

Speech by Susan Grant,  
Vice President, Public Policy and Director, NCL's Fraud Center  
National Consumers League  
2007 Interagency Consumer Complaint Conference  
Houston, Texas  
October 16, 2007

Thank you very much for inviting me to speak at your conference this year. I want to talk today about how financial institutions can and should do more to protect their customers from fraud. I also want to talk about the important role that complaint handlers at the regulatory agencies can play.

Let me start by saluting those of you who answer consumers' questions and help them resolve their complaints everyday. It's not an easy job, as I know from the many years that I did it in the Northwestern District Attorney's Office in Massachusetts. While I was Director of the Consumer Protection Division, it was a small operation and I handled questions and complaints like everyone else there.

Organizations such as the National Consumers League do important educational and advocacy work on behalf of consumers. But it's the direct, one-on-one help that people like you provide to individuals that puts the concept of consumer protection into action. The tangible results of your efforts strengthen people's belief in the fairness of the marketplace and in government as an instrument for achieving justice.

Consumer education is another key part of your jobs. Obviously, it's important for people to understand their rights and responsibilities and how to make wise choices in the marketplace. However, all too often the burden is placed on consumers to protect themselves from fraud and abuse, and when problems arise the solution is usually more consumer education.

But consumer education alone will not protect people from fraud and abuse in the marketplace. Businesses have a responsibility to protect their customers.

Let's take the foreclosure crisis as an example. Who is in a better position to evaluate the borrower's ability to pay – the unsophisticated first-time home buyer or the lender? Selling someone a loan when you know the person can't afford it or without making any effort to verify that the person can is a scam. So is overstating appraisal values. When banks and their subsidiaries engage in these practices or are party to them, they have failed their responsibility to protect consumers.

The government failed as well in this case. To prevent these abuses in the future, mortgage brokers and lenders must be held to a legal duty to sell products that are appropriate for the borrowers. Some particularly risky types of products, such as "no doc" loans and interest-only loans, should probably be prohibited.

These mortgage problems should have been easy to predict. Certainly, consumer groups sounded alarm bells early on. Complaints and inquiries to government agencies can help to identify problems like this that need to be addressed – and in some cases addressed quickly. I don't know the extent to which federal agencies that regulate financial institutions share information with each other about the questions and complaints they receive or whether they communicate with the relevant state agencies in that regard. But this kind of "ear to the ground" information is vital to collect and share and to move up the chain to policy makers quickly when it's obvious that a serious problem is developing.

Meanwhile, victims of these mortgage scams need help to refinance and work out payment plans to save their homes. Government complaint handlers could play an important role in providing this assistance.

Another example of where financial institutions could better protect consumers is identity theft. While some ID theft occurs because people have been careless with their personal information, in many instances they are tricked into revealing it or it is stolen in ways that are beyond their control.

Take phishing, where ID thieves lure people into providing their personal information by impersonating banks and other trusted entities. Phishing can happen by phone, but most often these scams are perpetrated online using fraudulent domain names in emails and on phony Web sites. The scammers use names that are identical or confusingly similar to those of legitimate financial institutions and other businesses – sometimes even government agencies. The FDIC has been impersonated by phishers.

One way that brand owners can combat phishing and protect their customers is by purchasing all of the domain names that are similar to their's. The cost of this is fairly insignificant, especially compared to the harm that phishing can cause. Once an ID thief has information such as your social security number, it's impossible to put the genie back in the bottle. Another thing that banks and other brand owners can do is police the use of the brands, using technology to detect copycats and taking legal action to stop the.

The IP Governance Task Force, a group that has been calling attention to this issue, contends that financial institutions are already required to protect their brands under various regulations but that they are ignoring that responsibility and regulators are not enforcing those requirements. More information is available at [ipgovernance.com](http://ipgovernance.com).

Banks and others that collect personal information also have a responsibility to safeguard it from internal and external theft. But it seems as though we are constantly hearing about major security breaches – and there are undoubtedly many breaches that are never disclosed. Requiring individuals to be notified when their personal information is improperly accessed would go a long way toward making the holders of that information more responsible for its safekeeping.

Then there is the issue of how to help consumers if they become ID theft victims. Many banks and other companies offer ID theft assistance, sometimes for a fee. Some also offer ID theft protection. But there are no standards for ID theft assistance or protection. Sometimes the claims made for these services are misleading. And often the services provided – credit reports and credit monitoring – are things that consumers could do themselves for free or at a much lower cost. Furthermore, stolen information can be used in ways that do not show up in credit reports, such as for employment fraud.

A requirement for better disclosures about what these services entail would be a good start. But there should also be minimum standards for the assistance that is provided to ensure that consumers get meaningful help. The questions and complaints that financial regulatory agencies may receive concerning these services could be very useful in formulating such standards.

Another issue that I'm sure you hear about is unauthorized debits from consumers' bank accounts. At the National Consumers' League's Fraud Center, which provides advice to consumers about telemarketing and Internet fraud and transmits information from consumers about suspected scams to law enforcement agencies, we hear about unauthorized debits mostly in the context of complaints about free trial offers for memberships in discount buyers clubs or similar types of services.

Often the consumers don't realize that their bank accounts will be debited at the end of the trial period unless they cancel. And sometimes their accounts are debited even though they never provided their bank account information or agreed to the offer. Once they discover the debits, these consumers often find it difficult to convince their banks that they never authorized them.

As you probably know, if debits go through the ACH system, they come under Regulation E and the rules of NACHA, the electronic payments association. In the last few years, NACHA has been committed to

reducing unauthorized debits by placing more responsibility on banks for abuses of the ACH system. We support NACHA rule changes which will be implemented soon to set thresholds for debits that are returned as unauthorized and improve reporting by the banks that put debits through the system. The rules will also enable NACHA to fine the banks for unacceptable levels of unauthorized debits and remove bad actors from the system.

In addition, NACHA has recently proposed new rules aimed at helping consumers challenge unauthorized debits more easily. They would require a recognizable name for the vendor that originates the debit to show on the consumer's bank statement. Currently, the name that appears is often different than the one that was used during the solicitation. The rules would also require the vendor to have a customer service number that operates during normal business hours and to provide that number to the consumer's financial institution so it can better assist the customer if there is a question or problem.

Information sharing between regulatory complaint handlers and payment systems such as NACHA could be very helpful in identifying problems and solutions to them.

Another way that consumers' bank accounts can be debited is through demand drafts, sometimes referred to as remotely created checks. These are not covered by Regulation E or the NACHA rules. A demand draft is essentially a check created and signed by the merchant on behalf of the consumer, supposedly with that person's authorization to debit the account to pay for something.

Demand drafts figure in many buyers club-type complaints. It's an easy way for unscrupulous merchants to debit consumers' accounts without actually having their authorization and without the safeguards and redress provided under federal banking regulations or NACHA rules. Demand drafts should be banned because there is no legitimate need for them and they can be abused too easily.

The last example I want to share of how financial institutions can take more responsibility to protect consumers is the explosion of fake check scams. There are situations in which con artists give consumers checks or money orders to pay them for items they're selling, as part of a work-at-home scheme, as an advance on the millions they have supposedly won in a sweepstakes or lottery, or for some other reason, and ask them to send money somewhere in return. But the checks or money orders are phony, and when they bounce, the consumer ends up holding the bag.

We first began to hear about fake check scams in 2003 and created a category for them in our Fraud Center database that December. As of September 2007, fake check scams are the top telemarketing fraud and the second most common Internet fraud reported to us.

At the root of the problem is the fact that consumers don't understand that there is a difference between the funds being available and the check being good. Victims are losing an average of \$3,000 to \$4,000 to these scams, but that's not the end of their problems.

Some banks are closing victims' accounts and reporting them as bad customers to ChexSystems, the reporting bureau that banks use to share information about checking account abuses. This often prevents victims from opening new accounts anywhere else. And some victims are even being prosecuted for check fraud.

I'm happy to report that as a result of discussions that we have had with ChexSystems, it has recently created two new reporting codes, one for 419 advance fee fraud and the other for 419 advance fee abuse. As you may know, 419 refers to a section of the Nigerian criminal code and has become a shorthand for many scams that originate in foreign countries, whether the perpetrators are in Nigeria or other places.

The 419 advance fee fraud code is intended for banks to use when they think that the customer knowingly participated in a scam. The 419 advance fee abuse code is for situations where banks think the

customer was an innocent victim but the account was closed anyway. Hopefully banks will give people with the 419 abuse code the benefit of the doubt when they seek to open new accounts.

Of course, it would be better if innocent victims' accounts were not closed in the first place. It's a lose-lose proposition – the banks lose their customers and consumers lose access to checking accounts. And it would be even better if the victimization could be prevented.

Banks are the first line of defense against these scams because they are in the best position to give consumers information at the key moment they need it – when they are depositing the checks or withdrawing the money to send to the crooks. As you know, federal law requires banks to tell customers when the funds will be available – but there is nothing to prevent banks from going further when customers ask if the check has cleared and explaining that just because the funds are available does not mean the check is good and that if it comes back as unpayable later, the customer will be responsible.

West Suburban Bank, a small chain of banks in Illinois, has trained its tellers to do just that – to communicate better with customers when they ask “Is the check good?” or “Has it cleared?” or if there is any other clue that a scam may be afoot. And the bank has gone one step further. Every customer who deposits a check for \$1,000 or more or withdraws \$1,000 or more is handed a flyer about fake check scams.

These efforts are relatively simple and they're paying off. In one year, the bank has cut losses from fake check scams by 85%. And the good will that it has generated with its customers is priceless. Other banks should follow its lead.

We believe that the requirements for fund availability disclosures should be changed to ensure that a more complete and meaningful explanation is provided to consumers.

Complaint handlers from financial regulatory agencies can help to educate banks about the benefits of better communication with their customers and about using the new ChexSystems codes.

We are pleased that so many major financial institutions and other companies joined the Postal Inspection Service and NCL in the recent launch of a public awareness campaign about fake check scams. As part of that campaign, NCL has created a new Web site, [fakechecks.org](http://fakechecks.org). You've probably seen the clever television commercials for it. The Web site describes the most common fake check scams and how they work. There are also answers to frequently asked questions, tests that people can take to gauge their vulnerability to these scams, and humorous Webisodes, mini-videos showing an actor trying to con people in person with a fake check.

There is a link to our online fraud reporting form and there is also a link to a Spanish-language version of the site. We welcome your referring consumers to the site for more information about these scams.

NCL produced a brochure, which is currently being revised, about fake check scams with the American Bankers Association. It is available for banks to purchase from [bankstuffers.com](http://bankstuffers.com).

There are also educational materials that were produced for the public awareness campaign that banks, consumer agencies, and other organizations can use. I can put them in touch with the appropriate person to get the disc containing those materials.

I appreciate your giving me the opportunity today to offer some examples of what banks can and should do to protect consumers from fraud. It is their responsibility, but it's not their's alone. All of us – consumer organizations, regulators, and the various businesses whose services are used to carry out these scams – have a responsibility to try to curtail fraud. By sharing information, discussing problems, and finding common ground

on practical solutions, we can help consumers avoid financial losses and give them more confidence in the marketplace.

I'd like to thank the OCC in particular for inviting me today and for sponsoring tips about ID theft and other subjects in NCL's consumer calendar. And thank you for the work you all do on behalf of consumers.

###