

United States Senate

WASHINGTON, DC 20510-2309

January 15, 2014

Brian T. Moynihan
Chief Executive Officer
Bank of America Corporation
100 N. Tryon St.
Charlotte, NC 28255

Dear Mr. Moynihan:

I write today regarding the security of American consumers' payment cards. In recent years, there has been a series of serious breaches of consumer data, most recently the hacking of customer information from Target, Neiman Marcus, and apparently other retailers during the 2013 holiday shopping season. Data breaches and payment card fraud are costly to retailers, financial institutions, and ultimately consumers, who experience the significant burden of dealing with compromised accounts and identity theft. In the wake of these breaches, retailers must reevaluate their internal security practices. At the same time, these incidents underscore the need for more secure payment systems in the U.S.

Unfortunately, the U.S. has not kept pace with the evolving threats to our payment systems even though more secure technology exists. In particular, the magnetic stripe on most U.S. payment cards allows card data to be more easily stolen and duplicated compared to more secure card technology. Adding security features, such as the chips in "EMV" cards that are used in most other industrialized countries, may help prevent the breach of usable cardholder data and make it more difficult to commit payment fraud.

This gap in security hurts American consumers and makes the U.S. a global center for card fraud. A 2013 Federal Reserve study reported that 29 million fraudulent card transactions occurred in the U.S. in 2012, totaling \$4 billion. According to *The Nilson Report*, the U.S. represented less than one-quarter of the world's payment card volume but accounted for nearly *half* of fraud losses in 2012.

I understand and am encouraged that many U.S. financial institutions are working to improve card security for American consumers and may be transitioning to the EMV cards in the coming years. I believe it is important to have an open dialogue around the advantages and disadvantages of this technology so that these improvements can be as effective as possible. I have six questions regarding EMV and other efforts to combat fraud and increase the security of card data:

1. What is the status of your institution's transition to EMV cards?
2. When will all cards issued by your institution be EMV cards or include similar security features?

3. What incentives do you provide to consumers, retailers, and financial institutions to encourage data security and the use of more secure cards? Have these been effective?
4. Could you expedite the transition process to EMV cards? What would the costs and benefits be to doing so?
5. What other improvements are you pursuing to protect consumer data and prevent fraud?
6. What are the main impediments to the adoption of EMV cards and other security improvements?

Please reply with written responses to these questions by February 5, 2014.

Protecting Americans' consumer data is a shared responsibility. I appreciate your efforts as we work to improve the security of our payment systems. If you have any questions, please contact Alvaro Bedoya on my staff at (202) 224-5641 or alvaro.bedoya@judiciary-dem.senate.gov.

Sincerely,



Al Franken
Chairman, Subcommittee on Privacy,
Technology, and the Law

United States Senate

WASHINGTON, DC 20510-2309

January 15, 2014

David W. Nelms
Chairman & CEO
Discover Financial
2500 Lake Cook Rd
Riverwoods, IL 60015

Dear Mr. Nelms:

I write today regarding the security of American consumers' payment cards. In recent years, there has been a series of serious breaches of consumer data, most recently the hacking of customer information from Target, Neiman Marcus, and apparently other retailers during the 2013 holiday shopping season. Data breaches and payment card fraud are costly to retailers, financial institutions, and ultimately consumers, who experience the significant burden of dealing with compromised accounts and identity theft. In the wake of these breaches, retailers must reevaluate their internal security practices. At the same time, these incidents underscore the need for more secure payment systems in the U.S.

Unfortunately, the U.S. has not kept pace with the evolving threats to our payment systems even though more secure technology exists. In particular, the magnetic stripe on most U.S. payment cards allows card data to be more easily stolen and duplicated compared to more secure card technology. Adding security features, such as the chips in "EMV" cards that are used in most other industrialized countries, may help prevent the breach of usable cardholder data and make it more difficult to commit payment fraud.

This gap in security hurts American consumers and makes the U.S. a global center for card fraud. A 2013 Federal Reserve study reported that 29 million fraudulent card transactions occurred in the U.S. in 2012, totaling \$4 billion. According to *The Nilson Report*, the U.S. represented less than one-quarter of the world's payment card volume but accounted for nearly *half* of fraud losses in 2012.

I understand and am encouraged that many U.S. financial institutions are working to improve card security for American consumers and may be transitioning to the EMV cards in the coming years. I believe it is important to have an open dialogue around the advantages and disadvantages of this technology so that these improvements can be as effective as possible. I have six questions regarding EMV and other efforts to combat fraud and increase the security of card data:

1. What is the status of your institution's transition to EMV cards?
2. When will all cards issued by your institution be EMV cards or include similar security features?

3. What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?
4. Could you expedite your transition to EMV cards? What would the costs and benefits be to doing so?
5. What other improvements are you pursuing to protect consumer data and prevent fraud?
6. What are the main impediments to the adoption of EMV cards and other security improvements?

Please reply with written responses to these questions by February 5, 2014.

Protecting Americans' consumer data is a shared responsibility. I appreciate your efforts as we work to improve the security of our payment systems. If you have any questions, please contact Alvaro Bedoya on my staff at (202) 224-5641 or alvaro.bedoya@judiciary-dem.senate.gov.

Sincerely,



Al Franken
Chairman, Subcommittee on Privacy,
Technology, and the Law

United States Senate

WASHINGTON, DC 20510-2309

January 15, 2014

Kenneth I. Chenault
Chairman and CEO
American Express
200 Vesey Street
New York, NY 10285

Dear Mr. Chenault:

I write today regarding the security of American consumers' payment cards. In recent years, there has been a series of serious breaches of consumer data, most recently the hacking of customer information from Target, Neiman Marcus, and apparently other retailers during the 2013 holiday shopping season. Data breaches and payment card fraud are costly to retailers, financial institutions, and ultimately consumers, who experience the significant burden of dealing with compromised accounts and identity theft. In the wake of these breaches, retailers must reevaluate their internal security practices. At the same time, these incidents underscore the need for more secure payment systems in the U.S.

Unfortunately, the U.S. has not kept pace with the evolving threats to our payment systems even though more secure technology exists. In particular, the magnetic stripe on most U.S. payment cards allows card data to be more easily stolen and duplicated compared to more secure card technology. Adding security features, such as the chips in "EMV" cards that are used in most other industrialized countries, may help prevent the breach of usable cardholder data and make it more difficult to commit payment fraud.

This gap in security hurts American consumers and makes the U.S. a global center for card fraud. A 2013 Federal Reserve study reported that 29 million fraudulent card transactions occurred in the U.S. in 2012, totaling \$4 billion. According to *The Nilson Report*, the U.S. represented less than one-quarter of the world's payment card volume but accounted for nearly *half* of fraud losses in 2012.

I understand and am encouraged that many U.S. financial institutions are working to improve card security for American consumers and may be transitioning to the EMV cards in the coming years. I believe it is important to have an open dialogue around the advantages and disadvantages of this technology so that these improvements can be as effective as possible. I have six questions regarding EMV and other efforts to combat fraud and increase the security of card data:

1. What is the status of your institution's transition to EMV cards?
2. When will all cards issued by your institution be EMV cards or include similar security features?

3. What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?
4. Could you expedite your transition to EMV cards? What would the costs and benefits be to doing so?
5. What other improvements are you pursuing to protect consumer data and prevent fraud?
6. What are the main impediments to the adoption of EMV cards and other security improvements?

Please reply with written responses to these questions by February 5, 2014.

Protecting Americans' consumer data is a shared responsibility. I appreciate your efforts as we work to improve the security of our payment systems. If you have any questions, please contact Alvaro Bedoya on my staff at (202) 224-5641 or alvaro.bedoya@judiciary-dem.senate.gov.

Sincerely,



Al Franken
Chairman, Subcommittee on Privacy,
Technology, and the Law

United States Senate

WASHINGTON, DC 20510-2309

January 15, 2014

Ajay Banga
President and CEO
MasterCard
2000 Purchase St.
Purchase, NY 10577

Dear Mr. Banga:

I write today regarding the security of American consumers' payment cards. In recent years, there has been a series of serious breaches of consumer data, most recently the hacking of customer information from Target, Neiman Marcus, and apparently other retailers during the 2013 holiday shopping season. Data breaches and payment card fraud are costly to retailers, financial institutions, and ultimately consumers, who experience the significant burden of dealing with compromised accounts and identity theft. In the wake of these breaches, retailers must reevaluate their internal security practices. At the same time, these incidents underscore the need for more secure payment systems in the U.S.

Unfortunately, the U.S. has not kept pace with the evolving threats to our payment systems even though more secure technology exists. In particular, the magnetic stripe on most U.S. payment cards allows card data to be more easily stolen and duplicated compared to more secure card technology. Adding security features, such as the chips in "EMV" cards that are used in most other industrialized countries, may help prevent the breach of usable cardholder data and make it more difficult to commit payment fraud.

This gap in security hurts American consumers and makes the U.S. a global center for card fraud. A 2013 Federal Reserve study reported that 29 million fraudulent card transactions occurred in the U.S. in 2012, totaling \$4 billion. According to *The Nilson Report*, the U.S. represented less than one-quarter of the world's payment card volume but accounted for nearly *half* of fraud losses in 2012.

I understand and am encouraged that you are working to improve card security for American consumers and will be transitioning to EMV technology in the coming years. I believe it is important to have an open dialogue around the advantages and disadvantages of this technology so that these improvements can be as effective as possible. I have six questions regarding EMV and other efforts to combat fraud and increase the security of card data:

1. What is the status of your transition to the EMV technology?
2. When will all issuers and acquirers on your network be required to issue and/or process EMV cards?

3. What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?
4. Could you expedite your transition to EMV cards? What would the costs and benefits be to doing so?
5. What other improvements are you pursuing to protect consumer data and prevent fraud?
6. What are the main impediments to the adoption of EMV cards and other security improvements?

Please reply with written responses to these questions by February 5, 2014.

Protecting Americans' consumer data is a shared responsibility. I appreciate your efforts as we work to improve the security of our payment systems. If you have any questions, please contact Alvaro Bedoya on my staff at (202) 224-5641 or alvaro.bedoya@judiciary-dem.senate.gov.

Sincerely,



Al Franken
Chairman, Subcommittee on Privacy,
Technology, and the Law

United States Senate

WASHINGTON, DC 20510-2309

January 15, 2014

Charles W. Scharf
Chief Executive Officer
Visa Inc.
900 Metro Center Blvd
Foster City, CA 94404

Dear Mr. Scharf:

I write today regarding the security of American consumers' payment cards. In recent years, there has been a series of serious breaches of consumer data, most recently the hacking of customer information from Target, Neiman Marcus, and apparently other retailers during the 2013 holiday shopping season. Data breaches and payment card fraud are costly to retailers, financial institutions, and ultimately consumers, who experience the significant burden of dealing with compromised accounts and identity theft. In the wake of these breaches, retailers must reevaluate their internal security practices. At the same time, these incidents underscore the need for more secure payment systems in the U.S.

Unfortunately, the U.S. has not kept pace with the evolving threats to our payment systems even though more secure technology exists. In particular, the magnetic stripe on most U.S. payment cards allows card data to be more easily stolen and duplicated compared to more secure card technology. Adding security features, such as the chips in "EMV" cards that are used in most other industrialized countries, may help prevent the breach of usable cardholder data and make it more difficult to commit payment fraud.

This gap in security hurts American consumers and makes the U.S. a global center for card fraud. A 2013 Federal Reserve study reported that 29 million fraudulent card transactions occurred in the U.S. in 2012, totaling \$4 billion. According to *The Nilson Report*, the U.S. represented less than one-quarter of the world's payment card volume but accounted for nearly *half* of fraud losses in 2012.

I understand and am encouraged that you are working to improve card security for American consumers and will be transitioning to EMV technology in the coming years. I believe it is important to have an open dialogue around the advantages and disadvantages of this technology so that these improvements can be as effective as possible. I have six questions regarding EMV and other efforts to combat fraud and increase the security of card data:

1. What is the status of your transition to the EMV technology?
2. When will all issuers and acquirers on your network be required to issue and/or process EMV cards?

3. What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?
4. Could you expedite your transition to EMV cards? What would the costs and benefits be to doing so?
5. What other improvements are you pursuing to protect consumer data and prevent fraud?
6. What are the main impediments to the adoption of EMV cards and other security improvements?

Please reply with written responses to these questions by February 5, 2014.

Protecting Americans' consumer data is a shared responsibility. I appreciate your efforts as we work to improve the security of our payment systems. If you have any questions, please contact Alvaro Bedoya on my staff at (202) 224-5641 or alvaro.bedoya@judiciary-dem.senate.gov.

Sincerely,



Al Franken
Chairman, Subcommittee on Privacy,
Technology, and the Law

United States Senate

WASHINGTON, DC 20510-2309

January 15, 2014

John G. Stumpf
Chairman, President, and CEO
Wells Fargo & Company
420 Montgomery Street
San Francisco, CA 94163

Dear Mr. Stumpf:

I write today regarding the security of American consumers' payment cards. In recent years, there has been a series of serious breaches of consumer data, most recently the hacking of customer information from Target, Neiman Marcus, and apparently other retailers during the 2013 holiday shopping season. Data breaches and payment card fraud are costly to retailers, financial institutions, and ultimately consumers, who experience the significant burden of dealing with compromised accounts and identity theft. In the wake of these breaches, retailers must reevaluate their internal security practices. At the same time, these incidents underscore the need for more secure payment systems in the U.S.

Unfortunately, the U.S. has not kept pace with the evolving threats to our payment systems even though more secure technology exists. In particular, the magnetic stripe on most U.S. payment cards allows card data to be more easily stolen and duplicated compared to more secure card technology. Adding security features, such as the chips in "EMV" cards that are used in most other industrialized countries, may help prevent the breach of usable cardholder data and make it more difficult to commit payment fraud.

This gap in security hurts American consumers and makes the U.S. a global center for card fraud. A 2013 Federal Reserve study reported that 29 million fraudulent card transactions occurred in the U.S. in 2012, totaling \$4 billion. According to *The Nilson Report*, the U.S. represented less than one-quarter of the world's payment card volume but accounted for nearly *half* of fraud losses in 2012.

I understand and am encouraged that many U.S. financial institutions are working to improve card security for American consumers and may be transitioning to the EMV cards in the coming years. I believe it is important to have an open dialogue around the advantages and disadvantages of this technology so that these improvements can be as effective as possible. I have six questions regarding EMV and other efforts to combat fraud and increase the security of card data:

1. What is the status of your institution's transition to EMV cards?
2. When will all cards issued by your institution be EMV cards or include similar security features?

3. What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?
4. Could you expedite your transition to EMV cards? What would the costs and benefits be to doing so?
5. What other improvements are you pursuing to protect consumer data and prevent fraud?
6. What are the main impediments to the adoption of EMV cards and other security improvements?

Please reply with written responses to these questions by February 5, 2014.

Protecting Americans' consumer data is a shared responsibility. I appreciate your efforts as we work to improve the security of our payment systems. If you have any questions, please contact Alvaro Bedoya on my staff at (202) 224-5641 or alvaro.bedoya@judiciary-dem.senate.gov.

Sincerely,



Al Franken
Chairman, Subcommittee on Privacy,
Technology, and the Law

United States Senate

WASHINGTON, DC 20510-2309

January 15, 2014

Jamie Dimon
Chairman and CEO
JPMorgan Chase & Co.
270 Park Ave
New York, NY 10017

Dear Mr. Dimon:

I write today regarding the security of American consumers' payment cards. In recent years, there has been a series of serious breaches of consumer data, most recently the hacking of customer information from Target, Neiman Marcus, and apparently other retailers during the 2013 holiday shopping season. Data breaches and payment card fraud are costly to retailers, financial institutions, and ultimately consumers, who experience the significant burden of dealing with compromised accounts and identity theft. In the wake of these breaches, retailers must reevaluate their internal security practices. At the same time, these incidents underscore the need for more secure payment systems in the U.S.

Unfortunately, the U.S. has not kept pace with the evolving threats to our payment systems even though more secure technology exists. In particular, the magnetic stripe on most U.S. payment cards allows card data to be more easily stolen and duplicated compared to more secure card technology. Adding security features, such as the chips in "EMV" cards that are used in most other industrialized countries, may help prevent the breach of usable cardholder data and make it more difficult to commit payment fraud.

This gap in security hurts American consumers and makes the U.S. a global center for card fraud. A 2013 Federal Reserve study reported that 29 million fraudulent card transactions occurred in the U.S. in 2012, totaling \$4 billion. According to *The Nilson Report*, the U.S. represented less than one-quarter of the world's payment card volume but accounted for nearly *half* of fraud losses in 2012.

I understand and am encouraged that many U.S. financial institutions are working to improve card security for American consumers and may be transitioning to the EMV cards in the coming years. I believe it is important to have an open dialogue around the advantages and disadvantages of this technology so that these improvements can be as effective as possible. I have six questions regarding EMV and other efforts to combat fraud and increase the security of card data:

1. What is the status of your institution's transition to EMV cards?
2. When will all cards issued by your institution be EMV cards or include similar security features?

3. What incentives do you provide to consumers, retailers, and financial institutions to encourage data security and the use of more secure cards? Have these been effective?
4. Could you expedite the transition process to EMV cards? What would the costs and benefits be to doing so?
5. What other improvements are you pursuing to protect consumer data and prevent fraud?
6. What are the main impediments to the adoption of EMV cards and other security improvements?

Please reply with written responses to these questions by February 5, 2014.

Protecting Americans' consumer data is a shared responsibility. I appreciate your efforts as we work to improve the security of our payment systems. If you have any questions, please contact Alvaro Bedoya on my staff at (202) 224-5641 or alvaro.bedoya@judiciary-dem.senate.gov.

Sincerely,



Al Franken
Chairman, Subcommittee on Privacy,
Technology, and the Law

United States Senate

WASHINGTON, DC 20510-2309

January 15, 2014

Michael L. Corbat
Chief Executive Officer
Citigroup Inc.
399 Park Ave
New York, NY 10022

Dear Mr. Corbat:

I write today regarding the security of American consumers' payment cards. In recent years, there has been a series of serious breaches of consumer data, most recently the hacking of customer information from Target, Neiman Marcus, and apparently other retailers during the 2013 holiday shopping season. Data breaches and payment card fraud are costly to retailers, financial institutions, and ultimately consumers, who experience the significant burden of dealing with compromised accounts and identity theft. In the wake of these breaches, retailers must reevaluate their internal security practices. At the same time, these incidents underscore the need for more secure payment systems in the U.S.

Unfortunately, the U.S. has not kept pace with the evolving threats to our payment systems even though more secure technology exists. In particular, the magnetic stripe on most U.S. payment cards allows card data to be more easily stolen and duplicated compared to more secure card technology. Adding security features, such as the chips in "EMV" cards that are used in most other industrialized countries, may help prevent the breach of usable cardholder data and make it more difficult to commit payment fraud.

This gap in security hurts American consumers and makes the U.S. a global center for card fraud. A 2013 Federal Reserve study reported that 29 million fraudulent card transactions occurred in the U.S. in 2012, totaling \$4 billion. According to *The Nilson Report*, the U.S. represented less than one-quarter of the world's payment card volume but accounted for nearly *half* of fraud losses in 2012.

I understand and am encouraged that many U.S. financial institutions are working to improve card security for American consumers and may be transitioning to the EMV cards in the coming years. I believe it is important to have an open dialogue around the advantages and disadvantages of this technology so that these improvements can be as effective as possible. I have six questions regarding EMV and other efforts to combat fraud and increase the security of card data:

1. What is the status of your institution's transition to EMV cards?
2. When will all cards issued by your institution be EMV cards or include similar security features?

3. What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?
4. Could you expedite your transition to EMV cards? What would the costs and benefits be to doing so?
5. What other improvements are you pursuing to protect consumer data and prevent fraud?
6. What are the main impediments to the adoption of EMV cards and other security improvements?

Please reply with written responses to these questions by February 5, 2014.

Protecting Americans' consumer data is a shared responsibility. I appreciate your efforts as we work to improve the security of our payment systems. If you have any questions, please contact Alvaro Bedoya on my staff at (202) 224-5641 or alvaro.bedoya@judiciary-dem.senate.gov.

Sincerely,



Al Franken
Chairman, Subcommittee on Privacy,
Technology, and the Law

United States Senate

WASHINGTON, DC 20510-2309

January 15, 2014

Richard D. Fairbank
Founder, Chairman, and CEO
Capital One
1680 Capital One Dr.
McLean, VA 22102

Dear Mr. Fairbank:

I write today regarding the security of American consumers' payment cards. In recent years, there has been a series of serious breaches of consumer data, most recently the hacking of customer information from Target, Neiman Marcus, and apparently other retailers during the 2013 holiday shopping season. Data breaches and payment card fraud are costly to retailers, financial institutions, and ultimately consumers, who experience the significant burden of dealing with compromised accounts and identity theft. In the wake of these breaches, retailers must reevaluate their internal security practices. At the same time, these incidents underscore the need for more secure payment systems in the U.S.

Unfortunately, the U.S. has not kept pace with the evolving threats to our payment systems even though more secure technology exists. In particular, the magnetic stripe on most U.S. payment cards allows card data to be more easily stolen and duplicated compared to more secure card technology. Adding security features, such as the chips in "EMV" cards that are used in most other industrialized countries, may help prevent the breach of usable cardholder data and make it more difficult to commit payment fraud.

This gap in security hurts American consumers and makes the U.S. a global center for card fraud. A 2013 Federal Reserve study reported that 29 million fraudulent card transactions occurred in the U.S. in 2012, totaling \$4 billion. According to *The Nilson Report*, the U.S. represented less than one-quarter of the world's payment card volume but accounted for nearly *half* of fraud losses in 2012.

I understand and am encouraged that many U.S. financial institutions are working to improve card security for American consumers and may be transitioning to the EMV cards in the coming years. I believe it is important to have an open dialogue around the advantages and disadvantages of this technology so that these improvements can be as effective as possible. I have six questions regarding EMV and other efforts to combat fraud and increase the security of card data:

1. What is the status of your institution's transition to EMV cards?
2. When will all cards issued by your institution be EMV cards or include similar security features?

3. What incentives do you provide or plan to provide to encourage consumers and retailers to use more secure payment methods? Have these been effective?
4. Could you expedite your transition to EMV cards? What would the costs and benefits be to doing so?
5. What other improvements are you pursuing to protect consumer data and prevent fraud?
6. What are the main impediments to the adoption of EMV cards and other security improvements?

Please reply with written responses to these questions by February 5, 2014.

Protecting Americans' consumer data is a shared responsibility. I appreciate your efforts as we work to improve the security of our payment systems. If you have any questions, please contact Alvaro Bedoya on my staff at (202) 224-5641 or alvaro.bedoya@judiciary-dem.senate.gov.

Sincerely,



Al Franken
Chairman, Subcommittee on Privacy,
Technology, and the Law