

Statement of Kim Mowder
BA Merchant Services
Bank of America
Before the
Committee on Energy and Commerce
Oversight and Investigations Subcommittee
U.S. House of Representatives

Chairman Whitfield, Congressman Stupak and members of the committee, my name is Kim Mowder, and I am the Head of Risk and Fulfillment for BA Merchant Services, a subsidiary of Bank of America. BA Merchant Services provides card processing services for approximately 700,000 merchants across the United States.

First, like my colleagues, we applaud the Committee's focus on this issue and the coalition that Ernie Allen so ably chairs. We are proud to be a part of this collective effort. We are equally proud to be associated with the National Center for Missing and Exploited Children. We subscribe to and whole heartedly agree with all the benefits and progress Mr. Allen has described for you.

I would like to begin my testimony by emphasizing that Bank of America's policy and practice is to vigorously screen for and avoid signing merchants that are engaged in any kind of questionable activity, let alone child pornography, and to terminate any relationships that subsequently change in that direction, should that happen. We simply have zero tolerance when it comes to issues like child pornography. And like our colleagues, we are closely aligned with and cooperative with law enforcement at every level in their efforts to combat this issue.

Bank of America is the second largest acquirer of merchant credit card processing in America. We have been processing credit cards for merchants since 1958 and have approximately 700,000 active merchants in our portfolio. We take great pride in our very conservative, risk averse approach to the merchant services business and do not hesitate to decline nearly 2,000 applications a year because the activity of the merchant is inconsistent with our policies.

In that regard, our underwriting policy clearly defines those merchant types whom we deem to be "unacceptable" for a card servicing relationship. We

are much more conservative than what is legally permissible. The following business types are routinely declined by us:

- Adult entertainment products/services
- Dating/escort services
- Debt collection firms
- Pornography products/services
- Tobacco products being sold via mail order, telephone order or Internet sales
- Wire transfer of money or any money service businesses (MSB) including payday loans and check cashing

No exceptions are made on these businesses entities and, again, we have zero tolerance for issues like child pornography.

Our process of thoroughly vetting merchant applications begins with a sales person talking directly to a merchant, often face-to-face. Together they complete a merchant application package that is then sent to the underwriting experts in our processing center. Our process is based on the principle of “know your customer,” not only to screen out undesirable activities but also to look for other potential business opportunities.

Merchant application packages contain profile information on the merchant's business that includes, but is not limited to, a description of products and/ or services being sold, a description of how sales will occur, and demand deposit banking information. In addition, the merchant application may include personal name, address and social security number information on the owner/officer of the business if it is a small or new business. This information is used in the due diligence process to validate the business type and ownership.

Underwriters reviewing new merchant application packages are charged with validating the merchant's physical business address, confirmation of the products or services being sold, and the methods of sale (retail store front, mail order, Internet, etc.). All verifications are documented should later comparisons become necessary.

And, of course, all pages and links in a merchant's web site are examined, copied and maintained for future comparisons.

We believe that validation of ownership, business address and type is a simple but critical part of this process and we use sources of information like the following to verify all application information:

- Local, state and federal record sites (county clerk, secretary of state, etc.)
- Multiple search engines (yellow pages, phone number search, reverse information look- up services)
- Telephone contact with nearby businesses to secure knowledge of merchant activity
- Calls to trade associations familiar with the merchant or merchant business type
- Better Business Bureau Reports
- Dun & Bradstreet Business Reports
- Marketing materials requested from the merchant
- Invoices for store inventory confirming products in inventory
- Invoices for previous sales (calls frequently made to buyers to confirm products purchased)

Based upon information received from the above sources, the underwriter may find it necessary to perform additional due diligence to arrive at a sound business decision. We will do whatever is necessary to ensure we are signing merchants consistent with our policies.

Again, should the merchant be selling products or services via the Internet, the merchant's Internet site is reviewed in depth, with substantial focus on embedded links to any other sites to identify products/services offered for sale through links in the merchant's site. This identifies merchants that may be assisting other parties in sale of products or services that are unacceptable under our policies. The underwriter copies all internet pages that have been reviewed and stores them in the merchant file, primarily so they can be periodically checked for subsequent deviations.

Screening for unacceptable activities does not end with the initial due diligence process. BA Merchant Services' Risk Department performs daily monitoring of merchant transaction histories on existing merchant accounts. Investigators use an in house merchant transaction tracking tool with features that are designed to ensure close monitoring of merchant's daily processing activity. Based upon parameters preset at the time of approval,

daily activity reports are generated on those merchants that appear to be processing sales transactions that are contrary to the expected norm based on the original terms of their processing agreement and the business size and type.

Risk investigators utilize the same due diligence tools to investigate merchants appearing on any exception reporting as those used by the underwriters on new merchant applications, all in an effort to gain an understanding of merchant's current processing behavior. Due diligence may include but not be limited to talking directly to cardholders to confirm transaction validity and makeup, communicating with the merchant's banking representative and speaking directly with the merchant to gain answers to specific questions. From their investigation, the investigator will determine what, if any, post due diligence action is required by our policies.

The risk investigator may elect to terminate the merchant account based upon the risk associated with the new information obtained in the investigation, establish a loss reserve fund to compensate for any elevated risk associated with the merchant's new method of operation, or take no

action at all, if new information learned falls into acceptable parameters for the business type.

Should the investigation determine that the merchant subsequently has begun engaging in unacceptable activities, the following actions are taken immediately:

1. Merchant processing capability is terminated immediately;
2. Merchant profile information is forwarded to Bank of America's Investigative Services Division for immediate investigation; and
3. The bank coordinates with law enforcement.

And, of course, we work in close partnership with the Card Associations. They employ on our behalf a vast array of protocols, all designed to be a formidable line of defense and capture real time potential illegal activities. Our efforts and their efforts are not discrete but a seamless and cooperative venture to ensure we all prevent the use of our payment networks for such purposes. It is a partnership, made stronger by the coalition Ernie chairs.

We have seen this work first hand. Although we are aware of only one instance in our nearly five decades of experience and with our 700,000

merchants, in 2005 MasterCard did alert us to the potential for child pornography being offered through a link that subsequently appeared on a merchant's web site, a merchant account that was opened for the sale of software. The merchant filed a police report to substantiate they knew nothing about the link and we do not know if the site was pirated from overseas or whether the merchant added it after the account was opened. For our purposes, it did not matter. We immediately closed the account, consistent with our zero tolerance policy. But this does demonstrate the effectiveness of the partnerships between acquirers and the associations, in addition to the due diligence we perform in combating these types of activities.

This single instance also highlights another point I would like to make. The merchant in question, even though they may have been victims, was acquired by a sales organization subsidiary that became affiliated with the bank in 2004. We have announced the divestiture of this company and are bringing all merchant acquiring in-house. We believe this strengthens our ability to vet, sign and re-verify merchant activity to ensure it is consistent with our policy.

In summary, Bank of America has a zero tolerance for anything related to child pornography. We believe strongly that our investigations and due diligence procedures provide assurance that no undesirable merchant activities are being processed through our service and we work closely with Card Associations to close any merchants they identify as posing a risk. Finally, we support the collective efforts of the coalition and of this committee to ensure the legitimate electronic payments industry is neither wittingly or unwitting facilitating the sale of online child pornography.