Identity Theft Task Force
(Established by Act 140, Session Laws of Hawai`i 2006)
State of Hawai`i
www.state.hi.us/auditor

Minutes of Meeting

The agenda for this meeting was filed with the Office of the Lieutenant Governor, as required by Section 92-7(b), Hawai`i Revised Statutes.

Date: Thursday, August 2, 2007

Time: 9:00 a.m.

Place: State Capitol
415 South Beretania Street
Conference Room 309
Honolulu, Hawai`i

Present: Chair Gary Caulfield, Financial Services Industry
Vice Chair Marvin Dang, Financial Services Industry
Clayton Arinaga, County Police Departments Designee
Senator Carol Fukunaga, President of the Senate's Designee
Fay Ikei, Department of Education
Jodi Ito, University of Hawai`i
Tim Lyons, Consumer and Business Organizations
Carol Pregill, Retail and Small Business Community
Mel Rapozo, Hawai`i State Association of Counties Designee
Robert Takushi, Consumer and Business Organizations
Rick Walkinshaw, United States Secret Service Electronic Crimes Unit
Sharon Wong, Department of Accounting and General Services
Christopher D.W. Young, Department of the Attorney General

Marion M. Higa, State Auditor, Office of the Auditor
Russell Wong, IT Coordinator, Office of the Auditor
Jayna Oshiro, Special Projects Coordinator, Office of the Auditor
Pat Mukai, Secretary, Office of the Auditor

Jeffrey Loo, J.W. Loo & Associates
Joanna Markle, Goodsill Anderson Quinn & Stifel
Jennifer Flynn, Consumer Data Industry Association

Excused: Lt. Andrew Castro, Honolulu Police Department's Criminal Investigation Division
Craig De Costa, Hawai`i Prosecuting Attorneys Association
Representative Jon Riki Karamatsu, Speaker of the House of Representatives Designee
Nathan Kim, The Judiciary
Paul Kosasa, Retail and Small Business Community
Stephen Levins, Director of the Office of Consumer Protection
Senator Ron Menor, President of the Senate Designee
Representative Colleen Meyer, Speaker of the House of Representatives Designee
Tom Terry, United States Postal Service

Absent: Ronald Johnson, United States Attorney for the District of Hawai'i Designee

Call to Order: Chair Caulfield called the meeting to order at 9:07 a.m. at which time quorum was established.

Chair's Report: <u>Announcements, introductions, correspondence, and additional distribution</u>
List of additional distribution:

1. CDIA outline of presentation
2. Social Security Number Presentation to the Identity Theft Task Force

Chair Caulfield thanked Senator Fukunaga's office for providing refreshments. Chair Caulfield also introduced Jodi Ito, Information Security Officer of the University of Hawai`i who is replacing David Lassner.

Chair's Report will continue after the CDIA presentation.

Informational Briefings/ Discussion: <u>Consumer Data Industry Association (CDIA)</u>
Jennifer Flynn, Senior Manager of Government Affairs, CDIA, briefed the task force.

CDIA represents the consumer reporting industry. Identity thefts fall into one of two categories:

- Account Takeover – involves the unauthorized use of financial account information to make fraudulent purchases or steal money.

- True Name Fraud – involves stealing information necessary for opening new accounts in the name of the victim or perhaps creating a new record such as a criminal history.

The Federal Trade Commission (FTC) Synovate data from September of 2003 indicated that account takeover crime accounted for 67.4% and true name fraud crime accounted for 32.6% of all ID thefts.

A recent study from the Javelin Group showed that 77% of consumers believe identity theft/fraud is increasing. However, the rates are actually declining due to more media coverage relating to identity theft.

The FTC Synovate and Javelin survey data showed a downward trend in total victims of identity theft from 10.1 million in 2002 to 8.9 million in 2005. The FTC data also showed that complaints in key categories have held steady or dropped between 2003 and 2005. The FTC Identity theft complaints continue to rise, but the rate of growth has dropped dramatically from 14.7% between 2003 and 2004, to 3.53% between 2004 and 2005.

A case study done in 2006 regarding credit fraud prevention revealed that there were over 33 million in-store credit applications processed by a single lender annually or over 90,000 applications per day. Approximately 60% of all applications, or 19.8 million annually, were approved. There was one fraud account per 1,613 approved applications.

There are several reasons as to the decline of identity theft. Most states have laws that consider identity theft a crime. Credit-reporting agencies will accept police reports as verification that someone has been a victim of identity theft. Most companies and financial institutions will take immediate steps to assist victims with solutions. Most states also have security breach notification laws that require entities to inform consumers when a breach occurs. Hawai`i is one of 39 states that have security breach laws. As of July 2007, the law allows consumers the option of locking down their entire credit report for a nominal fee. No one would be able to unfreeze the lockdown except for the consumer or law enforcement officials. A PIN number or password is required to unfreeze the report.

Some efforts that are driving the positive trends are:

- Public awareness campaigns that financial institutions, federal reporting agencies, legislatures across the country have implemented security measures.
- On September 25, 2005, Equifax, Experian, and TransUnion announced a cooperative effort to adopt coordinated encryption standards that can be used by more than 15,000 data furnishers supplying data to the nation's credit reporting system. MasterCard and VISA have both announced improved data security standards and stronger enforcement efforts relative to the protection of debit and credit card numbers.
- The private sector has offered tools such as credit file monitoring. Millions of consumers are subscribers each year. Consumers are using rights under existing laws. 3,461,571 fraud and active duty alerts were placed on consumer credit reports in 2005. Law enforcement investigations and prosecutions of identity thieves can help. More pressure is needed and more funding for law enforcement efforts as well.

Social Security Numbers: The Only Unique Identifier

Social security numbers (SSN) are the only unique identifier available to everyone. Many state laws require the use of the SSN for a wide range of important purposes dependent on accurate identification. The SSN alone will not cause someone to be a victim of identity theft. If someone steals your SSN, it does not mean that person will be a victim of identity theft.

The Patriot Act requires financial institutions to use the consumer's full SSN, obtained from "trusted private sources" to open an account.

The federal government has enacted the following laws to ensure that consumer's information is kept private:

- Gramm-Leach Bliley Act (15 U.S.C. 6826(b)) = relates to financial institutions.
- Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) = relates to credit reporting agencies.
- Section 5 of the FTC Act (15 U.S.C. 41-51) = certain commercial acts.
- Fair Debt Collection Practices Act (15 U.S.C. 1601 et seq.) = decides how debt is collected.
- Health Insurance Portability and Accountability Act (Pub. L. 104-191) = deals with health privacy and information on medical records.
- Driver's Privacy Protection Act (18 U.S.C. 2721 et seq.) = deals with information relating to driver's licenses.

The beneficial uses of SSNs:

- Access to home ownership
- Child support payment enforcement
- Locator services
- Locating sex offenders
- Employment/security screening
- Insurance fraud prevention

Without the use of SSNs:

- Incomplete data harms consumers
- Incomplete data harms our banking system
- Incomplete data prevents consumer access to goods and services

Member Rapozo stated that the Javelin study was the first study he has seen that showed the rates of identity theft declining. He asked what numbers were used in the Javelin

study. Ms. Flynn stated that she would obtain the information for the task force.

Vice Chair Dang asked what other states are doing about use of social security numbers in court judgments. Ms. Flynn responded that most states have social security numbers on the original documents but redact when the information is transferred or copied. Vice Chair Dang further stated that in Hawai`i, the only requirement that social security numbers be on court judgments is by the Bureau of Conveyances. Ms. Flynn replied that if the social security number does not appear on the judgment, it would not be placed on the consumer's credit report.

Senator Fukunaga asked if the industry is exploring alternatives to social security numbers, such as state driver's license numbers or other identifiers. Ms. Flynn replied, the there is no nationwide movement. State ID numbers are not unique. Even if there is an alternative nationwide identifier, it would have the same issues as the social security number. Databases are all set up for 9-digit national number.

Senator Fukunaga asked from a state policy perspective, if social security numbers are generally used for credit purposes, individuals applying for credit, mortgages, or loans, could voluntarily supply that information. The government should not be the conduit. What are other states doing? Ms. Flynn replied that it is a continuing debate. There are already other requirements that institutions have to follow and most of them require verification from social security numbers. For example, credit reporting agencies must comply with strict regulations about whom, with whom, and when the information can be shared. If the regulations are violated, there are huge penalties. Social security numbers should not be public. It should only be shared with individuals and entities that need it.

Member Lyons asked about the process to freeze one's credit file. Ms. Flynn explained that to freeze your credit file, you contact the credit reporting agency and pay a nominal fee. When you decide to lift it, you need to telephone the credit reporting agency and provide them with your PIN number. Member Lyons asked if the industry ever considered an automatic freeze for everyone. Ms. Flynn said this has been discussed, however, the way the system has been created, car loans, mortgages, student loans, etc. are all done automatically. If everything is locked down, requiring permission from everyone will slow the process down. If a credit file is locked down, anytime you need to open it, it has to be an affirmative action at that point in time.

Member Young asked what the difference was between fraud alert and credit freeze? Ms. Flynn explained that if someone believes they are a victim of fraud, they can call the credit reporting agency and tell them to put a fraud alert on their credit report. The fraud alert tells the reporting agency to double check information or to call the consumer before opening a credit account. A freeze literally locks down everything. There is no information that goes out about you. Only law enforcement or an entity with an existing relationship with the consumer has access.

Member Pregill indicated that credit freezes have been an issue for the retail industry for sometime. If a consumer wants to take advantage of instant credit, is the process to unfreeze a credit file available 24/7? Ms. Flynn said it would be in the future. The situation is currently being addressed. There are three credit reporting agencies and they are very competitive.

Member Young questioned the data that shows that ID theft is on the downward decline and that the FTC is the source of that information. Hawai`i used to be 11$^{th}$ when the FTC started, and currently, Hawai`i is forty something. From the law enforcement perspective, ID theft has not gone down. The FTC complaints data is based on self-reporting, is voluntary, and nothing happens when the consumer reports to the FTC. Ms. Flynn said she cannot speak for Javelin or for FTC specifically but her understanding is they are

taking police reports from states.

Member Young asked how many people are using credit freezes and fraud alerts, because that would be the best indicator where we are on ID theft. Ms. Flynn answered, the number is very small and the information is proprietary. In California, .001% of the population has a freeze on their credit file.

Chair Caulfield asked Ms. Flynn what CDIA is doing in education. Ms. Flynn responded the CDIA is working with a number of state attorney general's offices, and will be happy to work with Hawai`i attorney general's office.

Member Rapozo asked how about CDIA's membership. Ms. Flynn responded that CDIA represents 400 members, including all credit reporting agencies, ChoicePoint, and Lexis/Nexus.

Member Young asked about data brokers online. Ms. Flynn replied the only information they can provide legally is public record information. It would be illegal for them to provide credit card and bank information.

Member Young also asked if the credit reporting companies looked at verifying information before entering it into their system to cut down on fraud. Ms Flynn said the problem is the amount of information that is taken in on a daily basis. Millions of pieces of data come in daily. However, there is a dispute resolution system to correct information in a credit report. It can be done online and the credit reporting company has 30 days to fix it.

Chair Caulfield posed the following series of questions for CDIA:

1. Does CDIA keep track of data breaches? Ms. Flynn said they keep track of all security breaches.
2. Does CDIA have a standard program that says they have to meet certain standards? Ms. Flynn replied that members have to comply with federal and state laws.
3. Of the 400 consumer data companies, credit reporting, mortgage reporting, check verification, etc. are any of them just involved in data aggregation not related to this, where they gather, sell, and buy information? Ms. Flynn answered, yes.
4. Are any of CDIA's members just plain data aggregators that sell information they gather? Ms. Flynn said it may be a small percentage of its members.
5. In the presentation, there was a list of items that would stop commercial transactions. Does the association have examples or suggestions of where social security numbers or other kinds of information should be or should not be in government documents? Ms. Flynn said it is hard to say because there are so many different requirements that they may not be aware of, but it should not be on public websites.

Mr. Jeffrey Loo stated that some states have statutes that would not record a document if the document includes a social security number. What kind of consequences has CDIA seen regarding this? Ms. Flynn replied, if a title is recorded without a social security number, the mortgage company could not resell the mortgage.

Member Young asked about pre-approved credit cards. His understanding is, before someone gets a pre-approved credit card, the credit companies run a credit check on the individual to see what kind of credit they have. Ms. Flynn said credit companies do not run credit checks on individuals. Their offers are based on a pre-screened profile. If consumers want to opt-out of receiving pre-screened offers, there is a number they can call, 1-800-5-opt-out.

Chair Caulfield thanked Ms. Flynn for CDIA's presentation.

Chair's Report:

Minutes of previous meeting

Vice Chair Dang moved to approve the minutes. Member Ito seconded. It was voted on and unanimously carried to approve the minutes.

Auditor's Report:

The Auditor's Office received three responses for Requests for Qualifications for Phase II. Jeffrey Loo of J.W. Loo and Associates, has been selected as the consultant.

Consultant's Report

Jeffrey Loo of J.W. Loo and Associates, consultant, briefed the task force on the following:

He is in the process of putting together a statement of work for Phase II. Phase II will be completed prior to the December meeting to be included in the final report. Mr. Loo stated that the last two chapters of Phase I will be completed by the September 6th meeting. In addition, a section will be included on recommendations taken from the summary of existing practices. This section will be provided at the September 27th meeting. Mr. Loo also stated that he will be working on the Phase II activities that include the analysis on redaction and personal information collected by government agencies.

Mr. Loo also briefed the task force on a handout on Arizona. Arizona is one of the few states that enacted legislation to create a statewide information and security privacy office. Arizona developed a business case analysis to justify the office. The highlight was that Arizona was number one in terms of the states with identity theft incidents and that 60% of the breaches were from university or government sources. They also cited a concern that data breaches cost money to the state. They proposed a three-year phase-in. The first phase involves a risk assessment. Later phases include education and implementation controls. The office will be fully staffed with eleven employees by year three.

Member Wong shared with the task force that there was legislation to establish three positions for ICSD's security office. There was discussion about where to place the positions. In order to expedite the process, they chose to put the positions at the branch level. A division level would have been more appropriate, but would have required going through a lengthy reorganization process. So far, they have filled one position and are still recruiting for the other two. However, to be most effective we would have to get to a point similar to Arizona. ICSD does not have enforcement authority and cannot dictate to other departments what needs to be done. The task force should consider Arizona's approach in creating a separate security privacy office.

Mr. Loo stated at the last meeting he requested the task force members to review the draft report on the first two chapters and provide their feedback. He received comments from two task force members. He requested input on the sections of best practices and trends that should be included in the final report. Recommendations for implementation of best practices in Hawai`i, would be welcomed. At the September 27th meeting, Mr. Loo will present recommendations that will be included in the final report.

Investigative Working Groups – Reports:

Chair Caulfield stated that he had nothing to report at this time. Member Young also did not have anything to report at this time. Member Young is still waiting for suggestions as to type of legislation if any, and has not received any input.

Meeting Schedule:

Chair Caulfield indicated that the October 25th meeting is decision making on any proposed legislation. State Auditor Higa stated that under the task force's requirement, the task force would make its own report to the Legislature from the Auditor's Office. The Office's mechanism for legislation is to have the Legislative Reference Bureau draft the legislation, and including it in the task force report to the legislature. The normal practice is to ask leadership to introduce legislation.

The following are the remaining task force dates:

- September 6th = working group draft findings.
- September 27th
- October 25th = decision making on any proposed legislation.
- November 15th = approve the draft report.
- December 6th = last meeting to approve the final report.

Adjournment: Member Young moved to adjourn, seconded by Member Rapozo. It was voted on and unanimously approved to adjourn the meeting.

With no further business, the Chair adjourned the meeting at 11:20 a.m.

Next Meeting:
date: Thursday, September 6, 2007
time: 9:00 a.m.
address: to be determined

Reviewed and approved by:

Russell Wong
IT Coordinator

August 15, 2007

[ ] Approved as circulated.

ID Theft/080207