



**DAVID Y. IGE**  
GOVERNOR  
  
**SHAN S. TSUTSUI**  
LT. GOVERNOR

**STATE OF HAWAII**  
**OFFICE OF THE DIRECTOR**  
**DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS**  
335 MERCHANT STREET, ROOM 310  
P.O. Box 541  
HONOLULU, HAWAII 96809  
Phone Number: 586-2850  
Fax Number: 586-2856  
cca.hawaii.gov

**CATHERINE P. AWAKUNI COLÓN**  
DIRECTOR  
  
**JO ANN M. UCHIDA TAKEUCHI**  
DEPUTY DIRECTOR

**PRESENTATION OF THE  
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS**

**TO THE HOUSE COMMITTEE ON  
CONSUMER PROTECTION AND COMMERCE**

**THE TWENTY-EIGHTH LEGISLATURE  
REGULAR SESSION OF 2016**

**March 23, 2016  
2:30 p.m.**

**TESTIMONY ON H.C.R. 182  
SUPPORTING THE ADOPTION OF CHIP AND PIN TECHNOLOGY  
BY ALL FINANCIAL INSTITUTIONS TO IMPROVE THE SECURITY  
OF CONSUMER FINANCIAL TRANSACTIONS IN THE STATE**

**TO THE HONORABLE ANGUS L.K. MCKELVEY, CHAIR,  
AND MEMBERS OF THE COMMITTEE:**

My name is Iris Ikeda, Commissioner of Financial Institutions ("Commissioner"),  
testifying on behalf of the Department of Commerce and Consumer Affairs  
("Department") on H.C.R. No. 182. The Department supports this resolution, subject to  
the amendments described at the end of this testimony.

## TESTIMONY ON HOUSE CONCURRENT RESOLUTION 182

March 23, 2016

Page 2

This resolution promotes the safe and sound use of credit cards and debit cards (collectively, “cards”). This resolution would have the Legislature request:

- 1) That all financial institutions that issue credit or debit cards to Hawaii residents or businesses, replace those cards with chip and PIN cards;
- 2) That all Hawaii businesses that accept electronic payments upgrade or replace their point-of-sale terminals to accept payment by chip and PIN cards; and
- 3) That the Director of Commerce and Consumer Affairs transmit copies of the resolution to the five largest financial institutions that issue credit or debit cards and the ten largest retailers in the State.

The Commissioner supports the use of chip-embedded cards for both credit cards and debit cards. Chip-embedded cards are a form of smart payment card. They have an embedded microprocessor chip that encodes the credit card account number and other information that is transferred to the merchant. Each use of the chip on a chip-embedded card use generates a new transaction code. If transaction code information is stolen, the information is useless as it is unique to a single transaction.

Chip-embedded card transactions are verified in the U.S. by the customer’s signature, and the combination is known as a “chip and signature” card. Chip-embedded cards may also bear a magnetic stripe because not all merchants have a chip-embedded card point-of-sale terminal at this time. Magnetic stripe cards store information in the magnetic stripe on the back of the card. Such cards were involved in the massive Target data breach in 2013. Visa and MasterCard asked U.S. banks and

merchants to use chip-embedded cards by October 1, 2015. Those that did not make the switch may have to assume liability for counterfeit fraud.

In Europe, “chip and PIN cards” are widely used. The customer verifies the transaction with a Personal Identification Number or “PIN”. Some chip-embedded cards issued in the U.S. may have PIN capabilities, however, the chip and PIN” combination is not widely used in this country at this time.

Whether chip-embedded cards are verified by the customer’s signature, a PIN, or biometrics, they are considered safer against counterfeit fraud than magnetic stripe cards, because of the unique transaction code that is generated with each use of the chip on a chip-embedded card.

The Department takes no position whether businesses must upgrade or replace their point of sale terminals to accept payment by chip-embedded cards, as there may be a cost of implementation. By now, all businesses should be aware of the potential “liability shift” for “card-present fraud” if they did not implement the new chip-embedded card reader systems or issue chip-embedded cards.

The Department suggests that the resolution be amended as follows:

- 1) Change the resolution’s requests for “chip and PIN” cards, to “chip and signature” cards; and
- 2) Clarify phrases used in the bill.
  - a. First, “largest financial institutions” could be measured by dollar volume, or number of cards issued, or other means.

TESTIMONY ON HOUSE CONCURRENT RESOLUTION 182

March 23, 2016

Page 4

- b. Second, it is not clear whether the institutions referenced are limited to those that are State chartered. DFI is not aware of which nationwide financial institutions issue credit or debit cards to Hawaii residents, nor volume statistics.
- c. Similarly, DFI lacks information to identify the ten largest retailers, as that industrywide statistical information is not determined as part of regulation by DFI or the Department.

The Department supports this resolution, H.C.R. No. 182, and respectfully requests it be passed subject to the amendments recommended in this testimony.

Thank you for this opportunity to testify. I would be pleased to respond to any questions that you may have.

Presentation To  
House Committee on Consumer Protection and Commerce  
March 23, 2016 at 2:30 PM  
State Capitol Conference Room 325

**Testimony in Opposition to House Concurrent Resolution 182**

TO: The Honorable Angus L. K. McKelvey, Chair  
The Honorable Justin H. Woodson, Vice Chair  
Members of the Committee

My name is Edward Pei and I am the Executive Director of the Hawaii Bankers Association (HBA). HBA is the trade association representing eleven FDIC insured depository institutions with branch offices in the State of Hawaii.

The banking industry supports the migration of credit and debit cards to include the EMV (Europay MasterCard Visa) chip. Two thirds of the card fraud perpetrated today utilizes counterfeit magnetic stripe cards embossed and encoded with stolen credit and debit card numbers, from sources such as data breaches. The chip is much more secure technology that will make it very difficult to create a counterfeit card. It should drastically reduce counterfeit fraud. Today, the new chip card can be used along with a cardholder's signature or a PIN (personal identification number). However, new technologies are emerging that will make cardholder authentication even more secure.

The PIN can be helpful in curtailing lost and stolen card fraud, but that only represents less than 10% of the total card fraud losses today. PIN, typically a four digit numerical value, is old technology that is growing increasingly vulnerable to hackers. That is why the industry is looking to new technologies to replace PIN. There are many pilots and programs underway, the most common of which is probably the fingerprint. Retina scans and voice prints may sound futuristic but in fact new applications are appearing everywhere.

In summary, Chip and PIN are two completely separate issues. It is the chip, not the PIN, that makes cards more secure from data hackers and will reduce counterfeit fraud. Please do not commit the banking industry to an authentication technology that is static and outdated. We recommend that this resolution endorse the migration to chip cards but remove any initiative to require the industry to rely on PIN as the authentication technology for the future. With this change, we would support this resolution.

Thank you for the opportunity to offer our comments and please let us know if we can provide further information.



Edward Y. W. Pei  
(808) 524-5161



Testimony to the House Committee on Consumer Protection & Commerce  
March 23, 2016

In Opposition to HCR 182, Supporting the Chip and Pin Technology by all Financial Institutions  
to Improve the Security of Consumer Financial Transactions in the State.

To: The Honorable Angus McKelvey, Chair  
The Honorable Justin Woodson, Vice-Chair  
Members of the Committee

My name is Stefanie Sakamoto, and I am testifying on behalf of the Hawaii Credit Union League, the local trade association for 63 Hawaii credit unions, representing over 800,000 credit union members across the state. We are opposed to HCR 182 in its current form.

Hawaii's credit unions already support the migration of credit and debit cards to include the EMV (EuroPay MasterCard Visa) chip technology. Many of our member credit unions have already updated their debit and credit cards, and many more are in the process of doing so. The chip is much more secure and fraud-resistant than just the magnetic strip, and does help reduce incidences of credit card fraud. Chip technology is new technology which will eventually replace the old magnetic strip and personal identification number (PIN) process which currently exists. Thus, it makes no sense for this resolution to include the PIN process in its language.

Effective October 2015, merchants that have activated EMV-enabled point-of-sale terminals are not liable for fraudulent transactions using EMV chip debit or credit cards. If the merchants do not use an EMV-activated terminal, they assume the liability of fraudulent EMV chip debit or credit card transactions. Therefore, economic incentives for card issuers to issue EMV chip cards, and for merchants to activate EMV chip terminals already exists.

Thank you for the opportunity to provide comments.

LAW OFFICES  
OF  
**MARVIN S. C. DANG**  
A Limited Liability Law Company

MARVIN S. C. DANG  
JASON M. OLIVER  
SUMMER OKADA  
PAUL T. HOLTROP  
RENEE M. FURUTA  
AMY JACKSON  
SUN YOUNG PARK

MAILING ADDRESS:

P.O. BOX 4109

HONOLULU, HAWAII 96812-4109

TELEPHONE: (808) 521-8521

FAX: (808) 521-8522

E-MAIL: dangm@aloha.net

WEBSITE: www.marvindanglaw.com

March 23, 2016

Rep. Angus L.K. McKelvey, Chair  
Rep. Justin H. Woodson, Vice Chair  
and members of the House Committee on Consumer Protection & Commerce  
Hawaii State Capitol  
Honolulu, Hawaii 96813

Re: **H.C.R. 182 (Supporting the Adoption of Chip and Pin Technology by All Financial Institutions to Improve the Security of Consumer Financial Transactions in the State)**  
**Hearing Date/Time: Wednesday, March 23, 2016, 2:30 p.m.**

I represent **Visa, Inc.** ("Visa"). Visa operates the world's largest retail electronic payments network providing processing services and payment product platforms. This includes consumer credit, debit, prepaid and commercial payments. Visa facilitates global commerce through the transfer of value and information among financial institutions, merchants, consumers, businesses, and government entities.

**Visa opposes this Resolution as drafted, and Visa proposes an amendment.**

The purpose of this Resolution is to support the adoption of chip and pin technology by all financial institutions to improve the security of consumer financial transactions in Hawaii.

**Chip cards:**

This Resolution refers to "chip and PIN cards".

"Chip cards" are debit or credit cards that contain an embedded microchip. When a chip card is inserted into a chip-enabled terminal, a unique security code is generated. This prevents the reuse account information and protects against fraud.

"Chip and PIN cards" are chip cards which require the use of a PIN to complete a transaction.

A PIN, like a signature, is a form of authenticating a user, but it is also static data element, which can make it vulnerable to theft. If a consumer's PIN for a debit card is stolen, criminals can quickly access and drain that consumer's bank account at an ATM.

**Technologies:**

Visa is committed to protecting consumers from financial fraud involving credit cards and debit cards.

Today in the United States, **PINs** are most commonly used in connection with debit transactions. While PINs will remain a cardholder verification method in the payments ecosystem, they have limitations. As a static data element, PINs are subject to compromise and heavily targeted by thieves. PINs also address only a small portion of the fraud we see today: the portion attributable to lost and stolen cards, which represents only 9 percent of overall payment card fraud. And PINs do not address the rapidly expanding segment of “card-not-present” fraud -- the area of fraud that has experienced the greatest growth -- since PINs are not typically accepted for online and mobile transactions.

No single solution can fully eradicate fraud. To fight fraud, Visa deploys a layered approach, using technology, processes, and people to guard account information from cyber criminals. Technology, in particular, continues to evolve in ways that have helped fraud rates remain near historic lows.

A truly secure payments system requires a wide array of dynamic authentication technologies, including EMV, tokenization, and end-to-end encryption. “EMV” is the global standard for chip cards and the other technology used to authenticate chip card transactions.

**Chip technology** enables more secure payments by generating a one-time use code for each transaction. A benefit of chip technology is that it is flexible and supports multiple cardholder verification methods (including signature, PIN, and no cardholder verification) commonly used for payment cards in the United States. More than 60 percent of Visa’s transaction volume is categorized as low-risk and requires neither signature nor PIN. In addition, about half of merchants currently choose not to support PIN today.

Although the United States is in the early stages of migration to this chip technology, it is already the largest chip market in the world. When fully deployed, chip alone virtually eliminates counterfeit fraud, which represents up to 70 percent of in-store fraud. But to realize the fraud prevention capabilities of chip technology, both chip cards and chip-enabled terminals need to be widely adopted. Visa is working across the payments ecosystem to support broad adoption of chip technology among all stakeholders. To expedite chip migration, Visa supports a streamlined approach that allows financial institutions and merchants to adopt cardholder verification solutions in their own timeframe and in a manner that best fits their business needs.

2015 saw exponential growth in consumer and merchant adoption of EMV chip technology. It was a watershed year in the United States for the migration to chip cards, which officially kicked off on October 1, 2015. As of December 2015, with over 212 million Visa chip cards issued (a 644 percent increase in the last year) and 766,000 merchant locations chip-enabled across the United States (an 872 percent year-over-year increase), there has been tremendous gains in the shift to smarter and more dynamic payment security.

In markets outside the United States, including mature chip markets, new technologies are overtaking PIN and other static cardholder verification methods. For example, Australia, which moved to chip and then introduced PIN seven years later, is now adopting **contactless chip technology** that requires neither PIN nor signature verification. Today, over 60 percent of Visa transactions in Australia are completed using this technology. In Europe, contactless payments continue to grow, allowing consumers to transact at merchants without having to enter a PIN. Here in the United States, consumers conduct contactless payments through mobile devices that use biometrics to better authenticate consumers.

The industry is also looking beyond traditional methods of cardholder verification in order to combat the rise in new types of fraud, especially “card-not-present” fraud. Visa wants to point out three examples in this area.



First, Visa, working with other payment networks, has led the development of **tokenization technology** for digital payments. This innovative solution provides an additional layer of security by replacing cardholder information, such as account numbers and expiration dates, with a unique series of numbers that enables authorization without exposing sensitive account information. Mobile payment applications such as Apple Pay, Android Pay, and Samsung Pay use tokenization to offer enhanced security to consumers and merchants.

Second, Visa uses **advanced analytics** to combat fraud by evaluating up to 500 data elements in less than a second to spot suspicious transactions as they are occurring. In 2014, Visa systems identified nearly \$2 billion in fraudulent payments in this way. Consumers often experience Visa's anti-fraud technology when they receive a phone or text alert from their financial institution asking them to verify a potentially fraudulent purchase.

Third, through **mobile geo-location**, consumers can play an active role in preventing fraud. Visa has developed a new opt-in service that uses mobile geo-location information to more reliably predict whether it is the account holder or an unauthorized user making a payment with a Visa account. By matching the location of the cardholder through a smart phone to the location of the purchase, this service helps improve fraud detection and identify unauthorized transactions.

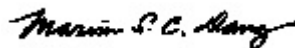
Staying ahead of criminals will always require the investments of many parties aligned toward a common purpose. Visa is committed to working collaboratively with policymakers, financial institutions, and merchants to secure the payments environment.

**Proposed amendment to this Resolution:**

As stated above, PIN, as an authenticating technology, is a static data element, which can make it vulnerable to theft. PIN should not be mandated as a specific technology in this Resolution because other types of technologies have been and will be developed and implemented.

**Accordingly, Visa proposes that all references to "PIN" in this Resolution, including in the title, be deleted so that this Resolution will refer to "chip technology" and "chip cards" (rather than to "chip and PIN technology" and "chip and PIN cards").**

Thank you for considering Visa's testimony.



MARVIN S.C. DANG  
for Visa, Inc.

(MSCD/Visa)

# HAWAII FINANCIAL SERVICES ASSOCIATION

c/o Marvin S.C. Dang, Attorney-at-Law

P.O. Box 4109

Honolulu, Hawaii 96812-4109

Telephone No.: (808) 521-8521

March 23, 2016

Rep. Angus L.K. McKelvey, Chair

Rep. Justin H. Woodson, Vice Chair

and members of the House Committee on Consumer Protection & Commerce

Hawaii State Capitol

Honolulu, Hawaii 96813

Re: **H.C.R. 182 (Supporting the Adoption of Chip and Pin Technology by All Financial Institutions to Improve the Security of Consumer Financial Transactions in the State)**  
**Hearing Date/Time: Wednesday, March 23, 2016, 2:30 p.m.**

I am Marvin Dang, the attorney for the **Hawaii Financial Services Association** (“HFSA”). The HFSA is a trade association for Hawaii’s consumer credit industry. Its members include Hawaii financial services loan companies (which make mortgage loans and other loans, and which are regulated by the Hawaii Commissioner of Financial Institutions), mortgage lenders, and financial institutions. Various members of the HFSA issue credit cards and debit cards.

**The HFSA opposes this Resolution as drafted, and proposes an amendment.**

The purpose of this Resolution is to support the adoption of chip and pin technology by all financial institutions to improve the security of consumer financial transactions in Hawaii.

## **Chip Cards**

Currently, banks and credit unions in the United States are issuing “chip cards”. These are high-tech and more secure credit and debit cards that are replacing the cards with the familiar magnetic stripe. There are already more chip cards issued in the United States than in any other market in the world.

These chip cards are also known as “EMV” cards. EMV is an acronym for Europay, MasterCard and Visa. EMV cards are the global standard for chip cards and the other technology used to authenticate chip card transactions.

EMV cards are being issued to help prevent criminals from fraudulently stealing consumer data. To combat such fraud, these cards use an embedded microchip as a data firewall.

Unlike the magnetic stripe cards which contain unchanging data that could be copied by criminals, when chip cards are inserted into a chip-enabled terminal, a unique security code is generated. This prevents the reuse of the card number and protects against counterfeit fraud.

Chip cards require chip-enabled terminals to read and process these secure transactions. Because retailers are still transitioning to chip-enabled terminals, the chip cards that are being issued by banks and credit unions are currently retaining the magnetic stripe so that the cards can still be used at retailers who don’t have chip-enabled terminals.

## **Some Other Authentication Technologies**

While EMV’s primary purpose is to reduce counterfeit fraud by requiring an interaction between the chip card and an EMV terminal which criminals can not replicate, EMV technology provides an additional opportunity to reduce “lost or stolen” and “card-not-received” fraud through a secondary form of authentication.

When EMV was first introduced in the 1990s in Europe, this authentication was limited to signature or Personal Identification Numbers (PIN). PIN is a long-standing and effective authentication technology, but it has limitations. Most people memorize the PIN for their debit card, but, with multiple credit cards in nearly every wallet or purse, people might not be as comfortable juggling multiple PINs. Even worse, they might use the same PIN for each card.

Mandating the use of a PIN could preclude the adoption of new security measures. With developing technology, even more secure forms of authentication than PIN have been introduced. These include contactless payments offered by mobile phone manufacturers.

In the future, even more sophisticated authentication methods can be expected, unless policy initiatives inadvertently slow the development of innovative new security technologies which read fingerprints, heartbeats, or voice patterns. These new technologies seem likely to provide better authentication in a way that inextricably links a chip card to a cardholder.

Innovation and security are best served when payment card issuers and merchants are able to choose how to deploy EMV chip technology based upon their business model and customer base. This flexible approach incentivizes participants in the payment ecosystem to deploy the safest and most secure tools in their business and to protect consumers from fraudsters.

It is important to view EMV adoption as a single element of a wider “secure-all-channels” approach to protecting payment data and incorporating emerging security technologies such as:

- Tokenization, where data is hidden with “tokens” that mask the underlying data, rendering it useless in a hack;
- Point-to-point encryption where payment card credentials are encrypted at the point of sale terminal; and
- Network-based monitoring, where consumer attributes and behaviors are quickly reviewed to identify fraudulent transactions.

New and emerging technologies can provide security at many different levels. For example, chip cards can prevent counterfeit in-store transactions; tokenization adds another layer of security both online and in stores; and point-to-point encryption secures the point of sale.

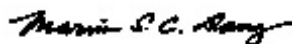
The number of emerging technologies explains why numerous federal banking agencies which regulate, supervise, and examine financial institutions have written to members of Congress opposing the adoption of any one single standard for payment security technology. The Federal Trade Commission has also rejected the notion that mandating a particular technology solution is wise policy.

In summary, PIN should not be mandated as a specific technology in this Resolution because other types of technologies have been and will be developed and implemented.

### **Proposed Amendment to this Resolution**

**The HFSA recommends that this Resolution be amended as follows: all references to “PIN”, including in the title of this Resolution, should be deleted. This Resolution should refer to “chip technology” and “chip cards” (rather than to “chip and PIN technology” and “chip and PIN cards”).**

Thank you for considering our testimony.



MARVIN S.C. DANG  
Attorney for Hawaii Financial Services Association



**SCHLACK ITO**  
A LIMITED LIABILITY LAW COMPANY

Matthew M. Matsunaga  
*Attorney at Law*

DIRECT 808.523.6061  
mmatsunaga@schlackito.com

MAIN 808.523.6040  
FAX 808.523.6030

Topa Financial Center  
745 Fort Street • Suite 1500  
Honolulu, Hawaii 96813

March 22, 2016

Testimony on

## **HCR NO. 182**

# **SUPPORTING THE ADOPTION OF CHIP AND PIN TECHNOLOGY BY ALL FINANCIAL INSTITUTIONS TO IMPROVE THE SECURITY OF CONSUMER FINANCIAL TRANSACTIONS IN THE STATE**

Before the

House Committee on Consumer Protection & Commerce  
Wednesday, March 23, 2016, 2:30 p.m., Conference Room 325

By

Matthew M. Matsunaga, Esq.  
Schlack Ito, a limited liability law company

Please accept this testimony in **opposition** to HCR 182, which would request that all financial institutions that issue credit or debit cards to Hawaii residents or businesses replace those cards with chip and PIN cards. This Concurrent Resolution is unnecessary for the following reasons:

- It's the chip that matters. The chip protects card data from hackers who breach retailers' firewalls. The PIN adds no protection in such retailer breaches.
- Banks are issuing chip cards to consumers now.
- Consumers won't bear any costs. Regardless of what technology is being used at the checkout counter or online, consumers are *not* held liable for fraudulent purchases.

House Committee on Consumer Protection & Commerce

March 22, 2016

Page 2

- PINs is a static technology which is increasingly vulnerable against certain types of fraud.
- Chips are only one of many steps card issuers are taking towards making data more secure.

Thank you for this opportunity to testify.

Sincerely,

SCHLACK ITO  
A LIMITED LIABILITY LAW COMPANY

*Matt Matsunaga*  
Matthew M. Matsunaga

MMM:ab