avoid hypothetical questions. Only answer questions based on the facts as you know them.
- Do not engage in speculation. Ever. Never speculate about the company, the crisis or competitors.

- ❖ Do not make personal comments. Any comment you make can be quoted as the company's position, which may not be the case.
- ❖ Stop, think, and correct your answer or statement. If you make a mistake or give a reporter inaccurate information it is important to correct the error immediately.

Appendix 4 – Contact Sheet

COMPANY President

COMPANY Director of Human Resources

COMPANY Risk Management

Legal Counsel

Public Relations Firm

Card Associations

Visa Fraud Control Group – (650) 432-2978

MasterCard Compromised Account Team – (636) 722-4100

American Express Merchant Services – (800) 528-5200

Discover Fraud Prevention – Nancy Petree nancypetree@discover.com (800) 767-7389

Payment Processor

Chase Paymentech Solutions Merchant Services - (603) 896-8333
Account Manager – **NAME**

Public agencies that must be notified if residents of their state or country are affected

New York:

New York State Attorney General's office
The Capitol
Albany, NY 12224-0341
(518) 474-7330
Website: http://www.oag.state.ny.us/home.html

New York State Consumer Protection Board
5 Empire State Plaza, Suite 2101
Albany, New York 12223
Phone: 518-474-3514
Fax: 518-474-2474
E-Mail: webmaster@consumer.state.ny.us
Website: http://www.consumer.state.ny.us/default.htm

New York State Office of Cyber Security & Critical Infrastructure Coordination
30 S. Pearl Street
Albany, New York 12207-3425
phone: 518-474-0865
fax: 518-402-3799
E-Mail: info@cscic.state.ny.us
Website: website@cscic.state.ny.us

Massachusetts:

Office of Attorney General
One Ashburton Place
Boston, MA 02108

Contact Sheet – Continued

Office of Consumer Affairs and Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116

New Hampshire:

New Hampshire Attorney General's Office
Department of Justice
33 Capitol Street
Concord, NH 03301

North Carolina:

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001

Norway:

The Data Inspectorate
Mail address: P.O. Box 8177 Dep, N-0034 Oslo, Norway
Telephone: +47 22 39 69 00
Fax: +47 22 42 23 50
E-mail:postkasse@datatilsynet.no
Website: http://www.datatilsynet.no/templates/Page____194.aspx (English version)
Contact Sheet - Continued

Credit Reporting Agencies

Acxiom Corporation
6111 Oak Tree Blvd.
Cleveland, Ohio 44131

Chex Systems, Inc.
Attn: Consumer Relations
7805 Hudson Rd, Suite 100
Woodbury, MN 55125

ChoicePoint Credit Consumer Center
PO Box 105289
Atlanta, GA 30348

Equifax
P.O. Box 740256
Atlanta, GA 30374

Contact Sheet - Continued

Experian
P.O. Box 9595
Allen, TX 75013-9595

First Advantage SafeRent
Consumer Relations Department
7300 Westmore Rd., Suite 3
Rockville, MD 20850-5223

Innovis Consumer Assistance
P.O. Box 1358
Columbus, OH 43215

ISO Customer Service Division
545 Washington Boulevard
Jersey City, NJ 07310

LexisNexis Matthew Bender
1275 Broadway
Albany, NY 12204

MIB, Inc.
P.O. Box 105, Essex Station
Boston, MA 02112

TeleCheck Services
5251 Westheimer
Houston, TX 77056

TransUnion
P.O. Box 2000
Chester, PA 19022

UD Registry
P.O. Box 9140
Van Nuys, CA 91409

Forensic Investigator
TBD

Direct Mail
TBD

Appendix 5 – Payment Card Entity Notice Requirements

Specific requirements for reporting suspected or confirmed breaches of cardholder data.

MasterCard Specific Steps:

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team by phone at 1-636-722-4100.

2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail, to compromised account team@mastercard.com.

3. Provide the MasterCard Merchant Fraud Control Department with the complete list of all known compromised account numbers.

4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).

5. Provide weekly written status reports to MasterCard, addressing open questions and issues, until the audit is complete to the satisfaction of MasterCard.

6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.

7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs; and

2. Distribute the account number data to its respective issuers.

Visa U.S.A. Specific Steps

Refer to documentation online at
http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html?it=c|/merchants/risk_management/cisp_if_compromised.html|Steps%20for%20Compromised%20Entities#anchor_3

In the event of a security breach, the Visa U.S.A. Operating Regulations require entities to immediately report the breach and the suspected or confirmed loss or theft of any material or records that contain cardholder data.

Steps and Requirements for Compromised Entities

1. Immediately contain and limit the exposure.

   To prevent further loss of data, conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:
   - Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT).[1]
   - Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
   - Preserve logs and electronic evidence.
   - Log all actions taken.
   - If using a wireless network, change Service Set Identifier (SSID) on the access point and other machines that may be using this connection (with the exception of any systems believed to be compromised).
   - Be on HIGH alert and monitor all Visa systems.

2. Alert all necessary parties, including:

   - Internal information security group and Incident Response Team, if applicable
   - Legal department
   - Merchant bank
   - Visa Fraud Control Group at (650) 432-2978.
   - Local FBI Office U.S. Secret Service if Visa payment data is compromised.

3. Provide the compromised Visa account or accounts to Visa Fraud Control Group at (650) 432-2978 within 24 hours.

[1] A person with unlimited access privileges who can perform any and all operations on the computer.

- Account numbers must be securely sent to Visa as instructed by Visa. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to Issuers and ensure the confidentiality of entity and non-public information.

4. Requirements for Compromised Entities

- All merchant banks must:
    - Within 48 hours of the reported compromise, proof of Cardholder Information Security Program compliance must be provided to Visa.
    - Provide an incident report document to Visa within four business days of the reported compromise
    - Depending on the level of risk and data elements obtained the following must be completed within four days of the reported compromise:
        - Undergo an independent forensic review
        - Complete a compliance questionnaire and vulnerability scan upon Visa's discretion

VISA Forensic Investigation Guidelines

An entity must initiate investigation of the suspected or confirmed loss or theft of account information within 24 hours of compromise.

The following must be included as part of the forensic investigation:

1. Determine cardholder information at risk.

    a. Number of accounts at risk, identify those stored and compromised on all test, development, and production systems
    b. Type of account information at risk
    c. Account number
    d. Expiration date
    e. Cardholder name
    f. Cardholder address
    g. CVV2[2]
    h. Track 1 and Track 2[3]

[2] CVV2 is an authentication process established by credit card companies to further efforts towards reducing fraud for Internet transactions. It consists of requiring a card holder to enter the CVV2 number at transaction time to verify that the card is on hand. This number is printed on MasterCard & Visa cards in the signature area of the back of the card. (It is the last 3 digits AFTER the credit card number in the signature area of the card).

[3] Track 1 is a "track" of information on a credit card that has a 79-character alphanumeric field for information. Normally a credit card number, expiration date and customer name are contained on track 1. Track 2 is a "track" of information on a credit card that has a 40character field for information. Normally a credit card number and expiration date are contained on track 2.

i. Any data exported by intruder

2. Perform incident validation and assessment.

   a. Establish how compromise occurred
   b. Identify the source of compromise
   c. Determine timeframe of compromise
   d. Review entire network to identify all compromised or affected systems, considering the e-commerce, corporate, test, development, and production environments as well as VPN, modem, DSL and cable modem connections, and any third-party connections.
   e. Determine if compromise has been contained.

3. Check all potential database locations to ensure that CVV2, Track 1 and Track 2 data are not stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments data on software engineers' machines, etc.).

4. If applicable, review VisaNet endpoint security and determine risk.

5. Preserve all potential electronic evidence on a platform suitable for review and analysis by a court of law if needed.

6. Perform remote vulnerability scan of entity's Internet facing site(s).

Visa Incident Report Template

This report must be provided to Visa within 14 days after initial report of incident to Visa. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to Visa and Merchant Bank. Visa will classify the report as "Visa Secret"*.

I. Executive Summary
   a. Include overview of the incident
   b. Include Risk Level (High, Medium, Low)
   c. Determine if compromise has been contained

II. Background

III. Initial Analysis

---

* This classification applies to the most sensitive business information, which is intended for use within Visa. Its unauthorized disclosure could seriously and adversely impact Visa, its employees, member banks, business partners, and/or the Brand.

IV. Investigative Procedures
    a. Include forensic tools used during investigation

V. Findings
    a. Number of accounts at risk, identify those stored and compromised
    b. Type of account information at risk
    c. Identify ALL systems analyzed. Include the following:
        i. Domain Name System (DNS) names
        ii. Internet Protocol (IP) addresses
        iii. Operating System (OS) version
        iv. Function of system(s)
    d. Identify ALL compromised systems. Include the following:
        i. DNS names
        ii. IP addresses
        iii. OS version
        iv. Function of system(s)
    e. Timeframe of compromise
    f. Any data exported by intruder
    g. Established how and source of compromise
    h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments data on software engineers' machines, etc.).
    i. If applicable, review VisaNet endpoint security and determine risk.

VI. Compromised Entity Action

VII. Recommendations

VIII. Contact(s) at entity and security assessor performing investigation

Discover Card Specific Steps:

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102.

2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.

3. Prepare a list of all known compromised account numbers.

4. Obtain additional specific requirements from Discover Card.

American Express Specific Steps:

1. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200.

2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.

3. Prepare a list of all known compromised account numbers.

4. Obtain additional specific requirements from American Express.

Appendix 6 – COMPANY Fact Sheet

COMPANY is the …

Appendix 7 – Public Agency and Credit Reporting Agency Notification Templates

[Required notice if more than 1,000 Indiana residents' personal information is disclosed]

[Insert date]

Acxiom Corporation
6111 Oak Tree Blvd.
Cleveland, Ohio 44131

Chex Systems, Inc.
Attn: Consumer Relations
7805 Hudson Rd, Suite 100
Woodbury, MN 55125

ChoicePoint Credit Consumer Center
PO Box 105289
Atlanta, GA 30348

Equifax
P.O. Box 740256
Atlanta, GA 30374

Experian
P.O. Box 9595
Allen, TX 75013-9595

First Advantage SafeRent
Consumer Relations Department
7300 Westmore Rd., Suite 3
Rockville, MD 20850-5223

Innovis Consumer Assistance
P.O. Box 1358
Columbus, OH 43215

ISO Customer Service Division
545 Washington Boulevard
Jersey City, NJ 07310

LexisNexis Matthew Bender
1275 Broadway
Albany, NY 12204

MIB, Inc.
P.O. Box 105, Essex Station
Boston, MA 02112

TeleCheck Services
5251 Westheimer
Houston, TX 77056

TransUnion
P.O. Box 2000
Chester, PA 19022

UD Registry
P.O. Box 9140
Van Nuys, CA 91409

Re: Unauthorized disclosure of personal information of more than 1000 Indiana residents

Dear Sir or Madam:

On _____, 20__, the personal information of approximately ___ Indiana residents was apparently disclosed to an unauthorized person when _____ . **[Describe the nature of the data breach, e.g., "a thief**

electronically penetrated one of COMPANY's servers and copied files that included customers' names and payment card information."]
COMPANY is planning to mail notices to all persons potentially affected by the disclosure, including Indiana residents. The notices will advise those persons that they may contact credit reporting agencies to request that a fraud alert be placed on their credit records. COMPANY asks that you cooperate with any individuals who make such a request of your agency. Please let me know if there is additional information that I may be able to provide to you regarding the data breach that is necessary to assist your agency prevent fraud.

Sincerely,

Executive Director, Finance

[Required notice if any Massachusetts resident's personal information is disclosed]

[Insert date]

Office of Attorney General
One Ashburton Place
Boston, MA 02108

Office of Consumer Affairs and Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116

Re: Unauthorized disclosure of personal information of Massachusetts residents

Dear Sir or Madam:

On _____, 20__, the personal information of approximately ___ Massachusetts residents was apparently disclosed to an unauthorized person when _____ . **[Describe the nature of the data breach, e.g., "a thief electronically penetrated one of COMPANY's servers and copied files that included customers' names and payment card information."]** COMPANY is planning to mail notices to all persons potentially affected by the unauthorized disclosure, including to Massachusetts residents. The notices will be substantially in the form of the letter and other documents enclosed. **[Enclose copy of draft notice letter and any "FAQs," credit monitoring offer, etc.]** We anticipate that these materials will be mailed over a period of __ days beginning _____ __, 20__.

In addition to sending the notices **[and credit monitoring offers, if they were sent]** to potentially affected individuals, COMPANY has taken **[or plans to take]** the following actions to respond to the incident: **[list each of the actions in general terms, e.g.,**

1. **Notified law enforcement of the breach;**
2. **Notified payment card entities and other payment processors of the breach;**
3. **Hired a forensic investigator to investigate how the breach occurred; and**
4. **Notified other public agencies of the breach, including _____ and _____.]**

If there is additional information about the incident that I may be able to provide to you to assist you regarding Massachusetts residents, please contact me.

Sincerely,

Executive Director, Finance

Enclosure[s]

[Required notice if any New Hampshire resident's personal information is disclosed]

[Insert date]

New Hampshire Attorney General's Office
Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Unauthorized disclosure of personal information of New York residents
Dear Sir or Madam:

On _____, 20__, the personal information of approximately ___ New Hampshire residents was apparently disclosed to an unauthorized person when _____ . **[Describe the nature of the data breach, e.g., "a thief electronically penetrated one of COMPANY's servers and copied files that included customers' names and payment card information."]** COMPANY is planning to mail notices to all persons potentially affected by the unauthorized disclosure, including to New Hampshire residents. We anticipate that the notices will be mailed over a period of __ days beginning _____ __, 20__.

Sincerely,

Executive Director, Finance

[Required notice if any New York resident's personal information is disclosed, with additional paragraph to use if more than 5,000 New York residents' personal information is disclosed]

[Insert date]

New York State Attorney General's Office
The Capitol
Albany, NY 12224-0341

New York State Consumer Protection Board
5 Empire State Plaza, Suite 2101
Albany, New York 12223

New York State Office of Cyber Security & Critical Infrastructure Coordination
30 S. Pearl Street
Albany, New York 12207-3425

Re: Unauthorized disclosure of personal information of New York residents

Dear Sir or Madam:

On _____, 20__, the personal information of approximately ___ New York residents was apparently disclosed to an unauthorized person when _____ . **[Describe the nature of the data breach, e.g., "a thief electronically penetrated one of COMPANY's servers and copied files that included customers' names and payment card information."]** COMPANY is planning to mail notices to all persons potentially affected by the unauthorized disclosure, including to New York residents. The notices will be substantially in the form of the letter and other documents enclosed. **[Enclose copy of draft notice letter and any "FAQs," credit monitoring offer, etc.]** We anticipate that these materials will be mailed over a period of __ days beginning _____ __, 20__.

[If more than 5,000 N.Y residents will be notified, include the following paragraph.] By the copy of this letter sent to the New York Attorney General's Office, COMPANY requests a copy of the list of consumer reporting agencies maintained by the Attorney General that must be notified of data breaches that may affect more than 5,000 New York residents. When we receive that list, we will notify the credit reporting agencies of the data breach.

Sincerely,

Executive Director, Finance

Enclosure[s]

[Required notice if more than 1000 North Carolina residents' personal information is disclosed]

[Insert date]

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001

Acxiom Corporation
6111 Oak Tree Blvd.
Cleveland, Ohio 44131

Chex Systems, Inc.
Attn: Consumer Relations
7805 Hudson Rd, Suite 100
Woodbury, MN 55125

ChoicePoint Credit Consumer Center
PO Box 105289
Atlanta, GA 30348

Equifax
P.O. Box 740256
Atlanta, GA 30374

Experian
P.O. Box 9595
Allen, TX 75013-9595

First Advantage SafeRent
Consumer Relations Department
7300 Westmore Rd., Suite 3
Rockville, MD 20850-5223

Innovis Consumer Assistance
P.O. Box 1358
Columbus, OH 43215
ISO Customer Service Division
545 Washington Boulevard
Jersey City, NJ 07310

LexisNexis Matthew Bender
1275 Broadway
Albany, NY 12204

MIB, Inc.
P.O. Box 105, Essex Station
Boston, MA 02112

TeleCheck Services
5251 Westheimer
Houston, TX 77056

TransUnion
P.O. Box 2000
Chester, PA 19022

UD Registry
P.O. Box 9140
Van Nuys, CA 91409

Re: Unauthorized disclosure of personal information of more than 1000 North Carolina residents

Dear Sir or Madam:

On _____, 20__, the personal information of approximately ___ North Carolina residents was apparently disclosed to an unauthorized person when _____ . **[Describe the nature of the data breach, e.g., "a thief electronically penetrated one of COMPANY's servers and copied files that included customers' names and payment card information."]** COMPANY is

planning to mail notices to all persons potentially affected by the unauthorized disclosure, including to North Carolina residents. The notices will be substantially in the form of the letter and other documents enclosed. **[Enclose copy of draft notice letter and any "FAQs," credit monitoring offer, etc.]** We anticipate that these materials will be mailed over a period of __ days beginning _____ __, 20__.

Sincerely,

Executive Director, Finance

Enclosure[s]

[Required notice if any Norwegian resident's personal information is disclosed]

[Insert date]

The Data Inspectorate
P.O. Box 8177
Dep, N-0034
Oslo, Norway

Re: Unauthorized disclosure of personal information of New York residents
Dear Sir or Madam:

On _____, 20__, the personal information of approximately ___ New Hampshire residents was apparently disclosed to an unauthorized person when _____ . **[Describe the nature of the data breach, e.g., "a thief electronically penetrated one of COMPANY's servers and copied files that included customers' names and payment card information."]** COMPANY is planning to mail notices to all persons potentially affected by the unauthorized disclosure, including to New Hampshire residents. We anticipate that the notices will be mailed over a period of __ days beginning _____ __, 20__.

Sincerely,

Executive Director, Finance