What to Know about Security and Privacy and the Policies that Insure it

Can insurers make a profit without Gotch’ya’s,
and ...
can distributors discern the indiscernible?
Massachusetts Financial Services Insurance Agency has worked with experts in their fields to present various insurance related topics. The instructors are the sole authors of the materials. Insurance forms and endorsements referred to vary based on insurance company; regulations; court decisions; and state jurisdiction. This instructional material is intended as a general guideline. Any interpretations provided by the presenters do not modify or revise insurance policy language.

Finally, the opinions expressed in this presentation is solely the opinions of the Authors(s)
Who is at risk of a Loss?

Anyone who collects personal or other sensitive data is at risk. You could be at risk if your files or databases contain any of the following information of third parties or even employees:

- Personal identification information, SSN’s, email or street addresses and phone numbers.
- Credit information, like credit card numbers or billing information or credit reports.
- Financial records, including investments and bank information for payroll direct deposits.
- Online access information, like user names and/or passwords.
- Health records and health insurance information of students or program participants.
- Information governed by non-disclosure agreements.
- Directors and officers ignore cyber risks at their own peril.
What is cyber insurance?

Cyber insurance is coverage for a broad range of scenarios in which sensitive stored information might be damaged or lost including a mix of 1st and 3rd Party coverages.

The loss of data property, ideas, confidential corporate information or its inappropriate publication can interrupt your business or cost you time and money. There are legal consequences for losing third party information, plus federal law and/or laws in 47 states, Puerto Rico, and the US Virgin Islands require you to notify those owners of the loss within certain time frames.

Unfortunately, traditional insurance doesn’t normally cover intangible data or intellectual property.
What Types of Coverage Exist?

Cyber Liability is a generic term for an insurance policy that includes one or more of the following coverages:

**Network Security coverage** – Coverage against allegations/claims made by third parties that were economically harmed by a breach in the insured’s network. It also covers identity theft and private information that is made public.

**Privacy coverage** – Extends network security coverage to paper files, Notification Costs, Credit Monitoring

**Digital Media coverage** – Coverage for content injury claims such as misuse or unauthorized use of copyrighted material.

* 1st & 3rd party mix
* GL/ Mgt Liab / Property / Crime / & Professional Liability- Some overlap does exist Cyber is the Hub for the spokes- fills in gaps Retro date issues- Date of Discovery
Typical AND MYTHICAL Coverage Items

Comprehensive media liability, including coverage for user generated content with Advertising and Personal Injury
Defamation, including libel and slander
Intellectual property rights infringement
Invasion of privacy
Blanket professional liability, Fiduciary Liability Coverage
Breach of contract Liability
Cyber liability, privacy liability and privacy breach notification costs, Virus Coverage, Reputational Coverage & Notification Costs Property and business interruption, including cyber perils
Common Cyber Risks

If you have a website, a third party may allege that you have published their copyrighted material.

If you are a financial institution or deal with patient records, you could have significant defense costs associated with an administrative action under GLB or HIPAA regulations.

If you sell internet access services to a third party and they allege they were denied access.

If you sell software to a third party that alleges damages as a result of software malfunction.
Common Cyber Risks

The most common threats are as follows:

Activities by a hacker to a third party whom alleges damages, including:

a. Accesses your computer to send a virus.
b. Accesses your computer system to release sensitive customer data.
c. Launches an attack that shuts down your computer system.
d. Accesses your network and launches an attack.
e. Accesses your network and transfers money or credit card information you are holding.
More Common Cyber Risks

Activities by a hacker to first party whom alleges damages, including:

a. Deletes data or alters your data and you incur costs to reproduce the data and lost income.
b. Sends a virus to your system and you suffer damages to data and lost income.
c. Gains access to your network and causes an electronic transfer of your funds to his/her account.
d. Extorts money by threatening to divulge sensitive data he/she collected over your network.
e. Changes all of your passwords and locks you out of your network.
f. Launches a Denial of Service (DOS) attack which makes it impossible to sell products over your website.
What Liability Exists?

* **Digital Asset Coverage** – Coverage for the loss of data and/or network resources.

* **Digital Business income coverage** – Covers the loss of income due to a network intrusion and/or other computer event that makes the network inaccessible or operates slowly.

* **Technology Errors & Omission** (Tech E&O), also known as Errors and Omissions Liability coverage, is coverage specifically designed for technology companies.

* Any individual or firm that provides technology services or products should consider obtaining Tech E&O coverage. A Tech E&O policy protects your firm by providing defense cost and covering potential settlements from any alleged or actual errors.
What’s happening out there

Corporate security breach is on the rise. The number of companies hit by an unauthorized access (hacking/cracking) isn’t even known. And only 1% of Corporate Boards have a Member that is technically proficient. e-Business activities make you a bigger target. Companies conducting business online are 57% more likely to experience a proprietary information leak and 24% more likely to experience a hacking-related breach.

New internet exposures threaten your network. Hackers/crackers (21%), malicious code (17%), email (15%) and secure remote access (14%) are claimed to be the greatest source of concern. A reported 77% of respondents had suffered losses from virus attack.

Companies are not ready for secure e-business as 52% of the respondents claimed their company’s state of information security is average or below. As well, 35% claimed that security doesn’t have high visibility. e-Business losses are more than financial. Of the respondents who admit suffering a security breach, there were significant interruptions to business operations and additional loss of reputation along with the financial loss.
What’s New in a New in a Young Industry

* E-TAILERS WITHOUT TECHNOLOGY INSURANCE TREAD DANGEROUS GROUND -
* In the last decade, e-commerce has gone from being almost nonexistent to completely mainstream, with what seems to be an infinite number of cyber retail web sites. Prior to the Internet, it was rare that retailers and consumers using paper catalogs would fall victim to marketing-by-mail fraud. [CYBER THREAT FROM WORKPLACE SOCIAL NETWORKING REAL, BUT MAY BE OVERHYPED]

* In just the last few years, social media has fundamentally affected the way many of us communicate. And statistics aren’t needed to prove it. If you’re under 40, chances are good that you have a Facebook, Twitter, and/or Linkedin account.

* DOCTORS AND HOSPITALS VICTIMS OF RECORDS THEFT - 29
* Digital records kept by medical providers contain highly sensitive data, such as test results, diagnoses, and financial information. And chances are very good that somewhere there is medical data server holding information about you. So, it’s easy to see why the all-too-frequent security breaches in hospitals and doctors offices are quite disturbing

FCC

Fisher Consulting Group, Inc.
Claim Causes

Many times companies wonder, “What goes wrong when losses are incurred?” Although many of the losses seem to be theoretical, they are very real issues that have occurred to many companies. Only by understanding that losses do occur and how to prevent them, can your company develop a viable cyber risk management program. Some examples of losses include:

- Firewall providers – breach of security due to malfunction in the software
- Software providers – Damages that are caused due to software malfunction
- Website Owners – Misuse of copyrighted material
- A virus is sent to your network causing third party damages.
- Network Owners – hacker actions that cause loss of funds and negatively affects both systems usage and reputation.
- Custodians of Confidential Data – Civil action due to unauthorized release of data protected by privacy laws.
- A customer initiates a suit because a computer consultant is alleged to have provided faulty advice which leads to a failed installation. Hacker steals your funds.
- Hackers send a virus which causes lost income and/or damage to data.
- Hacker extorts money by threatening release of confidential data.
- Hacker launches a “Denial of Service” attack to prevent usage of your website and/or damage to your website data.
- Hacker or disgruntled employee changes all passwords locking you out of the network
Laws are Everywhere

Health privacy laws
Financial privacy laws
Online privacy laws
Communication privacy laws

**Protection of nonpublic personal information.**

(a) Privacy obligation policy.
(b) Financial institutions safeguards.

**Obligations with respect to disclosures of personal information.**

(a) Notice requirements.
(b) Opt out.
(c) Limits on reuse of information.
(d) Limitations on the sharing of account number information for marketing purposes.
and the actual Statutes

Health Insurance Portability and Accountability Act -- Office for Civil Rights
U.S. Department of Health and Human Services

Financial Services Modernization Act (GLB), 15 U.S. Code §§ 6801-6810
Gramm-Leach-Bliley Act

Final Rule on Privacy of Consumer Financial Information, 16 Code of Federal Regulations, Part 313
Fair Credit Reporting Act (FCRA), 15 U.S. Code §§ 1681-1681u

List of Privacy Laws
[Privacy Act of 1974 (US)
Electronic Communications Privacy Act (US)
Privacy Act 1988 (Aus)
Data Protection Directive (EU)
Data Protection Act 1998 (UK)
Personality rights

Data protection (privacy) laws in Russia
Any good cyber insurance policy begins with third party and first party coverage called Network Security and Privacy coverage. It also can cover the following:

- Data stored on laptops and other portables
- Notification costs and regulatory defense
- Information stored on the cloud
- Information stored both offline and online
- Advertising and other content
- Business Interruption and data restoration
- Crisis management and PR costs
- Cyber extortion
- Rogue employees
- Breach of non-disclosure agreements
Products and Services

• Begin with the Assumption that the “product” sold to a Policy holder is how it responds when a claim is submitted

• Assume that Actuaries, in setting pricing, use historical data and other research, but may miss one important additional factor

• Finally, does the product meet “reasonable” expectations
Making a Profit

* Uncertainty increases costs and expenses
* Uncertainty increases unnecessary litigation
* Uncertainty can turn one claim against the Insured into 4 lawsuits
* Uncertainty resulting from the above can doom a program to failure as the above is actuarially unsustainable.
So- What are some “Gotcha’ya’s”?

* A Claims made Trigger “Gotch’ya”:

* “IT IS AGREED that the **Insurer** is not obligated to pay **Damages or Claim Expenses** or defend any **Claims** based upon or arising out of, either directly or indirectly from any legal actions, arbitration or other adjudicative proceeding instituted and pending prior to the Effective Date of this Policy, whether or not any **Insured was named as a party in such legal action, arbitration, or other adjudicative, proceeding prior to the Effective Date of this Policy.”

---

FCC

Fisher Consulting Group, Inc.
Circle Back to Gotchya’s Coverage issues to Look for

- Claims Made Triggers
- Extended reporting Periods
- A mix of Claims Made Coverages with Occurrence language
- Absolute Exclusions

* **Virus Coverage** - Extensions for Contractors – vendors – hosts Virus in the wild - not specific - Indiscriminate types - avoid “other Ins provisions” **Privacy Coverage issues** - Avoid Sub limits for Rg action, Need worldwide coverage, NO contract Liability Exclusions as almost all obligations are contractual, AVOID HARD CODED DEFINITIONS OF PII (personal Identifiable Information) OR SENSITIVE DATA – Include cover for fines - penalties (where insurable) Coverage trigger- Security Breach

* **Breach Notification** - the expensive part of the Cover - Losing a blackberry can trigger it Voluntary Notification beyond required

* Separate limits for breach notification/ 24/7 Claims response/ Coverage for credit monitoring - Forensic consultants – call center Type of breach = paper/ electronic / fault/ no fault

* **Multi Media Liability** - Not in every form Social Media - no prior review—Ensure no restricted Website/ email—Cover for social media and corporate blogging digital content regardless of distribution channel- seek cover for all risks except patent/trade secrets—far beyond media liability - **System damage**

* All risk – not named perils/ Avoid Breach Trigger /Include staff overtime for working to fix No exclusion for lack of Risk management/Cover perils at outsourced or cloud services **System Business Interruption**

* Financial retention v time retention / Scope of perils covered / Cover outsourced or cloud providers/ at least 90 day Indemnity period / Contingent loss of future sales (reputational loss) Indemnity Period – 3 mos - Contingent period- 1 year **Cyber Crime** Employee rime OR 3rd party Crime/ Cover for threats - extortion/ 3rd party theft of Electronic funds/ telephone hacking- VOIP line stealing/ Phishing scams

* **Other Key issues**

* Retro dates and cover for prior acts/ Pay on behalf v re-imbursement / TRA/ Encryption warranties risk management conditions
One good Example of an Exclusion

“based upon, arising out of, or in any way involving or resulting from, either directly or indirectly, any mechanical or electrical failure, interruption or outage, however caused, including any electrical power interruption or surge, brownout, blackout, short circuit, over voltage, or power fluctuation or outage to gas, water, telephone, wireless communications, data transmission lines, cable, satellite, telecommunications, the internet or any component thereof including hardware, Software or any other infrastructure, services, equipment or facilities; provided, however, this exclusion shall not apply to any failure, interruption, or outage of telephone, cable or telecommunications under the Insured’s direct control which is the result of an Insured’s Wrongful Act or a Denial of Service Attack directed against the Company’s Computer Systems”
Another Trigger Gotch’ya

* “This Liability Coverage shall not apply to, and the Company shall have no duty to defend or to pay, advance or reimburse Defense Expenses for, any Claim:

* 5. based upon, alleging, arising out of, or in any way relating to, directly or indirectly, any fact, circumstance, situation, transaction, event or 'Wrongful Act underlying or alleged in any prior or pending civil, criminal, administrative or regulatory proceeding, including audits initiated by the Office of Federal Contract Compliance Programs, as of or prior to the applicable Prior and Pending Proceeding Date set forth in ITEM 5 of the Declarations for this Liability Coverage;.”
Claim Reporting Gotch’ya’s”

* What if the definition of Claim is:
  * ”A written demand…” or “a lawsuit “ or the Commencement of any Administrative Proceeding” ??? …and the policy is claims made & Reported?

* What about Automatic Limited ERP’s, an expected feature of such a form:
  * Or... “Claim reporting:

* Any Insured shall, as a condition precedent to exercising their rights under any Liability Coverage Section, give to the Company written notice as soon as practicable of any Claim, but in no event later than the earliest of the following dates:

  * (i) (thirty to) ninety (30-90) days after the date on which any Insured Organization’s chief executive officer, chief financial officer, in-house general counsel, risk manager, director of human resources, or any equivalent thereof, first becomes aware that the Claim has been made;”

* So its not really a claims made and reporting during the policy term at all- Huh?

* So- who do you think will ultimately be responsible?

FCC

Fisher Consulting Group, Inc.
Which proves the original Point

* Uncertainty increases costs and expenses
* Uncertainty increases unnecessary litigation
* Uncertainty can turn one claim against the Insured into 4 lawsuits
* Uncertainty resulting from the above can doom a program to failure as the above is actuarially unsustainable
Thank You all!

Frederick J. Fisher, J.D. is currently President of Fisher Consulting Group, Inc. and was the Founder of E.L.M. Insurance Brokers, a Wholesale & MGA facility specializing in Professional Liability and Specialty Line risks. He is a Member of the Editorial Board for Agents of America; a Faculty Member of the Claims College, and Member of the Executive Council, School of Professional Lines sponsored by the Claims & Litigation Management Association and a course designer and webinar Instructor for the Academy of Insurance (sponsored by the Insurance Journal).

* Since his career began, Mr. Fisher focused on one vision: providing financial security to the client. The result was a successful 40 year career in Specialty Lines Insurance. In 1975, Mr. Fisher began his career on the service side, as an Independent E&O claims adjuster. In 1982, he bought the Company, continued with claims, while expanding the firm’s services to include qualitative claim auditing, risk management & loss control services, and acting as a TPA. In only 4 years, the annual billings increased by 400%. His claim auditing techniques and recommendations resulted in substantial client savings (including the SCRTD now known as the Los Angles MTA). Many Insurers and self-insured’s adopted not only the performance standards raised in the audits, but adopted his recommended Attorney Management Guidelines as a base, which are still in use today by many major insurers.

* In 1995, he formed what is now known as ELM insurance Brokers, a firm that has acted as an MGA and Wholesale Broker of Professional Liability Insurance and Specialty Lines. From nothing, the firm grew rapidly to a $30 Million dollar facility when sold in 2008. He has lectured extensively on professional liability issues since 1978, and authored over 64 articles in trade journals and periodicals. He is the author of BROKER BEWARE, Selling Real Estate within the Law. He designed a program to conduct on site pre-underwriting risk management assessments of a clients' professional liability exposures. In 1989, he became a Founding Member of the Professional Liability Underwriting Society (PLUS), and was elected to the PLUS Board of Trustees in 1993. After serving in all Officer capacities, he was elected President in 1997. He remains a Special Materials Expert for several RPLU courses and is the Senior Technical Advisor for The Professional Liability Manual, first published by the International Risk Management Institute in 1990. He has taught over 100 CE classes and lectures. He testifies regularly as an expert witness in cases dealing with the duties and obligations of professionals as well as on coverage and claims-made issues.

* Mr. Fisher can be reached at 310/426-2105, Cell 310/413-6200, or email-fjjfisher@fishercg.com

Fisher Consulting Group, Inc.
BANK CARD FRAUD PROTECTION

Massachusetts Financial Services Insurance Agency, Inc.
And
Tom Mulligan, Frates Insurance & Risk Management

January 2015
TOPICS

Bank Card Fraud
How the system works
The Impact of fraud on your business
What is Bank Card Fraud?
BANK CARD FRAUD

- Lost/Stolen Cards
- Friendly Fraud
- Account Testing
- Identity Theft
- Theft From The Mail
- Fraudulent Applications
- Data Compromise
- ATM Scams
- Internet MO/TO
- Account Takeover
- Phishing
- Counterfeit
HOW THE SYSTEM WORKS

Understanding
Bank Card
Fraud
AUTHORIZATION SYSTEM
CLEARING & SETTLEMENT
THE IMPACT OF FRAUD

Industry Trends
INDUSTRY FRAUD TRENDS

Credit card and debit card fraud resulted in losses amounting to $11.27 billion during 2012.

During 2012 credit card and debit card gross fraud losses accounted for roughly 5.22¢ per $100 in total volume, up from 5.07¢ per $100 in 2011.

Financial institutions incurred $955 million in losses due to debit card fraud in 2010 – a 21% increase from the $788 million in losses incurred during 2009.

67% more Americans were impacted by Bank Card Breaches in 2012 than in 2011. (Source: Nilson Report, August 2013)
SCOPE OF THE BUSINESS
LATEST THREATS TO THE SYSTEM

- Account Information Theft
  - (Cyber-Crime – Compromised Data)
- Skimming/Counterfeit
- Fraudulent Applications and Identity Theft
- Failure by an Institution to utilize all the available tools to prevent and control fraud
BASIC FRAUD SERVICES

Does your Processor (s) offer the following fraud reduction services for all your card programs?

- Credit
- Debit
- ATM
BASIC FRAUD SERVICES

- CVV/CVC for all cards & transactions
- Falcon/Advanced Authorization
  - (Restrict accounts 7X24)
- AVS – Address Verification Service
- Letters confirming Address Change
- Card Activation
- Chargeback and Compliance Recoveries
- MIS to track effectiveness
- Expiration Date Mismatch
- Do you utilize all of them?
- Rippleshot Breach Detection Service
UNDERSTAND FRAUD

Maintain Effective MIS:

“Know today what happened yesterday
So you can take action to
Prevent or Detect it tomorrow”
UNDERSTAND FRAUD

Fraud loss MIS should track fraud cases by:
- Fraud type (Lost, Stolen, Counterfeit, etc.)
- General location of activity
- Amount of loss on a case & Amount of recovery,
- Customer ID
- Date of report, date of first and last fraud transaction,
- Detected by fraud detection system or reported by account holder
- Date account opened.
- PIN or Signature
UNDERSTAND FRAUD

You can use this information to
- Analyze your losses
- Understand how to control fraud losses.
MONITORING FRAUD

“Neural network”
- Is the #1 fraud control tool
- Screens transactions and compares them to known fraud patterns and account normal spending patterns
- System identifies suspicious transactions
- Refers them to analyst who decides action to be taken
MONITORING FRAUD

System must operate 7 X 24
Must restrict the account even if unable to contact cardholder
- Very few cardholders are impacted
- .3 of 1% of accounts score 760 or greater
- .06 of 1% receive authorization declines or referrals
# The Magnetic Stripe

## Track 1

<table>
<thead>
<tr>
<th>SS</th>
<th>FC</th>
<th>Primary Account No. (19 digits max)</th>
<th>Name (26 alphanumeric characters max)</th>
<th>Additional Data</th>
</tr>
</thead>
</table>

**Notes:**
- Track 1 is limited to 79 characters including Start Sentinel, End Sentinel, and LRC
- SS: Start Sentinel, FS: Field Separator, LRC: Longitudinal redundancy check character, FC: Format Code

## Track 2

<table>
<thead>
<tr>
<th>SS</th>
<th>FC</th>
<th>Primary Account No. (19 digits max)</th>
<th>Additional Data</th>
</tr>
</thead>
</table>

**Notes:**
- Track 2 is limited to 40 characters including Start Sentinel, End Sentinel, and LRC
- SS: Start Sentinel, FS: Field Separator, LRC: Longitudinal redundancy check character, FC: Format Code

**Additional Data**
- Expiration Date 4
- Restriction or Type 3
- Offset or PIN Parameter 5
- Discretionary Data (CVV) 5
COUNTERFEIT/CARD CLONING

Both Track 1 and Track 2 contain a CVV code.

- This code is a “Card PIN”.

The value is an encrypted code derived from other data encoded on the magnetic stripe.

- If the encoded data is changed the verification will fail.
- If the code is missing validation will fail
COUNTERFEIT/CARD CLONING

Name on Track 1 is not used in CVV/CVC formula

- Name can be changed to match ID
- Some Authorization Systems can verify name
  - Effective tool in data compromise cases
COUNTERFEIT- SKIMMING

Skimming
- When cards are “skimmed” account information, cardholder name, expiration date and CVV/CVC codes are all captured without the cardholder being aware of the theft.
COUNTERFEIT- SKIMMING

- Magnetic stripe data copied using devices readily available today – Stolen information is then written to another stripe
- Available from eBay today - $450 - Portable
COUNTERFEIT

- Skimming devices can be located anywhere.
Here is one inserted into a gasoline pump, modified to obtain card information for counterfeit cards.
COUNTERFEIT- PHISHING

“Phishing” victims provide:
- Card number
- Expiration date
- PIN

If all authorization transactions verified these CVV/CVC codes - information obtained by Phishing could not be used to make Counterfeit cards
COUNTERFEIT – VERIFY CVV

Unfortunately not all systems verify these codes

Do your Processor (s) verify CVV/CVC for all authorizations?

- Signature Credit and Debit
- PIN Debit
- ATM
BANK CARD COMPROMISE

Magnetic stripe data is obtained from Merchants and Processors who store it in violation of Association Rules and state law.

Bank Card Compromises are over 1100 in 2014.
BANK CARD COMPROMISE

What do the data thieves do with the stolen data?
BANK CARD COMPROMISE

They sell it to other thieves

How?

Over the Internet, of course
Can Card Fraud ..... 
....Be Controlled?
FRAUD CONTROL

How can Fraud be controlled?
FRAUD CONTROL

Fraud is controlled if:
- Below maximum insurance coverage
- Below industry average
- Below insurance deductible
Prevent Fraud Losses
PREVENT FRAUD LOSSES

Encode CVV or CVC on all cards
Verify CVV/CVC on all authorization transactions
  ▪ Credit
  ▪ Signature debit
  ▪ PIN debit
CVV/CVC prevents losses from counterfeiting and phishing
Verify Expiration Date on CNP transactions
Prevent Fraud Losses

Bank Card Compromise
- Defeats CVV/CVC verification
- Only 2% of compromised accounts used fraudulently
- Progress is being made with major merchants and acquirers
  - Will it ever be 100%?
PREVENT FRAUD LOSSES

Limit cash availability –
- Authorization settings

Address Verification System (AVS)
- Codes are generated at the time the merchant requests credit card authorization.
- Primary use is with “card-not-present” transactions.
- AVS codes tell the merchant if the billing address provided on the order matches the billing address of record for the card number.
PREVENT FRAUD LOSSES

Customer address-change procedures

- Prudent security verification
  - CVV2/CVC2
- Send a confirmation letter
  - To old address
PREVENT FRAUD LOSSES

The FACT Act requires that you investigate requests for replacement cards, checks or PIN’s within 45 days of an address change:

- Processor provide alerts to such requests
- Sending the letters and delaying the fulfillment of the request will comply with this provision
PREVENT FRAUD LOSSES

Card activation has been successful
- Spoofing caller ID – www.spoofcard.com
- Manual procedures when caller ID fails
  - Verify CVV2 or CVC2
- Debit Cards
  - Activate at ATM – Using PIN
Detect Fraud
DETECT FRAUD

“Neural network”
- Falcon, Visa AA, others
- The # 1 fraud control tool

Can detect 60% of fraud cases

Can reduce losses by 40%
- Can’t prevent the fraud but can reduce the loss amount
Recover Fraud Losses
RECOVER FRAUD LOSSES

What % of your fraud disputes were recovered last year thru chargeback
- Industry average 36%
- Has exceeded 45%

Plastic Card Insurance Coverage
- Chartis offers coverage
RECOVER FRAUD LOSSES

CAMS/CANS alerts contain list of compromised accounts
- Maintain a data base of all accounts on alerts
CHARTIS BANK CARD PROTECTOR

Largest Insurer in the U.S. (AM Best Rated A+)

Limits up to $1,000,000

Deductibles as low as $1,500 with a cap of $10,000
  - no matter how many cards are involved in an occurrence

Broad Definition of a Bank Card – includes Credit, Debit, ATM, Smartcard and Radio Frequency Card

Broad Definition of a Loss
CHARTIS BANK CARD PROTECTOR
EXAMPLES OF COVERED LOSSES

- Lost/Stolen Cards
- Worldwide Coverage
- Data Compromise
- Skimming
- ATM Scams
- Internet MO/TO
- Identity Theft
- White Card
- Phishing
- Counterfeit
- Account Takeover
CHARTIS BANK CARD PROTECTOR QUESTIONS?

FOR FURTHER INFORMATION CONTACT:

Tom Mulligan
1-800-221-1825 x 409
Tom.Mulligan@fratesinsurance.com

Theresa Reardon
617-502-3850
treardon@massbankersinsurance.com
OVERALL PROGRAM EVALUATION

January 20, 2015

Indicate response at right by circling appropriate letter:

_____ = Very Good
_____ = Good
_____ = Fair
_____ = Poor

1. Overall, I believe this was an effective program
   a     b     c     d

2. The program objectives were relevant to my needs
   Yes ________   No ________

3. The pace kept me interested and involved
   Yes ________   No ________

4. The length of the program was appropriate
   Yes ________   No ________

5. The speakers were knowledgeable and interesting
   a    b    c    d
   Frederick Fisher
   Thomas Mulligan

6. What would you add, change or delete from this program to make it more effective?
   __________________________________________________________________________
   __________________________________________________________________________
   __________________________________________________________________________

7. What topics would you like to see discussed at future MBA seminars?
   __________________________________________________________________________
   __________________________________________________________________________
   __________________________________________________________________________

*How many from your institution participated in this teleconference?

Name: ________________________________ Company: ____________________________________

(Optional)

Please complete and fax to 617-523-5960 or email to Pat Tabolsky ptabolsky@massbankers.org.

Thank You!