Statement by Visa Inc.

"Visa payWave is Visa's contactless payment technology. It facilitates fast and convenient transactions at the point of sale and eliminates the requirement for a consumer to make physical contact with the terminal when making a purchase (therefore "contactless"). Consumers simply hold the card or phone in front of the contactless terminal in order to pay.

"Ensuring payment security is one of Visa's highest priorities and Visa payWave enabled payment cards and mobile devices are no exception. Visa payWave cards are as secure as traditional cards and meet all the same standards for security and more.

"Because information travels from card to terminal without any contact, there is a remote risk that data can be intercepted. However, we have built in multiple layers of security for every Visa transaction that helps protect against fraud using stolen information.

"Below are just a few examples of security measures working behind the scenes to prevent fraud:

- Visa payWave cards use advanced cryptographic security where every transaction includes a unique dynamic code, which changes with each transaction.
- Visa payWave cards do not transmit the cardholder's name during a transaction, providing greater privacy than even traditional card payments. Intercepting a Visa payWave transaction results in less sensitive information than when handing a card over to a clerk. Neither the cardholder name nor the three-digit security code on the back of the card are available when the card is read via a contactless reader.
- To protect against fraudulent eCommerce or telephone transactions, merchants use secondary security measures such as asking for the three-digit code imprinted on the back of the card, verifying the billing address associated with account, or an extra layer of password protection such as Verified by Visa. None of this information can be read electronically from the card.
- Some eCommerce merchants also use risk scoring services that are specialized for the online channel, such as those offered by CyberSource, a Visa company. For example, CyberSource can analyze if the cardholder is attempting an online purchase from a computer generally located near the billing address or from a country far away to help detect potential fraud.
- All transactions processed by Visa's global processing network, VisaNet, are analyzed in real-time and scored for its fraud potential. Visa is able to use a comprehensive view of the global payments system to identify fraud patterns and detect suspicious transactions right at the check-out.

"Such advanced capabilities and the multiple layers of security that protect every Visa transaction have helped keep Visa's global fraud rates near historic lows – fewer than 6 pennies for every $100 transacted. In fact, there have been no reports of fraud perpetrated by surreptitiously reading Visa payWave cards.

"Further, Visa payWave cardholders are protected by Visa's zero liability policy, which protects all Visa cardholders from unauthorized purchases. As always, we recommend cardholders check their statements regularly and report any suspicious activity to their issuers."

Jay Hopkins
CRC Public Relations (for Visa Inc.)

Statement to WTHR regarding RFID technology in American Express credit cards:

Overview
Security and privacy are top priorities in everything we do. We've been working with contactless technologies (i.e. RFID, radio frequency technology) for several years now, and we're continually addressing security at every layer to ensure the integrity of the transactions. With expresspay, we've created a product with both security and convenience in mind.

Security/Fraud
Information, such as the customer's actual name or address, is not transmitted through the expresspay signal, helping to prevent identity theft. expresspay uses different technology than the traditional card with a magnetic stripe. Both ways to pay have sophisticated fraud prevention methods that help protect our cardmembers. Every American Express charge goes through a fraud screen. Sophisticated fraud monitoring is used 24/7. As a long standing American Express policy, cardmembers are not held liable for fraudulent charges.

Physical Attributes
The account number on expresspay is a unique code that is different from the actual account number of the charge or credit card linked to expresspay. Essentially, the only relevant data involved during a contactless transaction is the unique code; thus, we protect the card account number. In addition, the expresspay card must be within 4 inches to communicate to a contactless reader in order to initiate a transaction.

How expresspay Works
The cardmember waves their card equipped with expresspay to initiate the transaction (must be within 4 inches of a contactless payment reader). expresspay contains a unique "key" that generates a different digital signature for each transaction. The expresspay key creates a unique code for each transaction (i.e. cryptogram), which we believe is one of the best technologies available today for ensuring the integrity of contactless transactions and minimizing the risk of fraud. Note: In the US, expresspay is featured on Starwood Preferred Guest from American Express, Blue from American Express and Zync.

Answers to WTHR questions

How is AXP protecting its cardmembers from RFID skimming?
No personally identifiable information (PII) such as name, address, or other types of information typically required for identity theft, is shared by the expresspay RFID. The card account number (i.e. on the front of the plastic card) is not shared by the expresspay RFID. Like any unauthorized transaction, cardmembers are not responsible for any fraudulent charges on their American Express Cards. Also, every American Express charge goes through a fraud screen, and we have sophisticated fraud monitoring 24/7.

Once someone skims information from an RFID card, is it possible for them to use any of that information fraudulently?
We don't talk about how people may or may not commit fraud. But what I can you is that we've looked at our fraud numbers across all expresspay cards and in the last 6 years that we've had expresspay, any fraud involving RFID—whether due to lost or stolen cards or any other reason—is extremely small. In fact, in comparison to our total charge volume over that period, our records show expresspay-based fraud to be close to zero percent. We're always working to reduce fraud, and we have one of the lowest fraud rates in the industry.

Through RFID skimming demonstrations, we have seen information obtained such as card account numbers and the type of cards. Is this true for all AXP RFID cards?
What you might have perceived in skimming demonstrations as an "account number" on expresspay is actually a unique code that is different from the actual account number of the charge or credit card linked to expresspay. The only relevant data involved during a contactless expresspay transaction is the unique code -- thus we're protecting the card account number. No personally identifiable information (PII) such as name or address is shared by the expresspay RFID. Also, expresspay contains a unique "key" that generates a different digital signature for each transaction.

Marina Hoffmann Norville
Director, Public Affairs & Communications
American Express Company

MasterCard statement to WTHR:

MasterCard PayPass cards and devices are as secure as paying with traditional MasterCard cards that have magnetic stripe technology. In fact, many consumers claim that they feel more secure with PayPass because they never have to turn the card over to a cashier and it never leaves their hand.

In response to the claims that you're hearing that a person could use a reader to capture someone's account number and expiration date, I think it's important to point out that they can't do anything with that data.

- You can't make an Internet or phone purchase, since the merchant should ask for CVC (card verification code) 2 data - the 3 digit code on the back, or zip code verification - to complete any purchase.
- You can't create a phony mag stripe card without CVC1 data in the mag. stripe
- You can't create a phony PayPass card without the key that is used to create a dynamic CVC3, which is held securely in the PayPass chip

We mandate the use of CVC3 in the chip, which makes it nearly impossible to duplicate a card or "replay" transactions" - because a code that accompanies an authorization request changes every time an authorization request is made. I've attached a fact sheet that goes into more detail, but this is a key point. For every transaction made with a PayPass card, there is a discreet authentication code that changes after each transaction. Without the proper code the transaction will not be authorized. The attached sheet will explain how the code is generated and what security measures are in place that make it so secure.

Lastly, MasterCard cardholders in North America enjoy the protection of the MasterCard Zero Liability policy, knowing that if their card was ever compromised, they are, as with all MasterCard payment programs, not responsible for unauthorized transactions on their accounts.

Erica Harvill
Business Leader
Worldwide Communications

Fact Sheet

MasterCard Worldwide

MasterCard *PayPass* Security

MasterCard *PayPass*™ is MasterCard Worldwide's "contactless" payment program that provides consumers with a simple and convenient way to pay. Using *PayPass*, consumers simply tap their payment card, or alternative *PayPass* device, on a specially equipped merchant terminal, eliminating the need to fumble for cash and coins, hand their card to a clerk or swipe the card through a reader manually. *PayPass* is ideal for quick payment environments where speed is essential, such as quick serve restaurants, gas stations, drug stores, sports stadiums and movie theaters.

Security behind MasterCard *PayPass*
MasterCard *PayPass* cards and devices are processed through the same financial payments networks that process millions of magnetic stripe and chip card transactions securely today.

The primary difference is that *PayPass* uses radio frequency (RF) technology to transmit card information to the merchant's RFID point-of-sale (POS) terminal, instead of requiring a magnetic stripe to be swiped or a chip card to be inserted. In all cases, the account number and expiration date are on the card and the magnetic stripe or chip, and are read by the terminal and used in the transaction. In the case of *PayPass* and contact chip transactions, additional security processes and data are used to secure the transaction and to make the account less susceptible to attack by ensuring that certain security checks have been performed before the transaction is approved. This significantly reduces the risk that any account number information can be used fraudulently.

Since 2000, MasterCard has conducted extensive research and development to create MasterCard *PayPass* and to test this new payment program through technology and market trials before making it available to its customer financial institutions, merchants and consumers. A large component of MasterCard's R&D efforts has focused on the sophisticated and powerful security behind *PayPass*, in order to protect all parties involved in contactless payment transactions.

***PayPass* Security Measures**
The following recommended security measures allow issuers to identify suspected fraud, decline a risky transaction and protect cardholder data:

- The *PayPass* chip does not contain the cardholder name.
- The *PayPass* chip's data values differ from the magnetic stripe values. The terminal sends an indicator of the Point-of-Sale Entry Mode of the data (the *PayPass* chip or the magnetic stripe) to assist the issuer in determining which of the values are appropriate for each transaction.
- Different CVC values distinguish a *PayPass* transaction from a magnetic stripe transaction.
    - Static CVC3 uses an authentication code different from the magnetic stripe CVC1 code.
    - Dynamic CVC3, the strongest authentication method, required by MasterCard, generates a discrete authentication code for each transaction. Dynamic CVC3 uses the well known "challenge-response" security technique where a challenge

is issued to the *PayPass* card or device by the terminal which responds back with a cryptographically calculated code (the Dynamic CVC3). When Dynamic CVC3 is used, each value is unique by transaction and cannot be reused. Moreover, subsequent values cannot be predicted successfully in a fraudulent environment.

- Address Verification, CVC2 checks, and/or SecureCode cardholder verification prevent use of account numbers and expiration dates in authorizing MOTO and electronic commerce transactions.

- A linked account number on the *PayPass* chip different from the magnetic stripe or contact chip account number is an additional security measure that can be employed by issuers to further reduce risk of fraud from stolen *PayPass* account numbers and expiration dates.

CVC3 calculations use the triple DES algorithm with 112 bit keys. This is a security best practice in the banking industry and is intended to protect against hacks or "key search" attacks. In the case of Dynamic CVC3, the triple DES key is stored in secure memory in every *PayPass* chip. Each chip that is type-approved for *PayPass* is evaluated through CAST (Compliance Assessment and Security Testing), MasterCard's leading chip security and approval process.

In addition to the state-of-the-art security built into *PayPass*, MasterCard cardholders continue to have the peace of mind they have come to expect – knowing that if their card was ever compromised, they are ultimately, as with all MasterCard payment programs in North America, SAMEA and Asia Pacific, protected by MasterCard's zero liability policy.

Combining the security of traditional payment cards and smart cards
With a secure chip and radio antenna embedded inside each MasterCard *PayPass* card or device, consumers benefit from smart card-related security measures. The combination of these security measures and the careful design and choice of specific data that can be incorporated into every *PayPass* transaction reduces the risk of fraud and makes *PayPass* more secure than traditional magnetic stripe cards.

###

Contacts:
Erica Harvill, MasterCard Worldwide, 914.249.6848, Erica_Harvill@mastercard.com