WORKING WITH CORPORATIONS ON CASE INVESTIGATIONS

INTRODUCTION

Our third panel, coordinated by Hedda Litwin, discussed the relationship between prosecutors and private industry in the context of cases involving Internet victimization.

Unlike the first two panels which focused on prepared questions and intermittent responses from the panelists, Panel 3 gave each panelist an opportunity to present information related to their particular employer or industry. This was followed by a more general dialogue that facilitated the exchange of ideas between industry and prosecutors. As such, what follows is the edited transcript of Panel 3 without a particular list of questions preceding it.

Marc M. Harrold

---

1 Cyber Crime Counsel, National Association of Attorneys General (NAAG).
2 Senior Counsel, National Center for Justice and the Rule of Law; Visiting Professor of Law, University of Mississippi School of Law.
PANELISTS:  

- Jack Christin, Jr., Senior Regulatory Counsel, eBay, Inc.  
- John Deerin, Vice President and Director of Security, Bank of Tampa  
- Mike Robinson, U.S. Anti-Piracy Director, The Motion Picture Association of America  
- Thomas Sadaka, of Counsel, Berger Singerman, former Assistant Statewide Prosecutor, Office of the Attorney General of Florida  

JACK CHRISTIN: The defendant in this case got a rude awakening one morning from Lieutenant Dermot Quinn of the Massachusetts State Police who works at the Attorney General's office. The defendant sold four cars on eBay, but didn't deliver them. It was a classic non-delivery case, although it was substantial because it involved thousands of dollars. Four people in four different states bid on and won the cars, but they never got them.  

We worked with the Attorney General's office and gave them all the information they needed to know about this defendant. While I don't know his current status, I know he was arrested and will be prosecuted.  

I do want to touch on what we call the "scourge." I think I can speak for the panel that phishing and spoofing e-mails are a real headache for corporate America. It angers us because of what it does to our good names—whether it's Bank of America or a smaller bank such as Tampa Community Bank. In this case, it's the good names of Washington Mutual Bank and PayPal. Basically, phishers take our name and our logo and send out an e-mail which says, "You need to update your account with us. Go to this page," or "Put in your user ID and password, and we'll make sure that your account remains open." Of course, there's a link to a fraudulent spoof site.

---

3 It should be made clear, at the outset, that the statements and opinions offered by the Panelists/moderator are solely their own and are not offered on behalf of any organization or agency.
We do a great deal of consumer education. We work with Digital PhishNet and law enforcement to try to stem the phishing problem. It still remains a problem because there are people out there who perhaps haven’t been educated about these types of e-mails and who may fall victim to them. So it’s a serious concern.

Here’s an example of an eBay spoof site. Like other corporations, we ask anybody who gets a spoof e-mail to report it to us at spoof@eBay.com or spoof@paypal.com. We have a security team that works very hard with the ISPs and hosting sites to get these sites taken down. It’s effective in a way because it gets them taken down. However, there are 100 other spoof sites going up every time you take one down.

So we’re trying to work with law enforcement and other private entities to deal with this problem. We worked on a case involving spoofing and phishing with the Romanian authorities, the State Department and U.S. Customs. It was basically an Eastern European Internet fraud ring headquartered in Romania. They dealt in stolen credit cards and all sorts of stolen identity information, as well as spoof sites and spoof e-mails. Eleven people were arrested last year based on an investigation in which we, as well as other private organizations, provided assistance. I think it’s a good example of how we work to stop phishing.

This case is placed at the top of our police blotter to send a signal to our community that we are working on this issue and that we do take it seriously. We can’t just turn our backs on the phishing and spoofing problem. I think it’s important for the private sector to make sure that law enforcement has the information they need to pursue these types of cases.

Finally, I think we’re the only company that actually sends a survey to law enforcement to ask how we did when responding to their request for records. The scores could always be better, but they’re usually in the high fours.

Basically, we want to know if you’ve had a problem reaching us, because we want to make it easier for you. If you weren’t satisfied with the timeliness of the response of the FIT team, we want to know because we want these bad guys off
our platform and prosecuted. There’s no gray area here. We want them in jail, so we want to work with you to do that. We send out the survey to make sure that we’re doing a good job.

We tell all our customers that we would never send them an e-mail which asks them to go to another web site. For example, we’ll send a monthly billing summary from eBay showing the account activity, but it doesn’t ask the user to go to another web site. It doesn’t ask for any information. It’s just a billing summary.

As much as you want to educate people and make them savvy, sometimes they then take a position that they’re going to delete any e-mail from, for example, a Bank of America, PayPal or eBay. I think that’s part of the reality of the phishing problem.

I don’t have any statistics on the number of people who actually fall for these scams or the amount of financial damage it does to our companies in terms of loss to our members. When we think about corporation victimization, we tend to think of it in terms of our members being injured, not us. Obviously people may try to do harm to our platforms directly, but my focus is on our community members either being injured by another member or by somebody pretending to be us in the phishing/spoofing context. I don’t know if there’s a dollar figure. The problem is that a court may say, “Who lost money here? Who was financially injured?”

We’ve established a good relationship with the Romanian police because a good deal of phishing originates in Romania. Part of the problem is basically the jurisdictional challenges in dealing with another country. Obviously they have their own priorities in terms of law enforcement. It might not be a priority for them to go into an Internet café and take down phishers when they have violent crime on the street corner. However, they have been responsive because they know it’s a problem. They understand that it’s a serious threat to the health of the Internet worldwide. They’re becoming a more modern country, so they’ve been very responsive. They worked on the case that I highlighted in conjunction with the State Department and Secret Service.
Digital PhishNet is a very good group. It's a consortium, and they share information and try to understand how we can work with law enforcement. Phishing and spoofing seem to be either international or federal, for the most part, but it's also happening in the United States.

Our first step is to get a phishing site down. We want our members to report the site to us. If we have information, we send it to law enforcement and basically say, "Here's a phishing case that needs to be pursued. It's a hot topic and needs to be addressed."

We have a very talented security team. They're very good at trying to trace e-mails but, like anybody else, we're limited in terms of our ability to do that. Sometimes it's based on how clever the perpetrators are. Sometimes it's based on resources. We have our contact information in a brochure, which also includes a detachable rolodex card. We're trying to make it as easy as possible for law enforcement to know how to contact our FIT team.

In 2002 eBay bought PayPal, so for the purposes of law enforcement, we're the same company. PayPal functions as a money transmitter, so many PayPal transactions have nothing to do with eBay. In terms of eBay, about 95 percent of eBay listings offer PayPal as a payment service, so if law enforcement is dealing with an eBay fraud case, there's a strong likelihood that PayPal will be involved as well.

Providing useful victim information to a law enforcement agency that is investigating fraudulent behavior by someone involving eBay and PayPal is key to our commitment to fight fraud by assisting law enforcement. We will search both PayPal and eBay records at law enforcement's request and will determine the identifies of the victims for the agency involved. We will also disclose the name of any agency with which a victim has filed a complaint, whether they contacted an Attorney General's office, the Internet Crime Complaint Center or any other law enforcement entity. We will give all of that information to law enforcement so that it will help in building the case.

We have a Security and Resolutions Center is on
eBay.com, with a prominent link to the Center at the bottom of every page on the eBay site. I urge everyone to take a look at it. It has a law enforcement page that addresses how to contact us. I also have a colorful two-page brochure which summarizes the information available to law enforcement from eBay and PayPal, as well as how to get it and how long it takes for us to send it. If just basic identifying information for a seller is needed, we can probably get that to law enforcement in three days. If it's a total listing history and PayPal history for a member, that might take two weeks. It just depends on the volume of requests that we're getting and how badly the information is needed. If it's really needed in a week, call me or the FIT team, and we'll do everything we can to get it. This is one-stop shopping on how to get information from us and what can be expected in terms of the timing.

This discussion is somewhat of a law enforcement DNA of eBay and PayPal. Since we knew that we were going to have relationships with law enforcement, we knew it was important to have former law enforcement people on the team. As an example, we have on our team a former member of the Australian police; we have a former investigator from Scotland Yard; and we have several former Assistant U.S. Attorneys. I think it gives us a culture of understanding of the challenges that law enforcement faces. We literally have been there in investigating these types of cases, so we can be sensitive to law enforcement's needs, and we can make sure that we work with law enforcement and that law enforcement gets what is needed from us.

For example, if one wants to get the Ohio Attorney General's attention, one way to do it is to sell $60,000 worth of Ohio State football tickets on eBay and not deliver them. Last fall when Ohio State played Michigan, Mark West posted several listings for tickets. People bought them; he never delivered them. He took off to Florida. eBay got complaints, such as, "I didn't get my tickets. The game is in three days. He told me he'd have them to me a week before the game." As we got complaints, we saw a pattern of behavior by this eBay user ID that concerned us. We called the Ohio Attorney
General's office, which is another example of the FIT team being proactive with internal information. They were already investigating the situation and preparing a request to us for information. However, we called them and said, "We've got a seller who we think is in Ohio. He's selling Ohio State football tickets." We were able to get them information. West just took off for Florida and was on the run for two months. He was arrested at a bar in Florida in mid-January and is now awaiting trial. The Attorney General's office is handling that case.

Here is another example of how we work with both federal and state law enforcement. Jeff Lee was selling pirated DVDs. The Ashland, Massachusetts Police Department got a tip that a person was coming into his local post office about five times a day and getting an unusual amount of packages from China. The post office thought it was suspicious and thought the police might want to investigate. The police theorized that he was getting pirated DVDs, which turned out to be true. He was selling them both online and offline. He was listing many of them on eBay. U.S. Customs in Boston contacted us with a fax request. We sent them all the basic fax request information. They developed the case and realized that he was a serious seller of pirated DVDs. Two weeks later, they subpoenaed us for his entire eBay history—everything involving PayPal. We gave them all the records pertaining to Jeff Lee. He's currently awaiting trial on these charges.

MIKE ROBINSON: Movie piracy is not just about actors, actresses and directors. It's about hundreds of thousands of people in every imaginable walk of life who are associated with and who make their living as part of the film and movie industry.

So it's not just the actors that are losing out because of movie piracy, it is truck drivers; it is painters; it is electricians; and it is seamstresses who are hurt by it. Of course, it's about actors and actresses-creative talents who want to get their artistry out in front of the public. However, at the end of the day, it's also about paying your bills and putting enough food on the table.
I think many pirates or the public in general have the conception that movie piracy is doing a service to these artists because they’re getting more people to see them on screen. They think that it is a good thing, but it’s not. The fact of the matter is that piracy is big business and is becoming more sophisticated. Pirates are smart, well-organized and well-funded. They also use their funds to perpetrate other crimes against us and the public.

So how does piracy occur? It’s very rare that we lose money when a movie is in production, but you can almost guarantee that as soon as the movie hits the theater, it will be stolen. It will be stolen in this country by someone in the theater recording it with a camcorder. You may think, “Who would buy one of those movies recorded with a camcorder?” Frankly, they buy them because of the sophistication of camcorders and their ability to record movies with good quality in a theater. Now that they tie into sound systems for the hearing impaired, they also get a good soundtrack.

We track movie theft. When we have a movie that was recorded by a camcorder in a theater, we can track that back to the specific theater where it was recorded. That’s because studios watermark all of their films and mark them differently, so you know the exhibitor who got a particular copy of a movie. You can say, “This was recorded by a camcorder at Cinema 12,” and that’s very helpful.

We don’t lose many movies during the marketing phase. All movies are rated by the Academy of Motion Picture Arts and Sciences for awards purposes. We also don’t lose many movies in non-theatrical efforts. However, we lose them just as soon as they are released on DVD.

The problem that we have with films that make it to theaters, both in this country and around the world, occurs when they are shown. The theaters receive normal reels of film, generally about eight to a movie. As the industry moves toward digital technology, and theaters move from reels to digital showings, it will obviously compound our problem.

There are generally two kinds of pyramids to the piracy problem that we address. First we look at the online side-the
release groups that get the material and send it to the consumer through peer-to-peer networking. Then we look at the side that we call hard goods, where they actually duplicate movies and put them out on the street through couriers and distribution networks. It is very similar to what drug traffickers might do in a distribution network to get drugs out for sale.

I'm going to focus my remarks on that pyramid on the left side—the Internet side of the problem. There is a great deal of sharing of content back and forth as we move down those streams. Where we're beginning to see more problems is in the online sales of pirated goods through web sites that are set up just for that purpose. I'm going to talk about two things. I'll talk about the method by which these encoding groups get the films to the peer-to-peer groups. I'll also talk about the pirate web sites on the Internet and the actions we're taking against them.

These groups are very sophisticated and bold. They actually try to recruit people who are in the movie business. These are the people who remain at the very top of that left pyramid, and these are the people who are getting a copy of the film, either in this country through a camcording or a DVD release of that movie, or from another country through a showing and release. They often put the film together with an audio track from another country, or they put it together with several audio tracks in different languages for redistribution around the world. This can be done in a matter of hours.

These groups are very sophisticated, and they're very small. They may contain only six or a dozen people. While they may never meet one another physically, they've met one another over the Internet and through chat rooms. They do their research about one another. You have to get into one of these groups through references and other connections. It's a very sophisticated and difficult operation.

We have within the Worldwide Anti-Piracy Office an Internet piracy program that tracks and investigates this type of activity on an international basis. The United States program also has Internet software that studies the crimes that
are being perpetrated in the United States. Since the Internet knows no international or state borders, these investigations are obviously very difficult to conduct.

The perpetrators move the copies after they have synchronized them with audio or stripped off the watermarks. They’re getting more sophisticated at stripping off the watermarks or stripping away the protections that we have on DVDs. Then they push the films out to their sites and then rapidly onto peer-to-peer sharing networks. You then have millions of people able to access that material, in many cases within a matter of minutes.

The studios really rely on what they call their “tent-pole productions,”—the movies that they are going to make and that are going to carry them through the year. For example, “The Chronicles of Narnia” and “Mission Impossible III” are coming out. We watch very closely to see how rapidly those movies are stolen and how rapidly that material ends up on the street.

These groups even rank themselves as to how good they are. They openly brag about how well they have conducted their business. A television showing of, for example, “24” on the East Coast will be encoded, downloaded and available on the West Coast within minutes after its completion.

The groups use IRC channels and also specific sites: eDonkey, eMule and BitTorrent. Since I came on board at the Motion Picture Association, we have taken a BitTorrent operation down in Sweden that had millions of users associated with it.

Obviously, these people are much more sophisticated than the average Joe. The average Joe might be able to put 50 movies on his system, but these other systems may have as many as 10,000 movies available for peer-to-peer distribution and downloading. It’s a serious issue.

The other serious problem is that we find some of these top sites are actually housed within corporate America. That’s due to the fact that if you get into these systems and see the advertising, and if you have large system capacity, you can set up within a corporate system where you have control, or you
can plug into a university or corporate system. We find many problems here because of that capacity.

There are piracy web sites, and the average person really can’t tell that these sites are marketing bad CDs. However, there are some tell-tale signs. The movies they’re marketing are still in theaters, and they use different selling prices which are tied to the quality of the DVDs that they market. They also have bad grammar because many of these sites are outside of the United States, and so the language translation is not always as smooth as it should be. Another sign is that you have no physical address if you want to get back to them.

The MPAA sends out thousands of letters every week to ISPs about sites that we have identified as problems to us and that should be taken down. I have to commend eBay and PayPal because they have been fantastic in assisting the Motion Picture Association. For that matter, they have been very responsive when we have identified someone on their system who is dealing or marketing pirated movies and music, as we work very closely with the Recording Industry of America as well. They help by closing the PayPal accounts of these pirates. The average person who goes to one of these pirate web sites sees that they can pay by Visa, MasterCard or PayPal, and that adds another sense of respectability to that site. The assumption then is that it must be okay or these sites would not be allowed to use Visa or MasterCard. I wish that was the case. We have had much better luck with PayPal and eBay than with some others in shutting down their accounts and systems.

Here are some of the questions that concern us. Are there ISP sites operating which are nothing more than pirate havens? If so, are they set up the same way as some flea markets or swap meets, or are they like some buildings in New York City which only house dealers of counterfeit goods? Is it only another marketplace for these goods? We’re looking into that right now. As we identify targets that have a consistent problem, or that continue to deal in these goods, we may come to law enforcement for assistance.

We’re working on some cases, such as in New York City.
The Motion Picture Association, the recording industry, Louis Vuitton and other brand owners have been into some buildings on Broadway in New York City with law enforcement time and time again, and yet they continue to operate. The owners and landlords of those buildings continue to allow pirating activity to occur. We need to investigate those building owners and perhaps put them out of business, instead of only investigating the marketers within those buildings.

It's the same way with those ISP sites. If we identify certain ISPs that are consistently a problem, there are people at those ISPs who we will want to go after, and we will ask law enforcement to help us.

How profitable is piracy? Why would you want to run a methamphetamine lab with the danger of blowing yourself up, or with the smell that makes it easy to be caught, or the penalties associated with that crime, when you can make more money with less risk by setting up a DVD burning tower in your bathroom? Well, guess what? Some people have asked themselves that question, and they've come up with the “more money less risk” answer. We're seeing gangs and other organized criminals migrate to movie and music piracy as a way to fund their other criminal activities. It's been a consistent and frightening pattern because we've had some serious threats made against our employees in other counties. We've also seen serious threats made against law enforcement people who have engaged in investigating these cases.

So it's a serious problem for all of us. There is also a link to terrorism. I believe there was an indictment unsealed recently in Michigan about a terrorist connection to pirated cigarettes and other illegal activities in the Dearborn area. The investigation on that case actually started while I was the State Police Director in Michigan. We worked with federal law enforcement agencies on it. After I came to MPAA, I saw that those same people we investigated in Michigan are now engaged in movie piracy as well, so there is a connection with terrorism. Piracy is not a harmless crime. It's not a crime that any of us can turn away from and consider as a minor offense.

One of my objectives in coming to MPAA is to convince
law enforcement that when they drive down the street and see someone selling pirated movies, they don't say to themselves, "Oh well, at least he isn't selling crack," and drive away. Piracy is a crime that's connected to terrorist activity, and we have to do something about it.

Obviously we can't do it without law enforcement's help. After 40 years of public service, I know what it's like to be in law enforcement's shoes. I know what it's like to have tight budgets and plenty of work and to not always have the resources needed to get it done. While we can't do the job without law enforcement, there are some things we can do to help on these investigations. We do research and analysis every time we see a new title that has been pirated, every time we see that title in another location and every time we see it in another country or state. We sample copies of disks. There are two ways of copying a disk. One way is by duplicating it by going through a presser machine. We take samples and exemplars from all of the pressing equipment around the world.

JOHN DEERIN: From a case management standpoint, the financial security business hasn't come very far. We continue to work on it, but the large banks are much more involved than the small banks. From a criminal referral standpoint, there are no dramatic improvements in working with law enforcement and referring cases. Here and there, we do things a little better.

How big is the problem? You hear astounding numbers put forth. I heard a number from an international security expert a month ago who said financial fraud is a three trillion dollar business worldwide. How do you come up with these numbers? How does someone calculate three trillion dollars? Could it be $2.5 trillion? Could it be $3.2 trillion? Let's just all agree that we know it's a big number. When you talk about fraud, it takes on so many aspects and makes a huge impact.

We take significant, hard losses that threaten our reputation. It's not just the corporate entities that take those losses. Those losses eventually are passed back to the consumers.

In the banking and financial industry, it's very sexy to
talk about Internet fraud. However, counterfeit check fraud is really hurting banks. One bank recently returned $803,000 in counterfeit checks during a one-month period. Another bank reported $1.2 million in counterfeit Canadian checks that had been deposited into United States accounts, again just in one month. These are statistics that I got from the American Banking Association recently. The numbers are incredible. One bank reported a 2,000 percent increase in check fraud between 2000 and 2005. These numbers tell us we need to do better. We need to do things differently. We need to “step out of the box” and figure out what’s going on.

Who’s the victim in the banking business? The victim is either the bank, which takes the “hit,” or the customer who doesn’t get the money back from the bank. Everything is about claims. The customer will eventually go to the bank and say, “Someone made this unauthorized transaction for $700 against my credit card or against my bank account. I want my money back.” Most of the time, the bank will have to give them their money back. However, many times, particularly as it relates to check fraud, the bank will utilize numerous defenses under the Uniform Commercial Code, and will not give the customer their money back.

For law enforcement, there’s a learning curve as to the identity of the real victim. The financial institution is a victim because if the customer must be reimbursed, the institution has to give them the money back. The customer is the victim if the financial institution denies the claim for reimbursement and the financial loss is shifted back to the customer. The victim is also the customer if he or she has been swindled or duped and has sent authorized funds to the fraud perpetrators. The bank is not going to take that loss.

The victim can also be both the bank and the customer if they’ve both been duped by some sort of phishing scam and have sent the money themselves. If the bank has paid that debit or check, and the account is now overdrawn by $4,000, the bank is out $4,000. The bank will pursue the customer to get that money back.

How are fraud schemes reported? Victims generally have
little knowledge of, or the ability to properly report, these crimes. Often the actual crime will be outside of the jurisdiction, and the victims will clearly be frustrated, both with the banks and with law enforcement as to what they need to do.

Some financial institutions have very well organized fraud departments. They’re very effective in helping customers in fraud situations and directing them in the right places. However, many of the medium and smaller sized banks, and even some of the large banks, don’t have good programs to ease their customers through these frustrations. Financial institutions will vary greatly in their ability and effectiveness to report these crimes. Some of the fraud departments in big banks work very closely with law enforcement, so they can be effective.

Many banks don’t even have security departments, or even full-time security people, so they obviously won’t have a knowledge base of what they or a customer needs to do in a fraud situation.

Many of the larger financial institutions, by the way, utilize very significant thresholds, and they won’t even get involved in a case unless it’s over $5,000 or $10,000. Obviously they’ll take a look at the circumstances, but it’s very difficult to develop fraud suspects, and the criminals know it. If it’s under their particular threshold, they just simply don’t have the ability to handle the case, and they’ll charge it off and walk away from it.

The mechanism by which financial institutions are required to report crimes is through the suspicious activity report, or SAR. It is required by the banks’ regulator to be filed with FinCEN, the Financial Crimes Enforcement Network, if there is a suspected crime with a loss exposure greater than $5,000 and a suspect has been identified, or a loss exposure of $25,000 and a suspect has not been identified. I can tell you that this law is loosely followed. First, there’s a nebulous nature to loss exposure, so many of the large banks, unless it’s a hard loss of over $25,000, may not complete a SAR on it. Many of the smaller banks probably are more diligent.

We file thousands of SAR reports electronically to
FinCEN, and then FinCEN redirects them back to the applicable federal agency, whether it's the Secret Service, the FBI, ICE or another agency. The agency will have its own intake process when they review these. As we know, a U.S. Attorney will not pick up the case for prosecution, or won't do much about it, if it's not over a "gajillion" dollars. That's the way the SARs work. You have to remember that these are only for fairly significant cases. The numbers don't include all the $800 or $3700 counterfeit check fraud and credit or debit card cases. These files alone represent fairly large loss numbers.

There has been a significant increase in the number of SARs since 2001. That increase was specifically related to September 11 when the government told banks that they needed to do a better job of monitoring cash activity and the money laundering potential. Banks obviously began to comply more than they had done previously and started overfiling these SARs. In 2004, banks filed 381,000 SARs, but in 2005 the backlog was so large that the government backed off a bit. Now you see that money service businesses, which include check cashers and other like businesses, are required to report SARs.

I'm told that the SAR database will be made available to state law enforcement. I believe that in some states it may already be available for data mining by state law enforcement. The proviso is that from a fraud standpoint the information in the SAR may not be relative to an investigation or case. However, it's certainly a resource to review.

A good point was recently made that while financial institutions spend so much time preparing these SARs, and rarely will they receive contact back from law enforcement to say that they've looked at or are working on this SAR. It's always good for law enforcement agencies and prosecutors to work closely with the company, whether it is a financial institution or another entity, which has reported a crime to them. Even if a decision to prosecute hasn't been made, it gives the entity a feeling that their actions have done something as opposed to just going into a black hole.

Where does all the money go? We know about the day-to-
day street level activity. Counterfeit check fraud, for instance, often goes just to support street level drug habits or lifestyles. We know that the large dollar financial crime has certainly been associated with international terrorist activity, particularly the large amounts of financial fraud in Florida in the early 1990s.

It's a systemic problem. Financial institutions for too long have just charged losses off, and it still continues with little or no effort to productively pursue the perpetrators. We charge losses off too quickly. For example, if you call American Express and say, "I didn't make this charge," it's off your account in two minutes and charged off. We just have to take more ownership of the problem.

That's one problem. Low to mid-level white collar crime generally brings minimal punishment compared to other crimes, so the low to mid-level perpetrator sees substantial and immediate reward with low risks. For us, it's a bad combination. The banks are quickly walking away from it. Secondly, on the prosecution side, the statutes, particularly the lower level statutes covering such things as check fraud, carry insignificant penalties.

A large financial institution even today will charge off, for instance, $30 to $40 million in their state alone in check fraud. That's how big the numbers are. Approximately $40 million a year in the state of Florida alone has been charged off to what they call "non-credit losses." A large portion of that is fraud-related; more specifically, check fraud.

When I first started as a credit card fraud investigator, fraud losses were less than one percent of your credit card portfolio. That was considered to be tolerable. The actual collection or the charge-off or delinquency number was about three percent. Now three percent is considered tolerable for fraud losses and five or six percent is tolerable for credit losses. There is just too much tolerance of these kinds of losses.

What are we doing about it? Prevention is the absolute key as opposed to chasing after it. We are continuing to develop banking industry systems to detect fraud early on. The artificial intelligence type of systems try to evaluate a
customer’s activity, and if the activity falls outside of the parameters, the customer will be contacted. We’re doing better. There’s a reconciliation system and the more the bank can sell that, the more they can help their customers. Right now the benefit is on the business side. Businesses will send in their issue file, or all the checks that they’ve issued that particular day. When the checks come in to clear through the bank, they will reconcile them against one another. Those are the kind of things that are going on to prevent losses.

We have to do a better job of making our customers aware of the scams and advise them not to enter their pin number on a phishing site that asks for their bank account information or pin number. That’s a critical area in which banks and the government have to do better.

We try to work with law enforcement. We try to recover the money while it’s still in the stream and trace the losses. We win some battles, but we’re probably not winning the war.

When bank security folks get together, we always tell each other that if we could identify the top ten perpetrators, and we could get law enforcement and prosecutors to take them out, we could reduce 60 or 70 percent of the fraud that’s occurring. We haven’t been able to do that. I think we need to look more at identifying those top ten players and try to maximize the penalties on them when they are prosecuted. How successful has prosecution been? It’s been occasional and sporadic. Many times, a defendant, particularly in check fraud operations, is recruited by the leaders of the organized rings. It’s really hard to get to those key perpetrators.

Jurisdiction is the number one barrier. I think we need more permanently established task forces to deal with this multi-jurisdiction activity. We have too many police departments and law enforcement agencies. It’s very frustrating for banks and customers. There are twenty law enforcement agencies the nearest two counties to my bank. There are staffing inefficiencies at both financial institutions and law enforcement. Sometimes we’ve had a $20,000 fraud case with good evidence that we’ve been trying to refer to a police department. It’ll just sit there, and the police won’t do anything. You
get very frustrated. Then you'll get a detective who will call you about his case about a $300 check that was cashed. It just doesn't make any sense. I guess there's an obligation on their part to take the cases as they get them, but we just need them to do better and attack the big cases.

Is there anything else we can do? We need to manage our cases better, both on the bank side and on the law enforcement side. We really need to attack these cases in a more organized and efficient way instead of chasing $300 checks when we have a $20,000 case over here. We need to prioritize. We need to utilize information-sharing databases, like the SAR database. Prosecutors need to share intelligence information on these bad guys to try to determine the identities of the top ten players and go after them.

Fraud-Net was actually established in Florida and then adopted first by the Florida Bankers' Association and then by the American Bankers' Association. It has become fairly successful in Florida. Both the Tampa Bay and Miami Dade regions, for example, have their own grouping. When they click on the Fraud-Net site, they will see listings of all the alerts, organized by the type of fraud or crime, such as check fraud or ATM/debit card fraud. It really is a great tool with which to share information between the private sector, financial institutions and law enforcement. It also has a directory where law enforcement can find the bank or the contact they need, or one can go on the law enforcement side and find out who's working on economic crime at that particular agency. It's been very helpful.

I would recommend that prosecutors identify and focus on organized activity within local and regional jurisdictions. Reconsider the multi-agency task force. I'm sure that many Attorneys General are trying to get their legislature to increase the penalties on these crimes.

We haven't seen the breaches of computer systems that many of us have been lead to believe have occurred. Most of the crimes that financial institutions face concern check fraud and counterfeit credit cards.
MIKE ROBINSON: Training for law enforcement is extremely important to us, whether it be for high-tech task forces, beat cops or other organized crime investigators. We would like to do more training with prosecutors and courts, quite honestly so that they understand the significance of the problem.

We do a great deal of the investigation ourselves before taking a case to law enforcement. We work through a network of over 100 private investigating firms in the country that we monitor very closely. They work on our behalf and have been very productive.

We'll provide some legal support as well. One ongoing project that we have goes through cases to develop some case history for law enforcement, so if we get a call from a prosecutor with a specific concern about a case, we can relay information about cases that have been adjudicated in other jurisdictions as well as contact information within those offices.

Public relations and public education are extremely important to us. We have a very aggressive program now that is targeting colleges and universities because a lot of activity is going on there. We also have an outreach program for school-aged children which tries to educate young people before they get involved in this illegal activity. We're here to assist in any way that we can.

We're working on a report right now that indicates that every business where cash money is handled has the potential for illegal activity, whether it's cigarettes or handbags or movies. We want to verify the facts that are reported in print in congressional testimony and other locations before the report is released.

We work very closely with the Recording Industry Association of America because there isn't a single location we go into that is selling movies that isn't also selling pirated music. We actually have three joint offices with the RIAA in Miami, Atlanta and Chicago, and we are about to open a fourth office in Boston.

The United States Chamber of Commerce has become very aggressive on behalf of their members where violations of
intellectual property rights are concerned. We’re working with them and their membership so that we’re not all running after law enforcement or prosecutors and pulling you in different directions when we all have the same goal in mind. You’ll see us doing more of that work together. We’re about to start a very aggressive effort in the Southwest border states in regard to counterfeit goods and property that are entering the United States and then being shipped to other locations. So again, we appreciate your help.

MPAA has offices in Washington D.C. where our state outreach program is managed by Vance Stevenson. He’s worked with states across the country to get state statutes enacted and to increase penalties for those crimes and move them from misdemeanors to felonies. I think there are only five states where we do not have an active program right now.

One other thing we do for prosecutors and law enforcement is that we can get the necessary records from the studio—the owner of that property—and they may possibly be available to testify on the value of the loss. That’s a difficult thing for us to put together, but we will do that.

JOHN DEERIN: I’ve been in the financial security business for almost twenty years. Before that, I was a beat cop for ten years. Then I worked for Barnett Bank, which became Nations Bank, which then became Bank of America, for 15 years. So I have worked in the corporate security group of the “as big as you can get” bank situation.

Then in 2002, I got a call from this local community bank which was also the 12th largest community bank in Florida, located in Tampa. I joined them, and now I’m working in the community, which really represents a much greater number of the banks that you would deal with on a daily basis.

So I’ve worked on both sides of the financial security business, and each gives you a different perspective. As a matter of fact, when I left Bank of America in 2002, we had 350 employees in our corporate security group. At the Bank of Tampa, we only have one, but it’s kind of fun.
JACK CHRISTIN: I came to eBay in 2004 from the Attorney General’s office. Basically, my job at eBay is to be law enforcement’s point of contact for any questions or concerns about things that you see on eBay, whether it be about sellers, buyers or the PayPal platform.

Our Fraud Investigation Team, or FIT, members investigate fraud on the eBay platform. This is a very dedicated group of about 20 individuals located in San Jose and Salt Lake City. Their job is to respond to law enforcement requests for information, whether it be by informal letterhead fax request, a subpoena or a search warrant. They have the tools to go into our systems and get everything needed by investigators and prosecutors to bring a case.

FIT doesn’t just do responsive work. FIT actually does a good deal of proactive work in terms of taking referrals from inside the eBay or PayPal companies and from sources other than law enforcement and trying to detect and identify fraudulent behavior that involves our platforms. In many cases, they refer a case to Attorney General offices rather than just reacting to requests.

FIT investigators also will testify in court to support your cases. In other words, they will do whatever they can to support investigations that involve eBay and PayPal. It essentially tells our community, “We will work with law enforcement and share information with law enforcement where appropriate—not third-parties or private corporations—but law enforcement agencies. If we get a verified request from law enforcement on their letterhead asking for information as part of an investigation, we will share basic information with them about you and about your conduct on eBay. If they need more information like credit card numbers or Internet protocol data, we will require a subpoena. We’ll give them basic information to help them at least initially start their case.”

Regarding PayPal records, anything that you need on the PayPal side requires a subpoena. PayPal is a money transmitter service, and thus involves our members’ financial information. In that case, contact me or the FIT team, and you can get it from us by subpoena.
JOHN DEERIN: When I was a credit card investigator, Visa and MasterCard told us in the early 1990s that credit card fraud would be eradicated by 1995 because they had holograms to put on the credit cards as well as more security features. The skimming is what we hear about — whether you go to the restaurant or whether you use your card at a gas pump. Those dollars skimmed are significant.

Right now the emphasis is on money laundering. If a bank has suspicious money laundering cash activity, it’s required to complete a SAR. There’s a strong emphasis, as well there should be, on stopping money laundering, so a great portion of SAR filings are on that situation. As far as actual crimes are concerned — whether it’s bank fraud, check fraud or credit-unless the crime meets those thresholds, a SAR report may not be made.

How many reports are actually picked up for further investigation and prosecution? I can only tell you that we never hear back on any of them, and I file hundreds of SAR reports. I don’t recall ever getting a callback from a federal agent or prosecutor about a case.

TOM SADAKA: If I were to tell you how to streamline your case management and your investigative process into a “bundle” that is readily prosecutable with very little more work that’s required either from the investigative side or the prosecutive side, could we do business today? The “bundles” that are put together by the financial fraud investigators at the larger and even the smaller banks are incredible pieces of investigative work. These individuals are often former trained law enforcement officers. They have access to information within the bank that you could access only with four or five different layers of legal process. They are able to use that information in the development of these investigative reports.

I talked to the head of security at a credit card security conference who told me they can spot a skimmed credit card within three uses and shut it down. So I said, “It would be wonderful if we could have a joint relationship between government and you as the private sector.” He was very much in
favor of trying to develop some type of task force or working agreement with prosecutors and law enforcement. He immediately talked to their vice president in charge of marketing, who said they wouldn’t be interested.

Their loss was $1.4 billion a year. Don’t you think that they’d be interested in doing something when their loss was that high? However, it was a pittance compared to the amount of revenue they had. In further digging down through the system, they wouldn’t be interested because they have little faith in the ability or the willingness of law enforcement and prosecutors to take the investigations in which they participated and prosecute them.

Historically, they had a reason for that. They got very little response from prosecutors when they tried to get these types of cases prosecuted. I hope I am preaching to the choir that we can’t handle these cases without the cooperation of the private sector. What better way than through an organized task force or through a relationship with these various institutions, whether it’s eBay, MPAA or a financial institution such as Bank of America or the Bank of Tampa.

I can tell you from personal experience that I’ve dealt with each of these organizations, and I had glowing praise for them. eBay is incredible. MPAA is willing to put someone on the next plane to fly down to train an investigator on how to work this case. Bank of America handed me an investigation that they had been working on for several years that saved us probably a year and a half worth of investigation and resulted in a conviction of a $13 million identify theft ring based in Miami. It was the Campbell case.

We were able to bring their investigators and their investigative packet before the grand jury and get an indictment with very little involvement of law enforcement. We had a statewide taskforce that was in place that focused primarily on identity theft, so we developed this relationship.

What happened to that task force? As many of you know, law enforcement relies on many positions, such as our community crime investigator or our financial fraud investigator, but the longevity of those positions is rather short-lived. Why?
The computer experts usually go to the private sector where they can make more money. The rest become career law enforcement officers. However, for those of you who understand how sheriff's departments, state police and local agencies work, is the fraud investigator going to be the next captain? Generally not, isn't that right? Instead, he will become a road supervisor or lieutenant. He'll end up in violent crime and then he'll get a position under the sheriff. You will not see the fraud investigator running for sheriff. I'm offended. I'm a fraud investigator. Why is that not a career position? We see it in prosecutor's offices. If you have a well-trained computer crime investigator, they end up getting moved or promoted into another division that deals with sex crimes or other violent crimes.

We need institutional memory. How do you accomplish that except through a task force or some type of joint cooperative effort between the public and the private sector? That taskforce has enough overlap and longevity to remember a specific case. They remember an investigation that might have gone stale. They remember how things were done in the past that were successful. That's really what we need to focus on.

MIKE ROBINSON: Before I joined the TSA, I spent 34 years with the Michigan Department of State Police. Most of that time was spent on the criminal investigative side of the operation as director of the Michigan State Police for nearly 12 years. During that time, I served as the president of the International Association of Chiefs of Police, which really helped me in my current job because it certainly requires a great deal of cooperation between the industry and law enforcement around the world.

I think that there's a misconception held by most people that the movie industry is all about making money. The fact is that the movie industry is as fragile as any other industry in the United States or internationally. Only a few movies ever really make money, and the studios hope that those blockbusters carry them through the rest of the year.

I learned as soon as I left my badge and ID in Michigan
and got into the private sector that there are things law enforcement can do that we in the private sector cannot do. We absolutely need your help. We absolutely need to work cases with you in order to achieve our goals as well. We can't do it without the tools that you have in your toolkit that we don't have.

JOHN DEERIN: The chargeback process is the first step in any type of credit card fraud. Banks are going to take their chargeback rights. It shifts the loss back to whoever accepted that credit card, whether they can get authorization or whether it was an online transaction that wasn't verified through Visa. I'm sure it complicates matters from a prosecution standpoint. The chargeback system has been in place forever and always will be as a recovery methodology.

When I was at Bank of America, we'd get many restitution checks per month in our Tampa office, and they'd all be for amounts such as $27, $18, $22. Restitution is almost a non-event from a recovery standpoint, unless it's a big prosecution case where we're able to get big money in return. The restitution checks at $26 a month don't get them excited.

TOM SADAKA: Frankly, you can't have a financial crime without technology being involved. When you're working with task forces, you have a combination of efforts and talents that will allow you to work these cases successfully.

Every prosecutor knows the Electronic Communications Privacy Act. What does it do for you? It gives you, as a government entity or official, a roadmap on how to get certain information from a provider of electronic communications. Do you have any idea how the people in the private sector can get that same information?

That was a rude awakening for me when I left government service. I had a public company as a client that was dealing with very negative postings about the company in a Yahoo! group. The poster had enough inside information about the company to legitimize what he was saying. It was all untrue. How do you get that information from Yahoo! if you're
not a government entity? I couldn’t send them a subpoena without filing suit. Could I file suit if I didn’t know who it was? Procedurally, I could file a John Doe suit and get the subpoenas required to get the basic information. Then I might have to send another subpoena to find out the IP information and another subpoena to the individual’s ISP to find out the identity of that person. So when the client asks how much that is going to cost, it might be as much as ten grand in legal fees. If we file suit, it will probably cost the client $100,000.

You have a statute that procedurally allows you to follow through. My purpose in discussing this is that when the private sector comes to you for help, and you find probable cause to predicate your investigation, don’t look a gift horse in the mouth when they’re presenting you with the investigative packet. Also, there may be a legitimate need, and that little case may turn into something big. That case may not be a good example of anything other than to show you that it’s difficult to get that information, but in a single online fraud case, there may be something else brewing beneath the surface.

I just encourage you to maintain relationships with the private sector and try to foster task forces. If there are ones that already exist, get involved with them if you aren’t already. If there’s somebody else in your agency who is involved but isn’t really handling those kinds of cases, perhaps it’s time for you to come forward and supplant that person within the task force. You may be amazed at the results.

JOHN DEERIN: I want to clarify that it’s not that we don’t care about restitution, because banks want to prosecute these criminals. From a bottom line standpoint, particularly at the Bank of Americas of the world, they may charge off $40 million. This is their strategy. If you’ve got a $20,000 credit card fraud, and you can effectively chargeback $10,000 of it, that will be your first course of action. At the Bank of Tampa, if you have a $3,000 check fraud case, and you work out a restitution agreement of $100 a month, it’s greatly appreciated. You can only imagine what that $100 check means to
Bank of America. However, if a victim has a $200 bad check, that’s the same to them as when Bank of America has a $100,000 fraud. Police departments can be in a quandary because they can’t decide to work the $100,000 fraud and not work on all the smaller citizens’ cases.

If a bank is not taking a hard dollar loss, they simply don’t have the resources to pursue it. It’s very frustrating to our customers because they don’t understand, even when they’re not out the money either, they’ve been violated.

TOM SADAKA: In an identity theft, the bank doesn’t consider itself a victim, but we still have a victim—that individual whose information was used. Now the bank is a witness in that case, and you can rely on whatever investigative information they have. If you have a task force, such as we have with the Florida Bankers’ Association, prosecutors can go to them to work together. I know that their security people would love to see these cases handled, but not the marketing people. You should work that as a point of communication between you and the financial institutions.

JOHN DEERIN: Some small banks, such as mine, have insurance on their credit portfolios, including their credit card portfolios through their credit card processor and other associations of which they’re members, such as the Credit Union Association or, in our case, the Community Bankers’ Association. This insurance has a deductible, but then you get 50 percent on your losses over that amount.

The realities of the banking industry are that there’s all kinds of internal theft possible. The big banks have huge internal call centers, with 500 to 600 people who have unlimited access. They try some front-end proactive approaches to analyzing who is looking at what information and what they’re doing with it. At the end of the day, the volumes of those transactions that these folks are handling are great. Their capabilities are significant.