

**DELETING COMMERCIAL CHILD PORNOGRAPHY SITES FROM THE  
INTERNET: THE U.S. FINANCIAL INDUSTRY'S EFFORTS  
TO COMBAT THIS PROBLEM**

**WRITTEN TESTIMONY OF WILLIAM MATOS  
GROUP MANAGER AND SENIOR DIRECTOR  
OF CREDIT AND RISK MANAGEMENT  
CHASE PAYMENTECH SOLUTIONS, LLC**

**Before the  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS  
HOUSE COMMITTEE ON ENERGY AND COMMERCE**

**September 21, 2006**

Good morning Chairman Whitfield, Ranking Member Stupak, and Members of the Subcommittee. My name is Bill Matos, and I am the Group Manager and Senior Director of Credit and Risk Management at Chase Paymentech Solutions, LLC. Chase Paymentech is strongly committed to combating child pornography, and it is my pleasure to appear before you today to discuss this important issue.

Chase Paymentech is one of the nation's largest processors of bankcard (*e.g.*, MasterCard or Visa) payment transactions for merchants. One of our primary roles is to contract with, and provide services to, merchants to enable them to accept MasterCard and Visa payment cards. The activities we perform in the bankcard systems are commonly referred to as "acquiring" or "payment processing" services. We provide these services for many types of electronic payment transactions, including those conducted by credit card, debit card, gift card, electronic check, and other payment methods. We are headquartered in Dallas, Texas and have facilities in Florida, New Hampshire, and Arizona among other states.

### **In General**

Chase Paymentech has a strict prohibition against our services being used in connection with child pornography or any other illegal activity. Our credit and risk management team for our e-commerce merchant platform consists of 20 employees dedicated to screening potential merchants and monitoring our existing merchant base for a variety of risks, including those relating to child pornography. Our proactive efforts to screen and monitor our merchant base involve an extremely thorough and comprehensive process designed to ensure that our merchants are engaged in legal activities in compliance with our standards and those of MasterCard and Visa. In addition to the resources we dedicate to prevent the processing of child pornography-related transactions, Chase Paymentech has also coordinated with the National Center for Missing and Exploited Children ("NCMEC"), a variety of law enforcement agencies, and other companies to combat child pornography on the Internet.

### **Proactive Due Diligence**

Chase Paymentech has strict standards that must be met before we approve a merchant's application for our services. We collect detailed information about merchant applicants and thoroughly review the application of each potential merchant to ensure the merchant meets our credit and risk management guidelines. This review process can take anywhere from two days for more well known merchants to five days for higher-risk merchants. Depending on the circumstances, we may collect the applicant's financial statements and other financial information, tax returns, corporate documents, background information on the applicant's ownership, detailed information relating to the applicant's business and its history with respect to payment card acceptance, and other information required by the USA PATRIOT Act to properly understand who the merchant applicant is and to assess our credit and risk exposure as a result of processing the merchant's transactions.

Not only do we assess the financial risks the merchant may pose to us as its payment processor, but we also engage in a thorough review of the compliance risks the merchant may present. Before we approve an applicant as one of our merchants, for example, we must understand the applicant's business model and product line thoroughly. For on-line merchants,

this includes a web site review by a member of our credit and risk management team who examines the merchant's entire site, including links the merchant intends to display. We also investigate the web site domain ownership and navigate through the checkout process in order to understand more fully the merchant's activities. If a merchant's site is not live or fully functional at the time of application, approval is placed into a "funds hold" status which prevents the merchant from being funded for any transactions until such time as the live site can be thoroughly reviewed. Chase Paymentech also participates in the MATCH program, which is hosted by MasterCard. The MATCH database lists merchants who have been terminated by other acquiring banks and serves as a reference tool to help protect acquiring banks, like Chase Paymentech, from entering into business with merchants that are known problems.

It is our experience that child pornographers and others who engage in illegal activity rarely apply directly to us to obtain payment processing services. This is probably due in large part to the increasing sophistication of the criminals, their awareness of the due diligence we undertake as part of the application process, and their awareness of our on-going monitoring activities described below. For example, a sophisticated criminal enterprise is unlikely to subject itself to our review of its financial situation, its ownership, its lines of business, and its web site. This type of direct scrutiny is a strong deterrent to child pornographers as well as other unqualified or unscrupulous applicants. If, nonetheless, we do uncover any activity or material that is illegal, we promptly report it to the appropriate law enforcement agency and offer our assistance in any law enforcement investigation.

### **On-Going Monitoring**

In addition to engaging in a thorough initial review of applications, we also proactively monitor our existing merchants. In fact, there are three proactive means by which we monitor our Internet merchant base. The first method we use is a periodic review of the merchant itself. This procedure is similar to our initial due diligence and consists of a member of our risk management team reviewing the merchant's business including its entire web site. We engage in the review for several purposes, such as ensuring that the merchant has not established new lines of business or activities without notifying us, and ensuring that the merchant's practices have not evolved in a manner that creates a legal or compliance risk for us.

The second mechanism involves the use of anonymous visits and purchases from the merchant's web site, also known as "mystery shopping." We engage in mystery shopping based on random samplings of merchants. We also engage in mystery shopping if we believe there are unusual transaction patterns or if "something just does not look right" with respect to the merchant's transactions based on the merchant's profile. We then assess whether the transaction pattern suggests a more significant problem and further investigation is warranted. The use of mystery shopping allows us to verify the products that are actually delivered to the consumer, and to make sure that the web site transaction process is not simply a "cover" for unscrupulous activities.

The third tool in our on-going review of merchants is transaction monitoring. Transaction monitoring is a continuous process that allows us the opportunity to flag and review factors that are indicative of suspicious or unusual activity on the part of a merchant. Our monitoring of transactions can take a variety of forms. For example, we monitor the volume of

transactions for each merchant as well as the merchant's average transaction amount to ensure that those parameters are consistent with that merchant's general business profile and comport with the parameters that were established upon our initial approval of the merchant. Any material discrepancy with respect to those parameters may suggest that the merchant is not engaged in the activities it once was or that the merchant is impermissibly processing transactions for another entity. Such unusual patterns would be a red flag indicating that the merchant should be examined more closely to ensure that it is still operating in a legitimate manner. If we have any reason to believe that any suspicious activity has taken place, we file the appropriate Suspicious Activity Reports with the authorities and investigate further. We also have the ability to suspend payment processing for that merchant.

In addition to our proactive efforts, we also obtain information from MasterCard and/or Visa relating to unusual activity that may be indicative of suspicious merchant behavior. For example, a bankcard association can analyze transaction activity involving a variety of card issuers and merchant acquirers to detect patterns that an acquirer alone may not be able to detect. MasterCard and Visa can also monitor the Internet for misuse of their brands by merchants, which is then relayed back to us and others whose merchant business may be affected. In these circumstances we work in concert with MasterCard and/or Visa to investigate and address the issue as quickly and thoroughly as possible.

### **Response to Child Pornography**

As I described above, Chase Paymentech currently provides payment processing services for a large portfolio of merchants. In the course of our processing payments for that portfolio, we are aware of two legitimate merchants who have fallen prey to fraudulent and criminal activity by child pornographers. In both cases, those merchants unwittingly became conduits for child pornography-related transactions that the merchants, in turn, submitted to us for processing. (I should note that in another circumstance, a merchant was foolish enough to apply to us directly for payment services, even though its web site had links to child pornography. We discovered the child pornography, reported the merchant to law enforcement, and denied the application.) Although it is extremely rare for a child pornographer to gain access to our system, we remain extremely vigilant and have an action plan we execute if such access occurs. If we become aware of facts suggesting that someone is attempting to process child pornography-related transactions through us, such as by doing so through another merchant, we immediately suspend our processing services for the merchant in question. It is important to understand that ceasing payment processing is a delicate issue, as it could "tip off" the criminals, in which case they would likely disappear without a trace. We therefore work closely with law enforcement authorities and, in addition to our efforts to stop payment processing, we immediately engage in other remedial action. For example, we visit the merchant's web site and engage in other research to obtain as much information as possible to determine the scope and nature of the merchant's activities. We also notify NCMEC through a dedicated web site, we notify the nearest office of the Federal Bureau of Investigation, and, where appropriate, we notify local law enforcement. Any ultimate termination of the merchant account is also reported to the MATCH system maintained by MasterCard.

## **Conclusion**

Chase Paymentech strictly prohibits the use of its payment processing services in connection with child pornography. We have sophisticated and effective mechanisms to prevent child pornographers from using our services, and we have been successful in our efforts to combat child pornography on the Internet. Chase Paymentech looks forward to working with the Subcommittee as we coordinate our resources to eliminate the financial viability of child pornographers on the Internet. It has been my pleasure to describe our efforts to thwart payments for child pornography, and I would be happy to answer any questions you may have.