

# ADVANCED RISK SOLUTIONS

NEWS AND NOTES ON INNOVATIVE ADVANCED TECHNOLOGY TOOLS

Volume 1 Issue 4 ■ 2004

## CONTENTS

- 2 Visa Cardholder Information Security Program (CISP) Update
- 3 Visa Bankruptcy Forecast Updates Scheduled for Quarterly Release—2005 Projection Now Available
- 3 VisaRiskUSA.com To Undergo Makeover
- 4 2003 Fourth Quarter Visa Credit Card Losses Show Rise in Counterfeiting Activity
- 5 Advanced Authorization Available to All Issuers
- 6 Upcoming Advanced Authorization for Issuers Web Conference Schedule



The VISA logo is displayed in white on a blue background. It consists of the word "VISA" in a bold, sans-serif font, with a yellow and blue swoosh underneath.

## Phishing Scamsters Out to Hook Unsuspecting Consumers

**Criminals are using phony e-mails and Web sites to steal financial and personal information**

### Who is Taking the Bait?

Hundreds of consumers are finding themselves the victims of a high-tech scam known as "phishing." It involves fraudsters who hide behind the anonymity of the Internet and pretend to be a legitimate financial institution or credit card company. The fraudsters send out "official-looking" e-mails designed to trick consumers into divulging financial and personal information such as account numbers, passwords, user names, Social Security numbers, and other sensitive data. Most of the e-mail messages claim there is an account problem or warn of a possible account fraud threat. In many cases, the e-mail also includes a link to a fake Web site that has been set up to mimic the legitimate online business. Either way—the whole idea is to convince the consumer there is an immediate need to update their financial information. Many of those who receive spammed e-mail do not have accounts or customer relationships with the legitimate business that the e-mails purport to come from. This is because the fraudsters who sent them most likely used a "spamming" (mass e-mailing) technique to reach thousands of people. They are counting on the fact that some e-mail recipients will have an account or customer relationship with the legitimate company, and that they will believe the e-mail has come from a trusted source.

### How Stolen Consumer Data is Being Used

Consumers who respond to phishing e-mails and turn over the requested financial or personal information may be putting their accounts and financial status at risk in the following ways:

- Phishing fraudsters can use the e-mail data received from a recipient to access existing bankcard accounts to withdraw money or buy expensive merchandise or services.

- They can also use the data to open new bank or credit card accounts in the victims' names and use the new account to buy merchandise or get a cash advance. If the phishing fraudster opens new accounts with the victims' names, but uses an address other than that of the victim, the crime can be classified as identity theft.
- In addition, a phishing scheme can involve the use of computer viruses and worms to disseminate the phishing e-mails to still more people.

### Help Your Customers Protect Themselves from Phishing Scams

Issuers can minimize their risk and help their customers avoid phishing scams by communicating these special precautions:

- ✓ **Treat unsolicited e-mail requests for financial information or other personal data with suspicion.** Do not reply to the unsolicited e-mail or respond by clicking on a link within the unsolicited e-mail message.
- ✓ **Contact the actual business that supposedly sent the e-mail to verify if it is genuine.** Visit a Web site or call a phone number that you know to be legitimate.
- ✓ **Look for the lock.** Prior to entering account information on any Web site, be sure to look for the "locked padlock" in the browser or "https" at the beginning of the Web site address to make sure the site is secure.
- ✓ **Be cautious.** Check your monthly statements to verify all transactions. Notify your bank immediately of any erroneous or suspicious transactions.
- ✓ **Forward any suspicious e-mails claiming to be from Visa or your Visa card issuer to [phishing@visa.com](mailto:phishing@visa.com).**
- ✓ **For more information on e-mail and Web security tips, go to: [www.visa.com/phishing](http://www.visa.com/phishing).**

[continued on page 2]→

# Visa Cardholder Information Security Program (CISP) Update

Every piece of cardholder account information that passes through the Visa payment system is vital to our business operation. However, without proper safeguards in place, this information can be extremely vulnerable to internal and external compromise(s), which can often lead to fraud and identity theft.

Mandated since June 2001, the Visa Cardholder Information Security Program (CISP) is intended to provide a well-aimed defense against data exposure and compromise. The program ensures that all Visa Members, merchants, and service providers are adequately protecting Visa cardholder data and is required of all entities storing, processing, or transmitting Visa cardholder data. Members must comply with CISP and are responsible for ensuring the compliance of their merchants and Agents, whether they support Issuing or Acquiring activity, for all payment channels, including retail (brick-and-mortar), mail/telephone-order, and e-commerce.

In addition to adhering to the twelve security requirements and sub-requirements, merchants and service providers must validate their compliance with CISP. Validation is a fundamental and critical function that ensures appropriate levels of cardholder information security are maintained. Visa has prioritized validation of CISP compliance based on the volume of transactions and the potential risk and exposure introduced into the Visa System by merchants and service providers (see chart below). Some merchants and service providers validate compliance through an on-site security review and system perimeter scan, while others complete a self-assessment questionnaire and scan.

## FOR MERCHANTS:

Validation Level	Selection Criteria
1	More than 6 million Visa transactions processed annually
2	500 thousand to 6 million Visa transactions processed annually
3	Less than 500 thousand Visa transactions processed annually

## FOR SERVICE PROVIDERS:

Validation Level	Selection Criteria
1	All VisaNet Processors (Member and non-Member) and all payment gateways
2	Any service provider that is not Level 1 and stores, processes, or transmits more than one million Visa transactions annually
3	Any service provider that is not Level 1 and stores, processes, or transmits less than one million Visa transactions annually

Service providers who have validated compliance with CISP are listed on the CISP Web site. A Visa Member who uses a service provider that has not validated its CISP compliance, or whose merchant uses a service provider not yet validated as compliant, should refer that service provider to the CISP Web site for information on how to become compliant.

For more information about CISP, visit [www.visa.com/cisp](http://www.visa.com/cisp)

## CISP FREQUENTLY ASKED QUESTIONS

### Q. To whom does CISP apply?

A. CISP applies to all entities that store, process, or transmit Visa cardholder data. Members must comply with CISP and are responsible for ensuring the compliance of their merchants and agents, whether they support issuing or acquiring activity, for all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce.

### Q. What does Visa define as "cardholder data"?

A. Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, Social Security number, etc. The account number is

the critical component that makes CISP applicable. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data; however, CISP applies even if the only data stored, processed, or transmitted is account numbers.

### Q. How do merchants and service providers determine the appropriate CISP compliance validation approach?

A. The CISP compliance validation processes are outlined on the CISP Web site at [www.visa.com/cisp](http://www.visa.com/cisp). Additionally, Visa Members should notify their merchants and service providers of specific compliance actions required.

## PHISHING SCAMSTERS [CONTINUED FROM PAGE 1]

Issuers should also advise customers who believe they may be victims of a phishing crime to file an online complaint with the Internet Crime Complaint Center (a joint project of the FBI and the National White Collar Crime Center) at <http://www.ic3.gov>.

## Phishing Statement Stuffer Now Available to Issuers

Visa has produced a new consumer education statement stuffer that is geared toward phishing fraud prevention. *Protect Yourself from Phishing Scammers* (VBS 02.10.04) can be printed or customized with the financial institution's name and logo at the Member's cost by calling the Visa Fulfillment Center at 1-(800)-235-3580.

