CYBER INSURANCE PROPOSAL FOR
ABC COMPANY

02/01/2022

JE Brown & ASSOCIATES

Powered by: SAYATA

WHAT'S IN THIS DOCUMENT

NEXT STEPS

1

CHOOSE COVERAGE

Select the option that best suits your coverage needs (see page 3).
Quotes must be bound prior to their expiration date.

2

OPEN THE APPLICATION

Click the "Review application" link below the coverage price.

3

COMPLETE, APPROVE AND SUBMIT

Complete and approve the application.
Get your policy faster by using the digital application.

*If you choose not to purchase coverage, please sign the Acknowledgement of Rejected Coverage form and return to your agent (see page 12).

CYBER COVERAGE OPTIONS FOR COMPANY ABC

Select your preferred option, and click "Review application." See footer below for more details.

COST AND COVERAGE MAY CHANGE BASED ON FINAL RESPONSES SUBMITTED IN THE APPLICATION.

		at bay	Coalition Admitted	HISCOX	Carrier name:
	VALID UNTIL	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	
	ADMISSION STATUS	Non-admitted	Admitted	Non-admitted	
	ISSUING INSURER	HSB Specialty Insurance Company	North American Specialty Insurance Company	Hiscox Insurance Company Inc.	
	AM BEST RATING Financial strength rating	A++ (Superior)	A++ (Superior)	A (Excellent)	
	AGGREGATE LIMIT Maximum amount paid by the insurance company for a claim	$1,000,000	$1,000,000	$1,000,000	$
	RETENTION The same as a deductible, the amount of a claim *you* pay	$1,000	$5,000	$1,000	$
FIRST PARTY COVERAGE	**NOTIFICATION COSTS** Cost to notify affected individuals after a data breach	$1,000,000	$1,000,000	$1,000,000	$
FIRST PARTY COVERAGE	**BREACH COSTS INSIDE/OUTSIDE** Will the breach costs erode the aggregate limit (inside) or are separate (outside)	Outside	Outside	Inside	
FIRST PARTY COVERAGE	**BUSINESS INTERRUPTION** Covers lost profits incurred due to not operating	$1,000,000	$1,000,000	$1,000,000	$
FIRST PARTY COVERAGE	**BI WAITING PERIOD** Minimum duration of business interruption before coverage starts	8 Hours	8 Hours	10 hours	
FIRST PARTY COVERAGE	**CONTINGENT BUSINESS INTERRUPTION** Losses from an interruption in a 3rd party computer services or software	$1,000,000	$1,000,000	$1,000,000	$
FIRST PARTY COVERAGE	**DATA RECOVERY** The cost of recovering lost data	$1,000,000	$1,000,000	$1,000,000	$
FIRST PARTY COVERAGE	**EXTORTION/RANSOMWARE** Covers damage and ransom payments from an attack	$1,000,000	$1,000,000	$1,000,000	$
FIRST PARTY COVERAGE	**BRICKING** When computers and electronic hardware are damaged beyond repair	$1,000,000	$1,000,000	$1,000,000	
THIRD PARTY COVERAGE	**NETWORK SECURITY AND PRIVACY LIABILITY** Third party liability costs	$1,000,000	$1,000,000	$1,000,000	$
THIRD PARTY COVERAGE	**PCI** Covers fines or penalties imposed by banks or credit card companies	$1,000,000	$1,000,000	$1,000,000	$
THIRD PARTY COVERAGE	**REGULATORY** In case you're fined by regulators (e.g., for breaching consumer privacy)	$1,000,000	$1,000,000	$1,000,000	$
THIRD PARTY COVERAGE	**MEDIA** When your content triggers legal action against you (e.g. - libel, plagiarism)	$1,000,000	$1,000,000	$1,000,000	$
CYBER CRIME	**COMPUTER FRAUD** Covers funds or property stolen resulting from a hack	$250,000 [1]	$100,000 [1]	$250,000 [1]	$
CYBER CRIME	**FUNDS TRANSFER FRAUD** When a criminal deceives a bank/institution to transfer funds	$250,000 [1]	$100,000 [1]	$250,000 [1]	$
CYBER CRIME	**SOCIAL ENGINEERING** When cyber criminals deceive a business to transfer funds willingly	$250,000 [1]	$100,000 [1]	$250,000 [1]	$
	TOTAL	(Approximate[2]) $[illegible] PREMIUM $[illegible] CARRIER FEE $[illegible] BROKER FEE $[illegible] PROCESSING FEE [3] $[illegible] + SL FEES & TAXES **TBD**	(Approximate[2]) $[illegible] PREMIUM $[illegible] CARRIER FEE $[illegible] BROKER FEE $[illegible] PROCESSING FEE [3] $[illegible]	(Approximate[2]) $[illegible] PREMIUM $[illegible] CARRIER FEE $[illegible] BROKER FEE $[illegible] PROCESSING FEE [3] $[illegible] SL FEES & TAXES $[illegible]	$ PREMIUM $ CARRIER FEE $ BROKER FEE $ PROCESSING FEE [3] $ SL FEES & TAXES $
		REVIEW APPLICATION *View Sample policy / Full quote*	REVIEW APPLICATION *View Sample policy / Full quote*	REVIEW APPLICATION *View Sample policy / Full quote*	* This quote was added manually by your broker.

1 Cyber crime ***retentions*** may vary. After confirming presumptions, check firm quote for full details.
2 All cost components are estimated. After the application is completed and signed you will receive a firm quote from the carrier. Costs may change based on final application responses.
3 Processing Fee is a client-related expense for processing quotes.
* Please review final quotes for the most accurate information, as comparison data above is a simplified view and may contain inaccuracies. Retentions may vary by coverage part.

FAQ

WHAT IS CYBER INSURANCE?

When a breach occurs, cyber insurance covers the range of expenses that arise. These include identifying and solving the breach, recovering data, customer notifications, PR costs, possible credit monitoring expenses, legal expenses, potential fines from compliance regulators, extortion costs from ransomware, and general business interruption.

DO HACKERS REALLY BOTHER WITH ATTACKING SMALL BUSINESSES?

Yes. Hackers use technology to scan the internet for businesses with weak defenses regardless of the size of the business.
A recent Verizon report notes that 43% of all cyber attacks are against small businesses. Worse, 63% of small businesses had experienced a breach in the last 12 months. Any business with a computer and an internet connection is at risk - even if you don't sell anything on your website.

WHAT'S COVERED?

First-party coverage - Covers damages a business suffers because of a cyber breach. This can include things like investigative services, business interruption coverage and data recovery.

Third-party coverage - Covers damages if a business' customers or partners are affected by a cyber attack. This can include legal fees, settlement costs, security failures and media liabilities.

Cyber crime - Covers damage due to any type of illegal activity that occurs using digital means. Examples of cybercrime are extortion/ ransomware, phishing, social engineering, and wire transfer fraud.

DOESN'T MY CURRENT BUSINESS INSURANCE INCLUDE CYBER ATTACKS?

Many general business policies only partially cover damage from cyber events, *if at all*. As mentioned above cyber coverage protects against the vast array of possible damages, expenses, and lost business that can occur from a cyber attack.

WHAT SHOULD I CONSIDER WHEN CHOOSING BETWEEN PURCHASING A STAND-ALONE CYBER POLICY VS. ADDING AN ENDORSEMENT TO AN EXISTING POLICY?

To be fully protected, ensure you have all coverages – first-party, third-party, and cyber crime. Further, since some cyber events can result in large expenses, confirm you have adequate sublimits for each of three above coverages.

WHY DO I NEED A "BREACH COACH"?

If your company gets hacked, you will need a breach coach to get your business back up and running fast. When a breach occurs, you need to assess and contain the damage, notify affected parties (e.g. customers and vendors), evaluate and act on the legal ramifications from agitated customers to regulatory bodies, and more. A breach coach will quickly assemble the right response team to deal with these issues. Without an expert it all falls on you, costing you time and money while adversely affecting your business. Fortunately, most insurance companies now provide a breach coach as part of a greater suite of services when you purchase stand-alone cyber insurance coverage.

DO SMALL BUSINESSES NEED CYBER INSURANCE IF THEY PRACTICE GOOD CYBER HYGIENE?

Being properly protected definitely helps. However, there is no way to fully protect against new threats or human error. Hackers are always adapting to overcome cyber defenses with new versions of current threats or creating brand new methods of attacking businesses. However damaging a new threat can be, the single biggest contributor to a breach is human error. Easy-to-hack passwords, phishing emails, or even a lost laptop all present potential entry points for a cyber criminal. Finally, a third-party vendor could be attacked impacting your ability to do business. A thorough cyber insurance policy is part of your overall risk management plan to ensure your business runs smoothly.

* All of the above are general terms which may vary based on context. Please consult the policy form or ask an agent/broker for precise definitions and details.

CLAIM SCENARIO

RANSOMWARE | Retail Trade

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

An employee of a music instrument retailer accidentally clicked on a malware link. The virus was downloaded onto the company server causing all data to be encrypted. The employee then received an email demanding $50,000 paid in Bitcoin within 48 hours to release their data files.

2,000 customer records including name, address, phone, and credit card information were encrypted. The retailer called their insurance company's cyber response team, who responded by assigning a "breach coach," which is covered as part of the retailer's stand-alone cyber policy.

The breach coach sent in a forensics team to assess the situation, including any computer or electronic hardware damage, and determine if paying the ransom was necessary. Concurrently, the insurance company confirmed coverage and assisted with opening a claim to minimize the effect of business interruption.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Incident response manager ("breach coach") fees	**$ 5,500**
Forensic investigation costs to locate malware, analyze damage, ensure containment and calculate loss	**$ 6,860**
Legal fees	**$ 4,000**
NOTIFICATION COSTS	**$ 1,230**
BUSINESS INTERRUPTION	**$ 31,325**
DATA RECOVERY Costs associated with replacing lost or corrupted data	**$ 10,100**
EXTORTION/RANSOMWARE Ransom payment	**$ 50,000**
BRICKING Damage to computer and hardware systems	**$ 12,050**
TOTAL	**$ 121,065**

RESOLUTION

While the business maintained regular back-ups online, the hackers also encrypted these files leaving the retailer no way to restore the data. The insurance company and breach coach agreed the fastest, best way to get the business back up and running was to pay the ransom.

The insurance company immediately paid the ransom via their pre-established Bitcoin account, releasing the records back to the retailer.

The swift assessment and payment, minimized the business interruption allowing the retailer to resume operations.

CLAIM SCENARIO

OUTDATED SOFTWARE | Educational Services

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

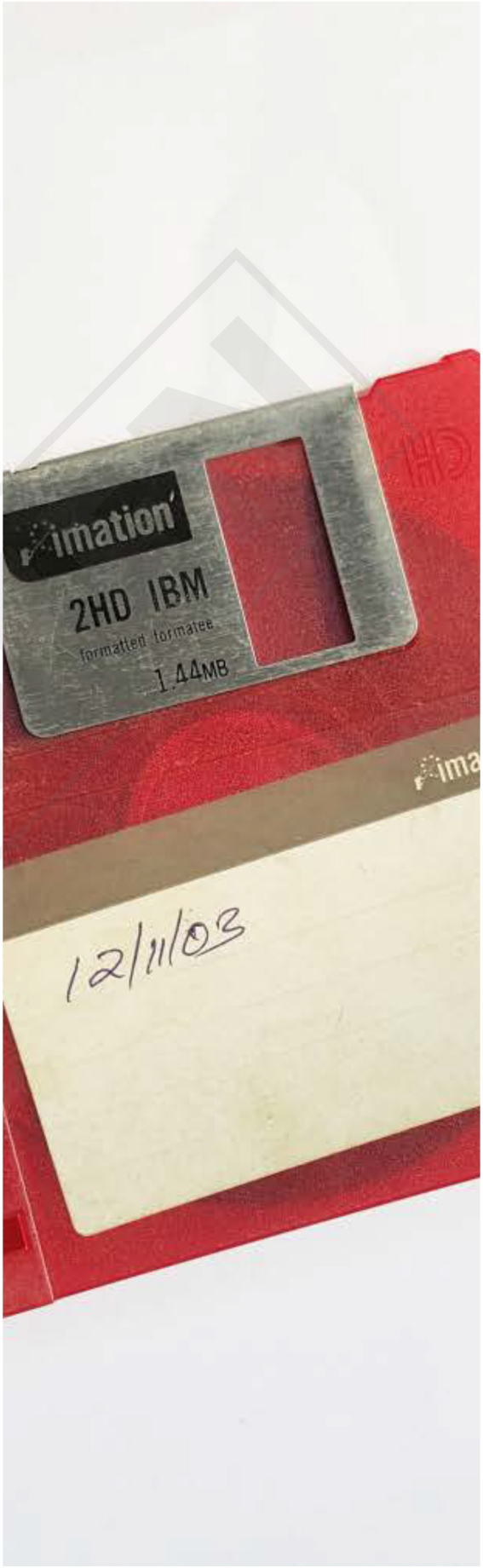
Hackers penetrated a graphic design school's network from a vulnerability in an outdated software application. 4,000 student names, addresses, emails, bank details and school records were compromised.

Local authorities received multiple complaints of suspicious activity, leading the school's IT department to discover an unauthorized user had accessed the system.

Once discovered, the school called their insurance carrier who immediately brought in forensic experts to initiate the school's IT recovery plan and notification program.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to isolate vulnerability, analyze damage, ensure containment and calculate loss	$ 11,850
Identity theft and credit monitoring services	$ 11,500
Incident response fees	$ 7,850
Public relations fees to minimize reputational impact	$ 10,050
Call center set up and operation to field inquiries	$ 10,200
NOTIFICATION COSTS	$ 1,865
DATA RECOVERY Costs associated with replacing lost or corrupted data	$ 14,850
REGULATORY	
Legal expenses arising from regulatory investigation due to mismanagement of private information	$ 22,175
Legal expenses and settlement costs for claims	$ 16,100
Business interruption	$ 39,318
TOTAL	**$ 145,758**



RESOLUTION

The school's cyber policy was triggered, giving them immediate access to response services. The insurance company dispatched a forensic team who quickly isolated the unauthorized user.

A claim was started immediately to help with impending legal, consulting and media costs. The insurance company, IT team and forensic consultants ensured the school had up-to-date cyber defenses including firewalls, intrusion detection software, and encrypted databases. Concurrently, officials worked with local media to notify affected students and offer credit monitoring services, while the legal team handled the backlash from those affected.

Finally, the forensic consultants helped develop a new plan that included regular updates, testing, and education of all staff to minimize future breaches.

CLAIM SCENARIO

SOCIAL ENGINEERING | Finance and Insurance

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

A mortgage broker's emails were accessed by an attacker who, posing as the General Manager, asked an employee to contact the broker's bank with instructions for funds to be transferred into the hacker's bank account.

When the mortgage broker discovered that unauthorized payments were made totaling $425,000, they immediately contacted their bank to freeze the funds and notified their cyber insurance carrier. Together, they were able to recover $354,000 of the unauthorized transactions.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to locate the breach, analyze damage, and ensure containment	**$ 13,500**
Legal fees	**$ 9,500**
FUNDS TRANSFER FRAUD Transferred funds not recovered	**$ 71,000**
TOTAL	**$ 94,000**

RESOLUTION

The mortgage broker has a stand-alone cyber policy that covers social engineering as well as provides crucial response services. Once the broker notified their insurance company, an IT forensic consultant was appointed to assist the broker in repairing the damage to their system as well as to prevent future attacks.

As the mortgage broker has expanded cyber crime coverage under their policy, they were reimbursed for the direct financial loss, less the deductible, of the unrecovered fraudulent transfers as well as their forensic and legal costs.

CLAIM SCENARIO

LOST HARDWARE | Health Care and Social Assistance

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

An employee of a medical group lost their laptop. An Excel file on the computer contained medical records of 1,500 patients including the names, addresses, dates-of-birth, medical record numbers, medications, and diagnoses.

Once the loss was realized, the medical group immediately notified their insurance company who provided a "breach coach" to assess the damage and help the insured comply with regulatory and notification requirements.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic costs to assess and contain damage	$ 8,000
Legal fees	$ 15,500
Public relations fees to minimize reputational impact	$ 10,000
NOTIFICATION COSTS	$ 1,250
DATA RECOVERY Costs associated with replacing lost or corrupted data	$ 9,550
REGULATORY Settlement fine	$ 25,000
Patient liability settlements	$ 52,200
TOTAL	**$ 121,500**

RESOLUTION

The breach coach assigned a forensics team, provided by the insurance company, to determine the potential exposure of the protected health information (PHI). It was determined that the patient PHI was, in fact, compromised. The patients were immediately notified and offered credit monitoring services.

Concurrently, the breach coach engaged a public relations agency to minimize the reputational damage as well as alerted counsel to help settle legal action from patients.

They were proactive in contacting the Department of Health and Human Service Office for Civil Rights and agreed upon a settlement amount as well as a corrective action plan that included employee cyber and data protection training.

CLAIM SCENARIO

FORMER OR ROGUE EMPLOYEE | **Arts, Entertainment, and Recreation**

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

A museum was hacked by a former employee, whose user credentials were not deleted when they were terminated. The employee sold 1,115 donor records on the dark web including name, address, email, and credit card number including expiry dates.

The museum notified their insurance company immediately. The carrier provided forensic expertise, legal services, and media relations help to investigate and control the damage.

In addition, the insurance company enlisted a "breach coach" to guide the museum in managing their actual and reputational damage.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to analyze damage and ensure containment	**$ 7,600**
Identity theft and credit monitoring services	**$ 5,620**
Legal fees	**$ 9,935**
Public relations fees to minimize reputational impact	**$ 8,380**
Call center set up and operation to field inquiries	**$ 5,700**
NOTIFICATION COSTS	**$ 1,025**
DATA RECOVERY Costs associated with replacing lost or corrupted data	**$ 8,450**
TOTAL	**$ 46,710**

RESOLUTION

The forensic team quickly identified the breach and worked with the museum's IT department to initiate repairs. The breach coach guided the museum to hire a call center to quickly inform affected donors, field questions, and offer identity protection and credit monitoring services to ensure trust going forward. The insurance company recommended seeking legal counsel to pursue civil action against the former employee.

Concurrently, the museum, in tandem with the media relations team, responded quickly and transparently to the media.
Finally, the insurance company and forensic team recommended an updated cyber response plan that included more rigorous IT policies and procedures as well as several technological updates to improve cyber hygiene. Due to the fast response, the costs and reputational damage to the museum were minimized.

CYBER INSURANCE GLOSSARY

BUSINESS INTERRUPTION
Cyber business interruption covers the net profit earned before taxes that would have been earned had there been no interruption due to a cyber event.

BI (BUSINESS INTERRUPTION) WAITING PERIOD
A predetermined amount of time that must elapse before any loss or expenses may be payable under the business interruption coverage.

BRICKING COVERAGE
Covers the cost to replace computer and electronic hardware that's rendered inoperable due to failed software, firmware update or purposeful attacks.

COMPUTER FRAUD
Insures against theft of funds or property specifically stolen by using cyber methods to transfer money or property from the insured.

CONTINGENT BUSINESS INTERRUPTION
A contingent business interruption loss occurs as result of a third-party supplier, service provider or distributor shutdown whose interruption, due to a cyber incident, directly impacts the insured's ability to produce a product or provide a service.

CYBER CRIME
Any type of illegal activity that occurs using digital means. Examples of cybercrime are extortion/ransomware, phishing, social engineering, and wire transfer fraud.

DATA RECOVERY
Covers the costs of recovering lost data due to a breach.

DATA RESTORATION
The process of copying backup data from secondary storage and restoring it to its original or a new location. Data restoration is done to return data that has been lost, stolen or damaged.

EXTORTION/RANSOMWARE COVERAGE
Coverage for the damage done to a business due to a cyber breach or attack including possible ransom payments to release key systems and data.

FIRST PARTY CLAIM
A claim triggered by a cyber breach or other qualifying event where coverage immediately responds to losses directly to the insured.

FUNDS TRANSFER FRAUD
Covers the loss stemming from unauthorized instructions from a third party to a bank without the insured's knowledge.

MEDIA (LIABILITY)
Provides coverage against media-related damage such as libel, privacy invasion, copyright infringement, and plagiarism stemming from the policy holder's media activities (e.g website content, printed articles).

NOTIFICATION COSTS
Covers the cost of notifying affected individuals in the event of a data breach. Customer notification is often required by law.

PCI (PAYMENT CARD INDUSTRY)
Coverage for assessments, fines or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS).

PRIVACY REGULATORY LIABILITY (REGULATORY)
Covers losses that arise out of an organization's failure to protect sensitive, personal or corporate information in any format.

SOCIAL ENGINEERING COVERAGE
Covers unintended payments made to cybercriminals who, through deception, convinced an employee or officer of a company to transfer funds to the criminal.

THIRD PARTY CLAIM/LIABILITY CLAIM
When a third party files a claim or lawsuit against the insured alleging that the insured caused some damage to the claimant due to a cyber event.

* All of the above are general terms which may vary based on context. Please consult the policy form or ask an agent/broker for precise definitions and details.

CYBERSECURITY GLOSSARY

DDOS (DISTRIBUTED DENIAL OF SERVICE) ATTACK
A DDoS attack is a malicious attempt to disrupt or shut down normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

MALWARE (MALICIOUS SOFTWARE)
Any code written for the specific purpose of causing harm, disclosing information or otherwise violating the security or stability of a system.

PATCH
An update or change to an operating system or application. A patch is often used to repair flaws or bugs in deployed code as well as introduce new features and capabilities.

PENETRATION TESTING (PENTESTING)
A security test where security experts mimic hackers to expose weaknesses.

PHISHING
A social engineering attack that attempts to collect information from victims. Phishing attacks can take place over e-mail, text messages, through social networks or via smartphone apps.

TWO-FACTOR/MULTI-FACTOR AUTHENTICATION
The means of proving identity using two or more ways to identify the user. It is usually considered stronger than any single factor authentication.

VULNERABILITY
Any weakness in an asset or security protection which would allow for a threat to cause harm.

REGULATORY GLOSSARY

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)
CCPA is broad-reaching legislation designed to protect the privacy rights and collected information of California residents including data held by companies outside of California.

GENERAL DATA PROTECTION REGULATION (GDPR)
GDPR is a European Union (EU) legal code, requiring all businesses, regardless of location, to protect the privacy and personal data collected about EU citizens, including the right of complete data removal.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)
HIPAA is a federal law that provides privacy standards to protect patient medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI-DSS)
Widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. The PCI-DSS was created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express.

RED FLAGS RULE
A federal regulation that requires financial institutions and creditors to develop and implement documented plans to protect consumers from identity theft.

* All of the above are general terms which may vary based on context. Please consult the policy form or ask an agent/broker for precise definitions and details.

ACKNOWLEDGMENT OF REJECTED COVERAGE

This page should only be signed if the applicant decided not to purchase the insurance coverage mentioned below.

I understand and acknowledge that the following insurance policies have been offered to me and that I have decided not to purchase the coverage at this time:

CYBER LIABILITY INSURANCE

The potential financial impact of not having these important coverages has been explained to me and I realize that my rejection of these options may result in the denial of claims in the future.

Signed: _____

Company: [Company name] _____

Date: _____