INSIDE SECURITY

Fall/Winter 2006

MasterCard Worldwide

MasterCard Worldwide

Letter from Chris Thom

Beginning with the MasterCard Global Risk Management Symposium this past spring, the last few months have been a time of phenomenal progress and change at MasterCard. The most newsworthy of the company's accomplishments was its transition to public ownership and the unveiling of the new corporate brand, positioning MasterCard at "The Heart of Commerce."

"The Heart of Commerce" speaks to the many ways MasterCard drives value for customers, merchants and cardholders. It also illustrates the approach MasterCard takes toward security leadership, reflecting our globally integrated effort to ensure the billions of transactions that pass through our network are safe and secure.

In recent months, we have made great strides in our collaborative effort to create the most secure payment network by joining with other stakeholders in the electronic payment value chain. Since we launched *Inside Security* in May at our annual Global Risk Management Symposium, which featured expert speakers from all over the world, we've continued to push to promote a security framework that includes the best in tactical access controls, enhanced risk solutions and a focused drive toward creating a true unique transaction environment. I am heartened by the level of buy-in to this framework everywhere around the world. But to make it a reality, we require the participation of nearly everyone who touches the payment network.

To ensure improved awareness, we continue to create programs that provide forums for the ever evolving discourse around implementing this framework. From our Webinar series about data storage and compliance with the PCI Data Security Standard or our anti-fraud workshops, to our Security Masters series of anti-fraud conferences in regions throughout the world, we are reaching hundreds of merchants, processors, financial institutions, and many others key to this industry-wide effort.

This issue of *Inside Security* advances our collaborative efforts further still with even more expert commentary from all corners of the industry and coverage of topics in the areas of technology, data security legislation and practical tools for securing the transaction environment. Additionally, *Inside Security* editors were privileged to sit down with Ben Fathi, Corporate Vice President in the Security Technology Unit of Microsoft to discuss the emerging concerns of not only players in the payment industry, but of any organization protecting sensitive data.

"The Heart of Commerce" is a bold promise to our customers, merchants and cardholders: that partnering with MasterCard to take part in the global economy will be accomplished by our commitment to enabling a safe and secure payment environment.

Chris

Chris Thom
Chief Risk Officer
MasterCard International

Achieving Fraud Mitigation Success: New Techniques and Best Practices

MasterCard Advisors

Across the globe, financial organizations are achieving new levels of fraud mitigation success with the implementation of multifactor authentication at various customer interaction points. Case studies have shown that certain implementations of multifactor authentication have helped reduce specific types of payment card fraud by as much as 45 percent[1]. The data shows that the addition of supplementary authentication is making it much more difficult for criminals to make use of stolen or counterfeit debit and credit cards and related data.

But the saying goes that if you build a better mousetrap, someone will build a better mouse. The same can be said for the fraud prevention techniques within the payment card industry. Criminals are constantly seeking new ways to commit fraud. In order to maintain the security of the payment system and the integrity of our industry, we must continue to innovate.

Traditionally, financial organizations have safeguarded accounts and customer information using single-factor authentication, with a notable exception being ATMs, where both a PIN and a card are required. But technology has evolved and single-factor authentication is no longer sufficient. In the U.S. this fact has driven the federal government, in the form of the U.S. Federal Financial Institutions Examination Council, to mandate a move to multifactor authentication in some circumstances, such as electronic transfers, by the end of this year. This directive lists many possible forms that these authentication factors can take, however the financial industry, both for reasons of cost and customer convenience, has generally taken this to mean moving from single to dual-factor authentication.

This additional level of protection enhances transaction security by requiring cardholders to supply pieces of information that are unique to them and not easily accessible through credit bureau reports, hacking, or even dumpster diving. By authenticating information that is truly unique to the customer account, transactions are more secure, especially when information previously considered secure, such as checking account history, mortgage history, or even the color of a formerly owned automobile, often can be obtained by fraudsters.

Multifactor authentication already has proved successful for some applications. Many corporations currently utilize such a form of authentication to provide their employees with remote access to the company's computer network. This multifactor system typically utilizes a password (analogous to a PIN) that must be entered in conjunction with a separate code randomly generated by an external device, such as a hardware token or FOB, that is normally small enough to be attached to one's key chain. This separate password is time sensitive, normally valid for no more than one minute, so even if intercepted, it cannot be reused.

Financial Services Institutions (FSIs) can replicate this second factor by utilizing the extensive information in their own databases that is collected throughout a cardholder's relationship and that extends the full breadth of that relationship. Another option is the use of a third-party authentication system. Both require the cardholder to answer different questions with each authentication occurrence.

This type of multifactor authentication can be extremely effective when used during Internet or phone banking. Certain activities associated with changes to a cardholder's account, such as a change of address, card request or fund transfer, can often identify an attempted account takeover, and, in these and other circumstances, the use of multifactor authentication could be an effective measure to prevent fraud. Alternatively, FSIs can leverage the investment to achieve a unique transaction environment by extending its use for other banking relationship activities.

Though multifactor authentication is not currently widely used as a mitigation technique at the point of sale, other forms of multifactor authentication are taking hold around the world. Going forward, the cardholder could be asked to key in some element of numeric information such as a one-time PIN number sent to the cardholder's mobile phone for entry as separate authentication of the cardholder's identity. This type of additional authentication could even be combined with customer selected levels of transaction value or merchant type.

Multifactor authentication represents the next phase in fraud remediation, but tried and true technologies that are currently effective at preventing fraud should not be discounted, as the two work hand-in-hand.

For many years, neural network technology has been an effective technique for spotting fraud by building detailed merchant and cardholder profiles and combining them with data based on known historical fraud patterns. By using artificial intelligence to help predict fraud, FSIs are able to minimize fraudulent activity with minimal impact on true customers.

Complementary to neural network technology are rules-based technology systems, which are fast becoming a cornerstone in preventing fraud. These are highly customizable for specific FSIs and are increasingly effective. By combining neural networking technology with a rules-based system like MasterCard's Aristion, and effective authentication rules at customer interaction points, FSIs and merchants can build an effective barrier to a number of today's fraud schemes.

These fraud mitigation techniques are only one part of the key to safeguarding the payments system. FSIs, merchants, processors, law enforcement and payments companies must also focus on creating an environment that fosters collaboration and communication. With cardholder data passing through the systems of so many partners, knowledge sharing and the distribution of best practices is crucial. Doing so enables us to keep the payment system safe and secure. ■

[1] 2003 Northampton, UK public trial

Q & A with Microsoft's Security Chief

Microsoft VP of Security Technology
Ben Fathi

In today's digital world, information security is a critical factor of success for financial institutions and other companies alike. As Corporate Vice President of Microsoft's Security Technology Unit, Ben Fathi leads Microsoft's companywide effort to improve security and Internet safety. Working with others at Microsoft, the industry and customers, Fathi is driving Microsoft's vision to create a world where individuals and organizations can use a variety of devices to be constantly and securely connected to the information, services and people that matter most to them. Inside Security *interviewed Fathi on Microsoft's approach to addressing security and his advice for the financial industry.*

Q ***What is Microsoft's primary strategy for enhancing security across all industries?***

A Microsoft's security and Internet safety efforts are focused on three primary areas: (1) Technology Investments: to improve the security of our products, improve the update process, and provide new features and products that improve safety; (2) Industry Partnerships: working collaboratively with partners, customers, governments and law enforcement agencies to help customers be more secure; and (3) Guidance: delivering broadly distributed, timely information to help make customers and their systems more secure and prepared for emerging threats.

Q ***How has software development changed with data security in mind?***

A For any company that develops software or even simply has a web site that may have sensitive information, security can no longer be an afterthought and must be a guiding principal from the very beginning of the development process. This principal was the driving force behind what we at Microsoft call Trustworthy Computing. Beginning in January 2002, we have invested considerable resources in creating a culture of security, and a key part of that effort involves developing secure code. We have a formalized process called the Security Development Lifecycle (SDL), wherein every product that stores personal information, is Internet-facing, or is used in the enterprise is required to go through. The SDL has a proven track record of reducing the vulnerabilities in our software. Microsoft makes detailed information about the SDL publicly available so that other companies can apply similar best practices for secure software development.

Q ***What technology improvements is Microsoft making to address phishing?***

A Our latest technology improvements include the Microsoft Phishing Filter, available in the Windows Live Toolbar, as an MSN Search Toolbar Add-in and in the upcoming Internet Explorer (IE) 7. The Phishing Filter is an opt-in service that relies on new browser-based heuristics to analyze Web pages in real-time and warn users about suspicious characteristics as they browse. This technology is combined with up-to-the-hour online information that helps prevent users from interacting with confirmed phishing sites reported to Microsoft by a network of third-party data-provider partners as well as our users, which number in the millions.

Q ***Beyond technology, what is Microsoft doing to combat the phishing problem?***

A We are taking a holistic approach to combating phishing. Beyond technology innovation, we're also focused on collaborating with industry partners and law enforcement, as well as providing consumer education. As a member of the Anti-Phishing Working Group (APWG), Microsoft is actively engaged with other industry leaders to help reduce the threat of phishing attacks by developing and sharing information about the problem and promoting the visibility and adoption of industry-wide solutions. Also, Microsoft works with governments worldwide to promote effective legislation that enables aggressive enforcement to stop spammers and phishers. We provide governments and law enforcement with technical training, investigative and forensic assistance, and new technology tools to combat cybercrime. Enforcement is crucial because it changes the economics of phishing and other cybercrime. By having to defend themselves in court, pay steep fines - even go to jail for their criminal activity - phishing becomes cost-prohibitive rather than lucrative. Enforcement is an effective deterrent to phishers and would-be phishers considering making money this way.

Consumer education is also essential. We provide multiple resources to help consumers understand what they should look for when receiving email to verify its authenticity and then how to proceed safely to a Web site with which they want to do business, such as their bank or online retailer. People can visit www.microsoft.com/athome/security or www.staysafe.org for additional information on how to avoid phishing. ■

Microsoft®

Data Security: The View From Capitol Hill

MasterCard Global Public Policy

Given the attention paid by media, the public and politicians alike to recent high-profile incidents involving the potential compromise of large amounts of data, the topic of data security and the need to notify consumers of data breaches has been the subject of much debate in Congress. Although there has been considerable discussion on these matters on Capitol Hill, it is unlikely that such legislation will be signed into law this year. However, as an industry it's imperative that all stakeholders work to understand the issues currently "on the table" in Congress, as these will likely form the building blocks for future activity, and perhaps even legislation signed into laws that could significantly impact how we do business.

There are many different pieces of legislation pending in Congress, all of which have been considered by at least one congressional committee. They each generally address similar themes and seek to enact similar mandates, and in many ways they reflect efforts the industry has already undertaken and practices already in place. First, entities in possession of sensitive consumer information must protect that information from unauthorized disclosure and use. Second, if that information is subject to a security breach, consumers should be notified at least in some circumstances. This is a key point of debate, as some would prefer notification to consumers of any security breach while others (including the financial services industry) would prefer to provide notice only if the consumer is at some level of risk as a result of the data breach. In most breach situations many factors must be weighed to determine whether or not broad notification is in the best interests of consumers and the payment system as a whole. Therefore blanket legislation or even an attempt to create an overly broad or complex categorical approach to notifications could be counter productive.

Although the legislation tends to focus on data security and data breach notification, some of the more contentious issues involve other aspects of the legislation such as the appropriate enforcement measures. For example, there is no consensus as to whether violations of the proposed law should be enforced only by federal agencies, or to allow enforcement through state attorneys general or even class action lawsuits.

There is also debate as to whether the federal legislation should preempt similar state laws. Perhaps the most difficult issue involves "credit freezes," whereby a consumer can "freeze" his or her file at a credit bureau. Although this would make it difficult for an identity thief to obtain credit in the potential victim's name, it also imposes significant costs and hardships on the consumer as well as financial institutions. One of the key issues is not only whether the consumer should be able to "freeze" a credit bureau's file, but also under what circumstances and how quickly should a credit bureau temporarily "unfreeze" the file, such as if the consumer is attempting to open a new credit account. More than 20 states have credit freeze laws on the books.

There is significant disagreement among the several congressional committees charged with reviewing data security/data breach legislation. Given the relatively short timeframe between now and the end of the current Congress, it is unlikely that any legislation will be sent to President Bush for his signature. It is likely, however, that this issue will receive considerable attention in the next Congress, especially as it relates to credit freezes. ■

The Regulators Clarify the Online Authentication Guidance: They Weren't Kidding!

Note: This article was abridged from TowerGroup Viewpoint #169, August 2006, by Senior Analyst George Tubin and Research Director Susan Feinberg. For the complete text, visit www.towergroup.com and log-in using your username and password.

Since the Federal Financial Institutions Examination Council (FFIEC) issued its "Authentication in an Internet Banking Environment" guidance in October of 2005, the banking industry has struggled with how to interpret the guidelines.

Among the requirements, the guidance directs financial institutions to undertake risk assessments to determine ways to reliably authenticate customers who are attempting to access Internet-based services. Moreover, the guidance clearly states that single factor authentication is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.

The guidance further states that where single-factor authentication is deemed inadequate (by the risk assessment), "financial institutions should implement multifactor authentication, layered security or other controls reasonably calculated to mitigate those risks." And this is where the confusion comes in.

Many institutions did not know whether the guidance was pertinent to their situation, how to conduct a risk assessment, or what authentication methods would be condoned by the regulators. Since the FFIEC guidance was issued in October, TowerGroup has received countless inquiries from financial institutions, vendors, and the press asking for help in understanding it.

Federal Financial Institutions Examination Council (FFIEC) Guidance on Authentication (2006)

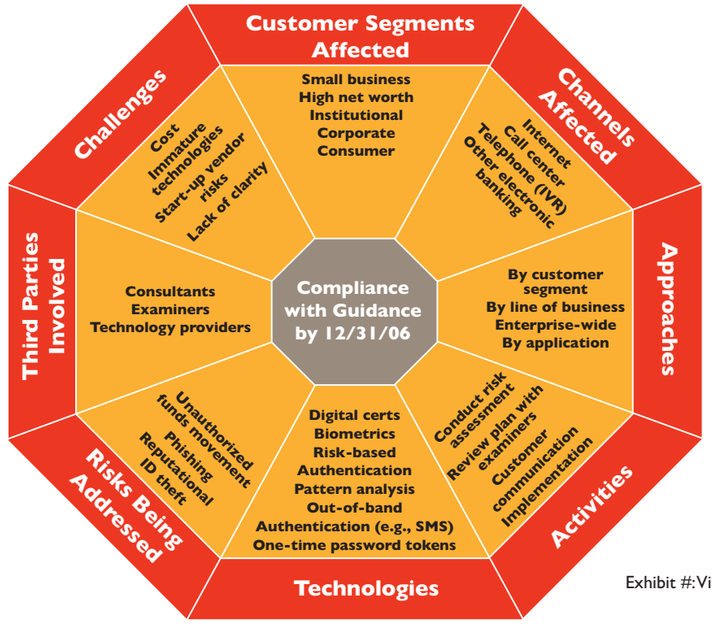

Exhibit #: ViewPoint Issue 169-E1
Source: TowerGroup

Implications for Commercial Banking

On August 15, 2006, the FFIEC issued a seven-page document containing responses to frequently asked questions regarding the authentication guidance. (See www.ffiec.gov for the original guidance and FAQ documents.) Following are specific implications highlighted in the FAQ document for commercial banking, although most comments are applicable to commercial banking as well.

Choice to Opt Out. Some banks have allowed customers to opt out based on UCC4a provisions. These provisions enable the bank to transfer responsibility for fraudulent transactions to customers if they refuse commercially reasonable security. This FFIEC guidance will likely cause banks to eliminate the opt-out provisions of their funds transfer and ACH agreements or to establish new alternative security procedures that go beyond username and password entry.

Use of a Second Password. The FFIEC indicates that including an additional password for initiating high-risk transactions would not be considered multifactor authentication. However, this approach could be used as part of layered security or other compensating controls.

Beyond Internet Banking. Bankers and technology providers should remember that the guidance applies to more than just Internet banking.

Alternative Methods. Small business customers have been increasingly demanding high-risk services that were previously offered only to large corporate customers. These demands are challenging banks to offer equivalent methods of security that reflect the risk of the activity without the high cost per user for their corporate clients.

Implications for Consumer Banking

Following are specific implications highlighted in the FAQ document for consumer banking, although most comments are applicable to commercial banking as well.

Telephone Banking. The regulators reiterated that the guidance pertains to all forms of electronic banking, including telephone banking. Fortunately, call center agents typically ask users for several pieces of information, including shared secrets (e.g., the amount of the customer's last mortgage payment), which can be used for high-risk transactions if the bank believes that this approach is an effective method to mitigate risk.

Multiple Possible Approaches. Multifactor authentication is only one of several methods that can be used when single-factor authentication is deemed inadequate through risk assessments.

Compliance Deadline Implications. The deadline for complying with the guidance, in its entirety, was again confirmed to be the end of 2006. The Agencies announced that financial institutions that fail to implement a solution by the end of the year will be assessed on a case-by-case basis. The regulators have been very clear on this point.

Risk Assessment. The FFIEC finally provided more direction to financial institutions regarding the approach for conducting a risk assessment. The FFIEC IT Examination Handbook, Information Security Booklet provides significantly more clarity to financial institutions on conducting an appropriate risk assessment, although the institution can alter the approach if it reasonably concludes that another method is more appropriate.

The time for banks to take action to comply with the FFIEC guidance is almost past. The regulators have stood firm and expect that banks will not only have completed their risk assessments but also will have implemented new security procedures. Many institutions have failed to act, hoping against hope for a last-minute reprieve. But the regulators are serious. Banks must stop stalling and fix their security holes because the regulators mandate it. What is more important is that the fraudsters are hoping banks don't. ■

Battling Fraud at the ATM

ATM crime is a problem being experienced globally. As professional criminals have realized the vulnerability of ATM networks, fraud has increased and is much more sophisticated. The first "Lebanese Loop" devices, which have been used to trap cards and money in the machine, were first seen as early as 1994. This was followed by the first reports of externally compromised ATMs in 1998. In recent years, there has been a growing number of occurrences where machines have been internally compromised, as well as external skimming and video devices being used to capture magnetic stripe data and customer Personal Identification Numbers (PINs). While the same ATM scams seem to appear everywhere, some techniques seem to be more popular in certain regions.

When it comes to ATM-based fraud, criminals are taking advantage of the proliferation of cash machines into non-banking locations, which make them an appealing target for adding skimming devices to capture Cardholder data. Criminals are also targeting small- and medium-sized institutions that may not have adequate security controls in place. Because these institutions have not traditionally been targeted, many do not have adequate defenses in place. They may not, for example, monitor their ATM terminals or be able to afford the sophisticated fraud detection technology necessary to identify patterns indicative of skimming and counterfeiting during card transactions.

To help combat ATM attacks MasterCard Security and Risk Services has gathered information about common ATM attack methods and developed best practices to increase customer awareness of the problem and identify ways to minimize losses associated with fraud attacks at ATMs. MasterCard customers can find a complete copy of MasterCard's Best Practices Series: ATM Fraud at www.mastercardonline.com. ■

Ensuring Security for PIN Debit Transactions

These days, consumers have a multitude of different options to pay for goods and services worldwide. One method that is growing in popularity is the debit or check card, which allows a consumer to enter a personal identification number (PIN) at the point of sale. According to *Cards and Payments* magazine, PIN debit transactions are poised for double-digit growth over the next few years - thanks in large part to consumers' confidence in the security of the PIN code system.

However, as criminals become more sophisticated and find ways to crack the PIN system, additional security measures must be adopted, especially considering that PIN debit fraud has the potential to have a more widespread impact on cardholders' lives by giving criminals access to checking and savings accounts.

A security breach earlier this year allowed thieves to steal valuable PIN-code data from a third-party entity and use that information to withdraw cash from consumers' bank accounts. This incident proves that additional solutions must be implemented - and MasterCard is already on the case.

To safeguard the PIN debit system, MasterCard recently rolled out a new anti-fraud solution developed in collaboration with BasePoint Analytics. The MasterCard Online Fraud Monitor is a new, sophisticated risk-scoring model to detect potential fraudulent PIN debit transactions during authorization processing in real time. The scores use advanced analytics that consider factors such as account spending, device-level (ATM and POS) activity, and historical transactions to calculate the likelihood of fraud on an individual ATM card or debit account.

In practice, this means that when a debit card is swiped and the PIN is entered, MasterCard's technology quickly examines and scores the transaction for potential fraud, allowing the issuing bank to advise the merchant whether to accept or decline the transaction in real time.

The MasterCard Online Fraud Monitor differs from other fraud mitigation tools currently in use because it is the only one specifically designed for PIN debit transactions. In addition, it does not require consumers to change how they use their cards.

By being the first to offer a risk solution specifically developed to identify all types of PIN-based debit fraud, MasterCard continues its heritage as being the industry's security innovator and a global leader in the world of PIN debit. ■

Update: Operation STOP IT

Shutting Down Phishing Sites, Defending Consumers and Working with Law Enforcement

More than two years ago, MasterCard International launched Operation STOP IDENTITY THEFT to protect consumers and combat illegal online activities by shutting down thousands of Web sites conducting phishing scams. Since its inception, the program has aided law enforcement agencies in arresting criminals who attempt to con unsuspecting cardholders into divulging their private account information.

Operation STOP IT aggressively hunts for cyber scams around the clock and works in cooperation with law enforcement to dismantle the online tools and venues data thieves use to steal personal information from unsuspecting consumers and helps ensure that criminals are prosecuted to the fullest extent of the law. ■