Responding to a Data Breach

Communications Guidelines for Merchants

Responding to a Data Breach

Communications Guidelines for Merchants

It all comes down to one word: TRUST. How merchants respond to data breaches can build or damage hard-earned trust and corporate reputation.

- A 2008 survey[1] of U.S. consumers found that an average of 79 percent cite loss of trust and confidence in any business they deal with as a consequence of a security or privacy breach.
- An October 2008 consumer confidence survey[2] found that 74 percent of U.S. consumers would not shop where they feel their financial or personal information may be at risk.

Because data compromises are often complex, it is challenging to make the rapid communication decisions needed to mitigate the potential harm of a breach. These situations are often further complicated by the reality that every data breach is different and there may be no precedent within your organization for responding. But the stakes for handling a breach effectively couldn't be higher, and the impact to your business — depending on a variety of factors — can be huge. The impact of a poorly handled breach can reach throughout your business in both the short and long term: bad press, lost sales, mitigation and litigation, as well as the uphill battle to rebuild your reputation.

Although it is true that every data compromise has its own challenges and extenuating circumstances, there are some good basic communications principles that can be applied to most data breach situations. This booklet is intended to provide some best-practice guidance for merchants on how to think about, prepare for and respond to data breaches.

The best line of defense is a thorough and ongoing data security program. This document presumes that your company has extensive prevention measures in place but also recognizes the critical need for every company to be prepared to communicate in the event of a data breach. These are not requirements from Visa but are merely best practices for your consideration.

Following are five principles for effective data breach communications that can be used to guide your internal strategy discussions.

[1] The CA 2008 Security and Privacy Survey, by CA Inc.

[2] Solidcore Systems, Inc. Survey

1. Consider a Breach Likely — and Prepare Accordingly

"In today's environment, it's not a matter of if a data breach will occur, but when it will occur, and how well you respond. Do everything you can to prevent data breaches, but also fully plan out how you will respond if you are breached. Today's media and business environment demands that two-pronged approach."

Brian Lapidus
COO, KROLL FRAUD SOLUTIONS

Data breach incidents exposing consumers' personal information to misuse were at an all-time high in the United States in 2008 — a dubious distinction for which business managers and communicators need to be prepared.

The statistics are overwhelming. It seems that you can't pick up a newspaper without reading coverage about another massive data breach, and it appears no organization is immune — government agencies, corporations, nonprofits. Even the most sophisticated, best-protected IT systems can be hacked or compromised, and sometimes no amount of technology security can account for human error or deception.

Therefore, the best approach is to assume you will be breached and prepare accordingly. It is easy to waste valuable days or weeks establishing processes and relationships that could have already been in place. Best practices indicate that to be prepared, you should:

- **Have an ongoing PCI DSS compliance program** and regular security assessments. The PCI DSS is a security standard developed by the electronic payment community to help create and promote consistent data security measures. The standard is designed to help companies proactively protect customer data and includes requirements for security management, policies, procedures, software design, network architecture and other critical protective measures. For more information, visit: *https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.*
- **Designate and empower an internal breach response team** that includes experienced communicators, key operations staff, legal counsel, risk officer(s) and senior managers. Minimizing the team and the bureaucracy can expedite approvals and response. Because there may be significant liability issues involved, it is strongly recommended that legal counsel be involved in any breach-related response planning and communication.

- **Identify and establish relationships and/or agreements with key vendors, including:**

  > Outside IT security forensics experts who can investigate if, when and how a breach occurred, and how to close and repair your system. Visa requires its partners to use external experts for this function, and doing so is critical to establishing credibility with the media, customers, investors and other key audiences. Also, consider using a different vendor from the one that may have done previous security assessments — they may be defensive or too concerned with the "how" rather than the "what," "when," and "where." A list of Visa-approved CISP Incident Response Assessors (QIRA) can be found at:
  http://usa.visa.com/download/merchants/cisp_qualified_cisp_incident_response_assessors_list.pdf

  > Support services vendors that can handle large mailings to your customer database, provide credit reports, set up toll-free hotlines and offer counselors and advisors. There is a wide range of providers of breach support services. Do your research in advance and consider factors such as relevant experience, security expertise and cost.

  > Outside communications/PR support with experience handling breaches and crisis communications if you believe your internal staff may lack the capacity or experience to respond. Also, internal staff may often have a difficult time advocating tough advice to senior managers who may need convincing of a particular approach.

- **Have a breach response communications plan in place.** Most effective breach response communication plans include personnel and processes with the lists and channels needed to execute all communications that might be needed.

Lesson Learned:

One of the nation's major grocery chains announced in March 2008 that a data breach at checkout lanes in its stores had exposed 4.2 million payment cards to fraudulent misuse — the largest breach to hit a U.S. grocery chain. Apparently, the problem was not that the grocery store chain ignored IT security but that the company's security did not evolve as fast as data theft practices. *Supermarket News,* in an analysis of lessons learned from cybercrime in its industry, said:

"The breach exposed a weakness in [the company's] card processing procedure that it has since addressed. The chain discovered that malware installed on its store servers was able to gather credit card numbers as the data was being transmitted from the card-swipe PIN pad across its private network to its centralized payment switch.

" 'Our customer card information is now encrypted from the [PIN pad] in the lane and remains encrypted the entire time it is on our network,' said [the company's] vice president of marketing. … 'In the past, the data was encrypted during "part of the trip" through [the company's] private processing network,' she noted. 'PCI standards require encryption for data in transit on public networks but not on private ones.' "

As a result of its experience, the company is currently installing new PIN pads, installing the MX830 terminal from VeriFone and implementing PIN TDES, or triple data encryption, which a company senior executive termed the "highest possible level of PIN encryption."

This major grocery store chain is taking numerous other steps to strengthen its security, including "borrowing from the military and industry for the retail environment," the vice president of marketing told *Supermarket News.* "The security bar gets raised all the time. **Security is not a point in time or a single event. It's an ever-escalating threshold and a continuous process."**

2. Be Accurate And Be Fast

> *"More than 55 percent of respondents said the notification about the data breach occurred more than one month after the incident, and more than 50 percent of respondents rated the timeliness, clarity, and quality of the notification as either fair or poor."*
>
> PONEMON INSTITUTE FOR ID EXPERTS, THE CONSUMER'S REPORT CARD ON DATA BREACH NOTIFICATION, SURVEY OF 1,795 U.S. ADULTS, APRIL 2008

Find the facts and tell them fast. This is the most fundamental of crisis communications principles.

However, most often, in the case of data breaches, the desire to be certain about all facts hinders the ability to provide information quickly. Everyone wants to know all the facts before communicating, but the reality of data breaches today is that security forensics takes time — often more time than applicable state laws allow prior to disclosure and a lot longer than the "court of public opinion" considers appropriate.

Most companies experiencing data breaches end up having to announce the news well before they feel ready, and certainly well before they have determined the facts to the degree of confidence they would like. There are situations when companies are obligated to withhold disclosure of a suspected or detected breach upon direction from law enforcement officials concerned about compromising their criminal investigation. In these cases, you may have no choice but to remain silent. Even then, best practices recommend preparing to communicate at the earliest appropriate opportunity.

Once a breach is discovered, it is important that corporate executives hear a subconscious clock ticking. Why? To avoid consumer discomfort — or worse, outrage — because they feel they were left at risk for too long before being notified. Also, in the worst situations, someone other than you breaks your news first. The following are some proven suggestions for "beating the clock":

- **Put yourself in your customers' shoes.** If you discovered that a company you do business with notified you that your payment card or personal information was exposed (or may have been exposed) months after they identified a breach, or many weeks after they knew your information was involved, how would you feel? Fortunately, given the prevalence and high profile of data breaches, many in the news media now understand that a discovery period is necessary and that even a few weeks may be needed to get the facts and avoid unnecessary alarm. But even enlightened media won't accept too long a delay. Remember that consumers are unlikely to respond sympathetically when the company announces itself a "victim" of a data breach.

- **Give yourself permission to notify before you know everything,** or before you know it with confidence. IT forensics investigations can be time-consuming and tricky. Because the breadth and depth of a breach can change dramatically with one new discovery, investigators are understandably hesitant to provide any premature information or even put a timetable on their work. However, if you are three-quarters of the way through your investigation and 90 percent sure of some key facts, that's probably enough to go forward with, even if you have to caveat heavily. However, if obtaining 100 percent of the facts seems reasonably only a week or less away, it probably makes sense to hold off until you have all of the information.

- **Offer timetables.** State laws often will drive your consumer notification schedule, thus forcing you to disclose to customers — and, by default, the media — well before you are ready. If this is the case, and you do not have all of the basic information that reporters will demand (such as when, how, how many), then inform them of what you know and when you expect to know more. Commit to updating them as more facts become available. Consider the dynamic on an airplane late for takeoff — the longer the passengers sit on the runway with no information, the angrier they get. However, if the captain announces that there is a problem, what's being done and when they will provide an update, the passengers may not be happy about it, but they are far less likely to be outraged.

- **Acknowledge that the situation may change.** It's always a good idea to preface any statements describing a breach with qualifiers such as "at this time" and "according to the independent forensics investigation, we currently believe." The news media is full of accounts where companies announce the size of a breach and then have to dramatically increase or decrease their estimates. This is uncomfortable and embarrassing, but is exacerbated if you have previously stated your facts with certainty. Know this: Even cases researched by premier investigators that appeared to be well understood and resolved have later been reopened and revised based on undiscovered or new data.

- **Make it a one-day story.** By communicating early and delivering on promised updates, the company reduces the chances the media may make more of the story than it might deserve. The harder a journalist has to work to dig up the information about your breach, the more value the reporter and his/her editors will place on the story — and this will be reflected in where it is played and how long it is considered newsworthy.

Lesson Learned:

In mid-June 2008, a specialty retail chain learned it might have a problem when two of its employees reported unauthorized transactions on their payment card accounts. The company communicated proactively, and the visibility of the incident was minimal. Only one story about this breach could be found.

It turns out The Company had issued a press release in July, less than a month after the initial discovery, alerting consumers that PIN pads at eight of its Southern California stores had been breached and providing store locations, dates, and helpful information and hotlines. It accepted responsibility, apologized and reiterated that the "privacy of our customers and their personal information is a matter of the highest concern to the company, and every effort is made to ensure that all personal information and financial data maintained by [the company] is secure and safe."

The release detailed the changes the company had begun enacting to strengthen security technology and protocols, and it assured consumers it was working closely with "the financial institutions and law enforcement officials to ensure that any of its customers impacted by this incident are identified. [The company] is also working with its merchant bank and the payment card issuers to ensure that any affected cards are blocked and reissued."

3. Be Open, Honest and Transparent

> *"In the past two years, the cost of a data breach to organizations rose an estimated 43 percent with an average cost of $197 per compromised record."*
>
> PONEMON INSTITUTE, 2007 ANNUAL STUDY: U.S. COST OF A DATA BREACH, NOVEMBER 2007

The initial questions retailers should consider asking themselves are:

1. Why am I disclosing this breach?
2. When will I disclose?
3. How will I go about it?

Often, the nature of legal disclosure compliance puts many companies in a defensive posture when in fact a company could potentially benefit more by taking the stance that the best reason for disclosing openly and quickly is because it's the right thing to do for your customers and your company.

Too often, companies take the approach of determining the minimum amount of disclosure required and then working to keep their breach as quiet and hidden as possible. From one standpoint this may seem appropriately conservative, but in today's world, it is no longer realistic.

Notification letters sent to even a few thousand consumers and communications issued to investors and others often find their way into the public domain. Business reporters have become quite adept at investigating data breaches and then breaking the news that corporations could have delivered and framed themselves. As a result, the company may come off looking arrogant, deceptive or downright deceitful instead of careful.

Although it may be uncomfortable, putting out your information quickly and with sufficient detail may be the best way to make your news a one-day story. On the other hand, stalling, limiting information and appearing guarded can be an invitation for reporters to press, probe and eventually leak out details of your story in multiple reports or publish critiques of how your company handled (or mishandled) the situation.

Also, to reiterate principle No. 1, be prepared by assuming it is likely you will be breached again. The way you handle your first breach will become the reference point (for the media, consumers, investors, analysts, partners — everyone) for analyzing your response to future breaches.

Simply put, **companies need to protect their ability to communicate in the future about this issue. The following are some best practices for doing so:**

- **Be transparent in your activity and demonstrate that you are getting the word out.** State your news plainly and publicize how you are notifying consumers. Let your actions speak for themselves and realize that your actions will be analyzed. For example, putting out an ambiguous and thin press release at 5 p.m. on a Friday may not indicate a good faith effort to notify.
- **Follow your normal media routine.** If you typically put your press releases on a certain wire distribution circuit, use that same process. If you have relationships with beat reporters that you regularly update, then include the breach news in your updates. If they follow your company, they'll find out anyway. Better to hear it from you.
- **Avoid absolutes.** Again, information about the breadth and depth of breaches can change quickly and dramatically. Since you can never be absolutely certain of the facts, try to avoid speaking in absolutes.

Some companies have tried to minimize the perception of their problem and maximize the impression of their control by expressing high confidence in their findings ("we are very confident that this incident only involved x consumers"), only to later appear either foolish or untrustworthy when they had to change their story.

- **Avoid misleading statements.** It can be tempting to selectively provide information or carefully construct statements to increase confidence or decrease concern. For example, "We know of no breach" may be a convenient statement, but it is unacceptable if you have reason to suspect a breach and are investigating, or if prosecutors and other government authorities have indicated they are investigating a possible breach involving your company.

- **Don't attempt to withhold key details.** It looks bad, and it won't work. Some companies initially refuse to provide the number of transactions or accounts that are involved. But one of the very first things reporters want to understand is scope. If the information is not provided, the media will inevitably ask. But best practices recommend that you should not make them have to ask. It's OK to admit that you don't have the exact numbers or are still investigating. However, do provide as much info as you can to limit the scope. For example, "our current research indicates the breach was likely limited to less than 5,000 cardholders in Southern California" is a far superior answer to "I can't comment on that now." It's worth noting that a breach involving fewer than 1 million payment cards is unlikely to garner much media attention in today's environment.

- **Stay focused and concise.** Determine the important information to deliver, provide it directly and efficiently, and then stop talking. Avoid excessive communication that might prolong the life of the story.

Lesson Learned:

When a major global hotel chain suffered a data breach in Europe in August 2008, its public comments about the breach began to receive more scrutiny than the breach itself. "Most companies experiencing data breaches quietly apologize and hope the story goes away, but [the company] is doing everything it can to keep this story in the spotlight," wrote Ben Worthen in *The Wall Street Journal's* Biz Technology blog.

It turns out that a Scottish newspaper notified the hotel chain that a cybercriminal had obtained illegal access to about 8 million customer records in its computer reservation system, and when it contacted the company for comment, it was thanked for the alert and told that the breach had been closed, according to an article later that month in *The Times* of London by Bernhard Warner, under the headline: "Online security breaches are getting increasingly common, so we may as well settle on the right kind of response."

According to *The Times,* within two days of thanking the Scottish newspaper, hotel chain officials issued an irate denial, dismissing the paper's "grossly unsubstantiated" article and saying the company had found "no evidence" to support the story.

"For the next 36 hours, confusion reigned," *The Times* said. "A Google News search pulled up over 200 articles debating whether [the company] had or had not been hacked." The following day, the hotel chain "was back again with a third statement, this one contradicting its second statement. In fact, there was a data breach, the company now informed the public. But just 10 customers were affected, not 8 million."

Still, "in changing its story so many times, it left the public baffled about the extent of the damage and who, if anybody, is at risk," the article said.

4. Be Accountable — Always

"The risk is real. Data is streaming out of companies at an alarming rate, with at least one new breach reported daily. Businesses, nonprofits, and government agencies face a host of regulations making it clear that they have a responsibility to protect data. … The consequences of noncompliance can be severe, potentially resulting in financial penalties, reduced stock value, loss of customer confidence, and lost sales revenue."

Brian Lapidus,
COO, KROLL FRAUD SOLUTIONS

By now, the vast majority of consumers and media understand that data compromises happen. They can and will forgive companies for security lapses, bad luck or both. However, the public is very unforgiving of companies who do not accept responsibility for the security of their data. From a consumer's perspective, the issue is relatively simple: "I gave my information to you, you exposed/lost it, and it's your fault. Period."

A good practice is to immediately and consistently accept responsibility for the issue and to demonstrate ownership of the problem. Following are some recommended best practices for doing so:

- **Take ownership.** Immediately acknowledge responsibility for the breach and express regret for its impact. Once you've done so, you can quickly move to talking about the solution (what you are doing), rather than the problem. Avoid the blame game, which might include placing responsibility on an employee or vendor.
- **Don't play the victim.** Ten years ago, when announcing a data breach, it may have been possible for companies to successfully portray themselves simply as fellow victims. Today, this is a flawed and dangerous strategy. Although you may have had a crime committed against you, the public and business press will still hold you accountable and will not consider you a co-victim. Best practices recommend that rather than announce that your company was the "victim of a criminal computer hacker," you should announce that you became "aware of unauthorized access to our computer system," or some alternate phrase.
- **Express regret.** Apologizing is a critical step in taking ownership. Avoid qualified or conditional apologies. For example, "We don't think anyone was affected but regret if anyone is inconvenienced" might be worse than not apologizing at all.

- **Put an executive face on the issue.** Visibly involve a senior executive in your communications. Issuing press quotes or public comment from an IT employee, customer service representative or low-level manager does not signal commitment. Neither does sending a generic, unsigned notice as a notification letter. However, sending a personalized notification letter signed by the president or CEO demonstrates how seriously a company is taking the issue.

- **Be careful how you portray PCI compliance.** Some companies will cite PCI compliance as a defensive measure. However, data security experts point out that just because a company passed an assessment in the past and was deemed PCI compliant doesn't mean it is still compliant today. In fact, the experts say that if your company has had an unauthorized system intrusion, it is highly likely you were not PCI compliant at that time. You can discuss your PCI compliance program as evidence of your commitment to security, but be careful about appearing to use it to deflect accountability.

Lesson Learned:

A major clothing retailer and a shoe discount chain both waited more than a month after federal indictments were announced in early August 2008 in the largest single recorded data breach to release any information about their roles, according to *The Wall Street Journal* and other news accounts. *ComputerWorld* on Sept. 16, 2008, reported that the clothing retailer only said in a statement that nearly 99,000 payment cards were compromised from 2004 to 2007 but offered no explanation for the delay. Instead, it "stressed that it has complied with the requirements of the credit card industry's Payment Card Industry Data Security Standards (PCI DSS) since they went into effect. And it noted it has been certified as being PCI-compliant since 2007."

The article noted that officials from the clothing retailer did not return a phone call seeking comment and that a toll-free number to answer consumer questions carried a recording that "invited callers to leave their names and phone numbers with the promise that someone from the company would get back to them. A message seeking comment left at that number was not returned either."

Several other major retailers targeted in the massive data breach refused to tell *The Wall Street Journal* if they had made any consumer disclosures. "Computer searches of their Securities and Exchange Commission filings, Web sites, press releases and news archives turned up no evidence of such disclosures," the newspaper reported on August 11, shortly after the indictments were announced.

"If I were these companies, I would be issuing public disclosures five nanoseconds after the indictments were announced,"Evan Stewart, a Fordham University School of Law adjunct professor and data breach expert, said in the article.

5. Get the Word Out – Be Thorough

> *"Sixty-three percent of respondents said notification letters they received offered no direction on the steps the consumer should take to protect their personal information. As a result, 31 percent said they terminated their relationship with the organization. Fifty-seven percent said they lost trust and confidence in the organization."*
>
> PONEMON INSTITUTE FOR ID EXPERTS, THE CONSUMER'S REPORT CARD
> ON DATA BREACH NOTIFICATION, SURVEY OF 1,795 U.S. ADULTS, APRIL 2008

Audiences to Consider

- Cardholders
- Employees
- Customer service
- Shareholders
- Analysts
- Media
- Partners
- Regulators
- Legislators

The notification letter to customers is important, but do not become so fixated on that one task that you delay or ignore other communications. You have multiple audiences and channels to consider, and therefore it is important to be systematic in your approach. The following are recommended practices from experts in data breach communications:

- **Consider all audiences.** No audience or stakeholder wants to feel like they are the last to be informed. Having lists and systems in place to send out notifications quickly can ensure that no one feels slighted.
- **Don't forget the front lines.** Although it would be nice to control all interaction with consumers regarding a breach, it is neither possible nor practical. No matter how thorough your mailings and media statements are, there is a high likelihood that curious or concerned customers will approach company personnel in your stores with questions. Rather than expecting store personnel to address individual inquires, and to avoid having them appear uncooperative, consider providing handouts or "take ones" that can be available at the point of purchase and other key locations.

- **Leverage the power of zero liability.** Often, the fastest way to reduce consumer concern or panic is to remind consumer cardholders that they will not be held liable for any fraudulent purchase made using their payment card. Best practices recommend this message be present and prominent in all of your communications.

- **Take credit for what you are doing.** Explain how you have addressed the problem (cooperation with law enforcement, internal review, third-party forensics investigation, etc.) and what you are doing to support customers. Demonstrating activity will advance your objective of reducing customers' security concerns.

- **If law enforcement is involved,** say the company is cooperating, and if illegal usage of card data is suspected or even possible, work with Visa to monitor for fraud and say this publicly.

Lesson Learned:

Two high-profile data breaches illustrate the range of impact an organization's breach response can have on its corporate reputation. The Department of Justice announced 11 indictments in August 2008 in the largest U.S. data intrusion, which was committed against a major retail corporation overseeing multiple brands. Associated Press business writer Mark Jewell wrote in April 2007 that "for at least 17 months, someone had free rein inside [the company's] computers." The total impact of the data breach is believed to have involved at least nine retail companies and more than 40 million payment cards. The trail of fraud, and the suspects in the case, crisscrossed the U.S., Canada, U.K. and several Eastern European countries.

In 2008, the U.S. Federal Trade Commission reached a settlement with the retailer in which the company agreed to upgrade and implement comprehensive security procedures and submit to audits by third parties every other year for 20 years.

The company issued its first press release alerting consumers to the massive breach a month after it was discovered (the delay was at the request of the U.S. Secret Service, subsequent regulatory filings showed) and has provided extensive information for consumers online and via hotlines since January 2007. The breach has been costly to the company — reports indicate more than $200 million has been reserved — and the retailer has taken a reputational hit as well. Deepak Taneja, chief executive of Aveksa, a security software company, told the AP: "Unfortunately for [the company], I suspect they are going to become the poster child for poor data security."

However, redemption can follow a even record-breaking data breach. "In a remarkable turnaround, [a large data services company] excoriated two years ago for its lack of precautions as it went about gathering and selling personal data, has recast itself as a model corporate citizen," was the lead in a *USA Today* story in April 2007. (The data services company revealed in February 2005 that it had sold the personal information of at least 166,000 people to a Nigerian con artist posing as a debt collector. The widely publicized incident led the FTC to issue a record $10 million fine against the company and order it to set aside $45 million to aid victims of the data breach.)

"The once-obscure data broker ... embraced extensive reforms," *USA Today* reported. "The result: [The company] is regarded by a dozen leading privacy advocates interviewed by *USA Today* as the most responsible company among dozens in the lightly regulated, fast-growing field of aggregating and selling sensitive information."

" '[The company] transformed itself from a poster child of data breaches to a role model for data security and privacy practices,' says Gartner analyst Avivah Litan."

- **Provide real, customer-focused support.** There is no better way to restore trust and credibility than to demonstrate to consumers what you are doing on their behalf and what support you are offering.

  > **Toll-free information lines.** Call centers and hotlines are commonly offered to customers whose data were or may have been exposed and are used as proof points of corporate support. However, these services can present some challenges. If the call center is understaffed or if consumers can't get any information beyond a regurgitation of the notification letter they received, then avoid a live operator, as that can increase frustration or outrage. One option is an automated menu with preprogrammed Q&A information that extends beyond what was in the notification letter.

  > **Credit monitoring.** Although you may not feel it is needed or warranted, credit monitoring can provide comfort to consumers. Many customers are familiar with the service because they read in the media about other breached companies offering it or because they have received offers themselves following other breaches. While only a small percentage of consumers sign up for monitoring, the offer is generally appreciated. If personal identifier information was included in the breach or is suspected of being included, then it would be wise to strongly consider credit monitoring.

  > **Investigators or identity restoration services.** When customers become a victim of fraud related to your exposure of their personally identifiable information (such as Social Security numbers), you may want to consider providing access to case investigators or identity restoration services.

- **Use the Internet to inform.** In addition to putting statements and Q&A documents on your corporate website where customers will be able to find them, consider other options, such as conducting a live web chat on the subject with a top executive, which could be archived on your website. Also, consider purchasing Google search keywords (such as the name of your company in conjunction with "breach" or "hack") to help ensure that any consumers or media searching online for information about your breach will find a link directly to your best information.

- **Monitor all information sources.** Most companies will monitor news coverage as standard procedure, and many include online and blog searches as part of that monitoring. Monitoring can help you understand how your situation is being portrayed and reveal opportunities to react and respond. If reporters get some facts wrong, be very careful what you try to correct. Your pursuit of an error could pump additional life into the story. Also, don't assume no news coverage means that consumers won't notice. There still may be concerns based on word of mouth and what's being said on the front lines within your company. If you have a particularly large breach, consider doing consumer polling to better understand its impact on attitudes and corporate reputation.

Conclusion

"The key lesson of the [major retailer] security breach, may be that it is impossible to prevent data crimes against the card system. The ease of access to valuable consumer information, the considerable rewards for stealing it, the failure of law enforcement to prevent it, and the increasingly prohibitive cost of protecting it all militate against any easy solution."

Duncan McDonald
FORMER GENERAL COUNSEL TO CITIGROUP INC.'S EUROPE AND NORTH AMERICA CARD BUSINESSES
IN "VIEWPOINTS," *AMERICAN BANKER,* APRIL 20, 2007

Organizations that do business with payment cards recognize the realities cited in the *American Banker* column — including the rising odds of experiencing a data breach in the future — and have taken most, if not all, of the steps suggested here in this booklet. The most important of them is the need for advance preparation and internal structures and protocols to monitor, assess and upgrade security.

Then, when the alarm goes off, your organization will be able to respond rapidly to assemble the correct information; be honest, open and accountable; communicate with consumers and other important audiences as quickly as possible.

Although no formula can account for the many variations and circumstances that may be involved in individual data breaches, the five principles outlined in this booklet will help you navigate most situations. Following these recommended best practices from experts in data security and communications should allow you to prepare, react and respond with confidence — and then look back with no regrets.

VISA

RESPONDING TO A DATA BREACH
Communications Guidelines for Merchants

www.visa.com

© 2008 Visa Inc. All Rights Reserved.