Filing at a Glance

Company:	The Surety & Fidelity Association of America
Product Name:	Crime Protection Policy - Social Engineering Fraud
State:	District of Columbia
TOI:	23.0 Fidelity
Sub-TOI:	23.0000 Fidelity
Filing Type:	Form
Date Submitted:	06/01/2015
SERFF Tr Num:	SURE-130089148
SERFF Status:	Closed-APPROVED
State Tr Num:	
State Status:	
Co Tr Num:	SFAA-F-299
Effective Date Requested (New):	08/01/2015
Effective Date Requested (Renewal):	08/01/2015
Author(s):	Daniel Wanke
Reviewer(s):	Angela King (primary)
Disposition Date:	06/24/2015
Disposition Status:	APPROVED
Effective Date (New):	08/01/2015
Effective Date (Renewal):	08/01/2015

State: District of Columbia **Filing Company:** The Surety & Fidelity Association of America
TOI/Sub-TOI: 23.0 Fidelity/23.0000 Fidelity
Product Name: Crime Protection Policy - Social Engineering Fraud
Project Name/Number: /

General Information

Project Name:
Project Number:
Reference Organization: N/A
Reference Title: N/A
Filing Status Changed: 06/24/2015
State Status Changed:
Created By: Daniel Wanke
Corresponding Filing Tracking Number:

Status of Filing in Domicile: Pending
Domicile Status Comments: N/A
Reference Number: N/A
Advisory Org. Circular: N/A

Deemer Date:
Submitted By: Daniel Wanke

Filing Description:

The Surety & Fidelity Association of America ("SFAA") submits for filing the following endorsements to the Crime Protection Policy (SP 00 01) and the Crime Protection Policy for Public Entities:

(Insuring Agreement 9) Include Coverage for Fraudulently Induced Transfers
SE 01 67 08 15

(Insuring Agreement 8) Include Coverage for Funds Transfer Fraud
SE 00 41 08 15

In addition, SFAA files the enclosed application for Coverage for Fraudulently Induced Transfers (SA 6259).

Coverage for Funds Transfer Fraud (SE 00 41) "covers loss of funds caused by a fraudulent instruction to a financial institution to transfer funds from the insured's account" (as stated in our filing letter when the form was filed initially in 1999). Thus, the coverage contemplates that the instruction purportedly sent from the insured to the insured's bank was fraudulent or phony, and then the bank acted on those phony instructions and wired funds to the fraudsters account.

In recent months, businesses have experienced a fraudulent scheme that was not contemplated under SE 00 41. In particular, the fraudster impersonates a vendor, customer or employee of the insured and contacts the insured requesting a wire transfer of funds. Then, based on this phony information, a legitimate employee of the insured contacts the bank to place the order for a wire transfer. Thus, the instruction sent from the insured to the bank is legitimate, as it is sent by a legitimate employee intending to do so. However, the employee was induced fraudulently into contacting the bank and making the order for the wire transfer. The exposure for such scams can be significant. According to the Federal Bureau of Investigation Internet Crime Complaint Center, between October 2013 and December 2014, such scams resulted in losses totaling $214,972,503.30. However, as noted above, the scam was not contemplated under the coverage provided under SE 00 41. Therefore, to ensure that the SFAA Crime Protection Policy provides relevant coverages that addresses the exposures of the day, SFAA has created SE 01 67.

SE 01 67 covers loss caused by a "fraudulently induced transfer" causing funds to be transferred out of the insured's premises or banking premises. A "fraudulently induced transfer" is defined as a transfer resulting from a payment order (to make a wire transfer) or check, made or written on the good faith reliance of the instructions provided by a person impersonating an employee, customer, vendor or owner of the insured. The form establishes internal controls as a condition precedent. Specifically, before sending the payment order or issuing the check, the insured is required to verify the instruction by calling back the purported employee, customer, vendor or owner at a predetermined telephone number or through some other verification methodology approved by the insurer.

State: District of Columbia **Filing Company:** The Surety & Fidelity Association of America
TOI/Sub-TOI: 23.0 Fidelity/23.0000 Fidelity
Product Name: Crime Protection Policy - Social Engineering Fraud
Project Name/Number: /

The current funds transfer fraud form (SE 00 41) has been revised to ensure there is no unintended overlap of coverage between the “traditional” funds transfer fraud coverage and the new coverage for fraudulently induced transfers. Specifically, prior to revision, SE 00 41 defined a “fraudulent instruction” to include three scenarios. The third scenario stated that a fraudulent instruction included:

[a]n electronic, telegraphic, cable, teletype, telefacsimilie, telephone or written instruction initially received by you which purports to have been transmitted by an Employee but which was in fact fraudulently transmitted by someone else without your or the Employee's knowledge or consent.

This scenario references the impersonation of an employee. However SE 00 41 did not contemplate the current scams described above. These scams are a relatively new development that did not exist in 1999 when the form was filed originally. In addition, by the terms of the coverage, the fraudulent instruction is one “directing [a] financial institution” to transfer, pay or deliver funds from your transfer account.” In the current scams, the instruction being sent by the fraudster to the insured does not direct the bank to do anything, but requests that the insured contact the bank to make the wire transfer. This third scenario has been deleted from SE 00 41 to avoid any misinterpretation that the two forms (SE 00 41 and SE 01 67) cover the same exposure.

SE 00 41 also has been revised to use the term “payment order” to refer to a specific instruction to the bank to transfer a specific amount. We have observed that “instruction” in the prior version could refer to either an instruction received from some party to the insured or an instruction sent by the insured to the bank to wire funds. The use of two different terms will distinguish the different scenarios. The definition of “payment order”, which already is included in the Crime Protection Policy, is based on the definition of payment order from the Uniform Commercial Code.

We thank you for your consideration. Please feel free to contact me at 202-778-3630 or rduke@surety.org if you have any questions.

Company and Contact

Filing Contact Information

Daniel Wanke, Manager - Regulatory and Government Affairs
1140 19th Street NW
Suite 500
Washington, DC 20036

dwanke@surety.org

202-778-3631 [Phone]
202-463-0606 [FAX]

Filing Company Information

(This filing was made by a third party - SAA01)

The Surety & Fidelity Association of America
1101 Connecticut Ave., N.W.
Suite 800
Washington, DC 20036
(202) 778-3626 ext. [Phone]

CoCode:
Group Code:
Group Name:
FEIN Number: 26-0003391

State of Domicile: District of Columbia
Company Type: Rating
State ID Number:

Filing Fees

State: District of Columbia **Filing Company:** The Surety & Fidelity Association of America
TOI/Sub-TOI: 23.0 Fidelity/23.0000 Fidelity
Product Name: Crime Protection Policy - Social Engineering Fraud
Project Name/Number: /

Fee Required? No

Retaliatory? No

Fee Explanation:

SERFF Tracking #:	*SURE-130089148*	***State Tracking #:***		***Company Tracking #:***	*SFAA-F-299*

State:	*District of Columbia*	***Filing Company:***	*The Surety & Fidelity Association of America*
TOI/Sub-TOI:	*23.0 Fidelity/23.0000 Fidelity*		
Product Name:	*Crime Protection Policy - Social Engineering Fraud*		
Project Name/Number:	*/*		

Form Schedule

Item No.	Schedule Item Status	Form Name	Form Number	Edition Date	Form Type	Form Action	Action Specific Data		Readability Score	Attachments
1	APPROVED 06/24/2015	Supplemental Application for Coverage for Fraudulently Induced Transfers under the Crime Protection Policy	SA 6259	08/2015	ABE	New			0.000	fraud.induced.transfer.application..cpp.FINAL.pdf
2	APPROVED 06/24/2015	Include Coverage for Fraudulently Induced Transfers	SE 01 67 08 15	08/2015	END	New			0.000	social engineering fraud broad.FINAL..pdf
3	APPROVED 06/24/2015	Include Coverage for Funds Transfer Fraud	SE 00 41 08 15	08/2015	END	Replaced	*Previous Filing Number:*		0.000	funds.transfer.revised.final.pdf, SE 00 41 Redline.pdf
							Replaced Form Number:	*SE 00 41 04 12*		

Form Type Legend:

ABE	Application/Binder/Enrollment	**ADV**	Advertising
BND	Bond	**CER**	Certificate
CNR	Canc/NonRen Notice	**DEC**	Declarations/Schedule
DSC	Disclosure/Notice	**END**	Endorsement/Amendment/Conditions
ERS	Election/Rejection/Supplemental Applications	**OTH**	Other

This form must be completed for each new policy and at the beginning of each premium period for renewal policies.

SUPPLEMENTAL APPLICATION FOR COVERAGE FOR FRAUDULENTLY INDUCED TRANSFERS UNDER THE CRIME PROTECTION POLICY

Application is hereby made by _____

_____
(List all Insureds)

Principal Address_____
(No.) (Street) (City) (State) (Zip Code)

for

Insuring Agreement	**Limit of Insurance**	**Deductible Amount**
Coverage for Fraudulently Induced Transfers	$	$

to become effective or to be continued as of 12:01 a.m. on _____ to 12:01 a.m. on _____

1. INTERNAL CONTROLS - CUSTOMERS:

(a) Do you have procedures to verify the identity and authenticity of new customers before entering into transactions with them? Yes☐ No ☐

If so,explain your screening procedures for new customers

_____

_____

(b) Indicate whether you follow the following specific procedures:

i) Investigate new customers through a credit reporting agency Yes☐ No ☐
ii) Verify and confirm the customer's bank account information(account numbers, routing numbers, bank name and address) by calling the bank directly Yes☐ No ☐
iii) Verify any request to change the customer's bank account information by calling the customer at a telephone number previously provided by the customer Yes☐ No ☐
iv) Verify and confirm that the amount requested to be transferred equals the amount due to the customer Yes☐ No ☐

(c) Do you accept funds transfer instructions from customers over the telephone, fax, email or some other electronic communications method? Yes☐ No ☐

If yes, please describe your procedures to authenticate the instructions_____

_____

_____

(d) Do you control access to customer information in your computer systems? Yes☐ No ☐

If yes, please indicate whether you:

i) Implement access controls and firewalls in your database of customer information Yes☐ No ☐
ii) Restrict access to only particular employees of yours Yes☐ No ☐
iii) Require the customer to authenticate his or her identity using passwords, personal identification numbers, shared secrets, tokens or biometrics before the customer may access his or her data. Yes☐ No ☐

(e) Do you control the dissemination of customer information? Yes☐ No ☐

If yes, please indicate whether you:

i) Have a company policy prohibiting the dissemination of any personally identifiable information pertaining to the customer Yes☐ No ☐
ii) Provide customer information only to a designated representative of the customer Yes☐ No ☐
iii) Require the customer requesting customer data to authenticate his or her identity using passwords, personal identification numbers, shared secrets, tokens or biometrics . Yes☐ No ☐

2. INTERNAL CONTROLS - VENDORS:

(a) Do you have procedures to verify the identity and authenticity of new vendors before entering into transactions with them? Yes☐ No ☐

If so, explain your screening procedures for new vendors_____

_____

_____

(b) Indicate whether you implement the following specific procedures:

i) Investigate new vendors through a credit reporting agency Yes☐ No ☐

ii) Verify and confirm the vendor's bank account information (account numbers, routing numbers, bank name and address) by calling the bank directly Yes☐ No ☐

iii) Verify any request to change the vendor's bank account information by calling the vendor at a telephone number previously provided by the vendor Yes☐ No ☐

iv) Verify and confirm that the amount requested to be transferred equals the amount due to the vendor Yes☐ No ☐

v) Require review of any changes of the vendor's bank account information (account numbers, routing numbers, bank name and address) by a supervisor before the change is made in your records Yes☐ No ☐

vi) Require vendors to maintain a crime insurance and cyber liability insurance policy Yes☐ No ☐

(c) Do you accept funds transfer instructions from vendors over the telephone, or by fax, email or some other electronic communications method? Yes☐ No ☐

If yes, please describe your procedures to authenticate the instructions_____

_____

_____

3. INTERNAL CONTROLS – EMPLOYEES

(a) Do you accept funds transfer instructions from your employees, officers and owners over the telephone, or by fax, email or some other electronic communications method? Yes☐ No ☐

If yes, please describe your procedures to authenticate the instructions_____

_____

_____

(b) Do you verify any request to transfer funds made by an employee, officer or owner by calling back the employee, officer or owner at the telephone number listed in your company directory? Yes☐ No ☐

4. WIRE TRANSFER CONTROLS

(a) Is there a written policy regarding wire transfers? Yes☐ No ☐

(b) What is the average monthly number of fund transfers? _____

(c) What is the largest single amount that can be transferred? _____

(d) Do all your employees receive training on social engineering or phishing scams? Yes☐ No ☐

(e) Do wire transfers to an account outside the United States require review and approval by a supervisor? Yes☐ No ☐

(f) Is the authority to execute wire transfers limited to specified employees? Yes☐ No ☐

5 **The insured represents that the information furnished in this application is complete, true and correct. Any misrepresentation, omission, concealment or incorrect statement of a material fact, in this application or otherwise, shall be grounds for the rescission of any policy issued in reliance upon such information.**

Dated at_____ this_____ day of_____ , 20_____

_____ By_____

(Insured) (Name and Title)

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

INCLUDE COVERAGE FOR FRAUDULENTLY INDUCED TRANSFERS

A. COVERAGE

We will pay for loss of **funds** resulting directly from a **fraudulently induced transfer** causing the **funds** to be transferred from your **premises** or **banking premises** to a person, entity, place or account outside of your control.

B. LIMIT OF INSURANCE AND DEDUCTIBLE

The Limit of Insurance and Deductible Amount are shown in the Declarations.

C. DEFINITIONS

As used in this Insuring Agreement only:

a. **Fraudulently induced transfer** means:

A transfer resulting from a **payment order** transmitted from you to a financial institution, or a check drawn by you, made in good faith reliance upon an electronic, telefacsimilie, telephone or **written** instruction received by you from a person purporting to be an **Employee,** your customer, a **Vendor** or an **Owner** establishing or changing the method, destination or account for payments to such **Employee,** customer, **Vendor** or **Owner** that was in fact transmitted to you by someone impersonating the **Employee**, customer, **Vendor** or **Owner** without your knowledge or consent and without the knowledge or consent of the **Employee**, customer, **Vendor** or **Owner**.

b. **Vendor** means any entity or person that provides or has provided goods or services to you pursuant to a preexisting agreement.

c. **Funds** means **money** and **securities**.

d. **Employee** means any natural person:

(1) While in your service or for 30 days after termination of service; and

(2) Whom you compensate directly by salary, wages or commissions; and

(3) Whom you have the right to direct and control while performing services for you.

e. **Owner** means a natural person having an ownership interest in you.

D. CONDITIONS

It is a condition precedent to coverage under this Insuring Agreement that before forwarding the **payment order** to a financial institution or issuing the check, you verified the authenticity and accuracy of the instruction received from the purported **Employee**, customer, **Vendor** or **Owner**, including routing numbers and account numbers, by calling, at a predetermined telephone number, the **Employee**, customer, **Vendor** or **Owner** who purportedly transmitted the instruction to you, or by some other out of band verification procedure approved in writing by us, and you preserved a contemporaneous **written** record of this verification.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

INCLUDE COVERAGE FOR FUNDS TRANSFER FRAUD

A. COVERAGE	We will pay for loss of **funds** resulting directly from a **fraudulent instruction** directing a financial institution to transfer, pay or deliver **funds** from your **transfer account**.
B. LIMIT OF INSURANCE AND DEDUCTIBLE	The Limit of Insurance and Deductible Amount are shown in the Declarations.
C. DEFINITIONS	As used in this Insuring Agreement: a. **Fraudulent instruction** means: (1) A **payment order** transmitted to a financial institution which purports to have been transmitted by you, but which was in fact fraudulently transmitted by someone else without your knowledge or consent; or (2) A written instruction (other than those described in Insuring Agreement 2.) which purports to have been issued by you and which was sent or transmitted to a financial institution to establish the conditions under which transfers are to be initiated by such financial institution through an electronic funds transfer system and which was issued, forged or altered without your knowledge or consent. b. **Transfer account** means: An account maintained by you at a financial institution from which you can initiate the transfer, payment or delivery of **funds**: (1) By means of a **payment order** communicated directly to the financial institution or through an electronic funds transfer system; or (2) By means of written instructions (other than those described in Insuring Agreement 2.) establishing the conditions under which such transfers are to be initiated by such financial institution through an electronic funds transfer system. c. **Funds** means **money** and **securities**.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

INCLUDE COVERAGE FOR FUNDS TRANSFER FRAUD

A. COVERAGE	We will pay for loss of **funds** resulting directly from a **fraudulent instruction** directing a financial institution to transfer, pay or deliver **funds** from your **transfer account**.
B. LIMIT OF INSURANCE AND DEDUCTIBLE	The Limit of Insurance and Deductible Amount are shown in the Declarations.
C. DEFINITIONS	As used in this Insuring Agreement: a. **Fraudulent instruction** means: ~~(1) An electronic, telegraphic, cable, teletype, telefacsimilie or telephone instruction~~(1) A **payment order** transmitted to a financial institution which purports to have been transmitted by you, but which was in fact fraudulently transmitted by someone else without your knowledge or consent; or (2) A written instruction (other than those described in Insuring Agreement 2.) ~~issued by you, which was forged or altered by someone other than you without your knowledge or consent, or~~ which purports to have been issued by you~~, but was in fact fraudulently issued without your knowledge or consent; or~~ ~~(3) An electronic, telegraphic, cable, teletype, telefacsimilie, telephone or written instruction initially received by you which purports to have been~~ and which was sent or transmitted ~~by an Employee but~~to a financial institution to establish the conditions under which transfers are to be initiated by such financial institution through an electronic funds transfer system and which was ~~in fact fraudulently transmitted by someone else~~issued, forged or altered without your ~~or the Employee's~~ knowledge or consent. b. **Transfer account** means: An account maintained by you at a financial institution from which you can initiate the transfer, payment or delivery of **funds**: (1) By means of ~~electronic, telegraphic, cable, teletype, telefacsimilie or telephone instructions~~a **payment order** communicated directly ~~or though~~to the financial institution or through an electronic funds transfer system; or (2) By means of written instructions (other than those described in Insuring Agreement 2.) establishing the conditions under which such transfers are to be initiated by such financial institution through an electronic funds transfer system. c. **Funds** means **money** and **securities**.

SERFF Tracking #:	*SURE-130089148*	***State Tracking #:***		***Company Tracking #:***	*SFAA-F-299*

State:	*District of Columbia*	***Filing Company:***	*The Surety & Fidelity Association of America*
TOI/Sub-TOI:	*23.0 Fidelity/23.0000 Fidelity*		
Product Name:	*Crime Protection Policy - Social Engineering Fraud*		
Project Name/Number:	*/*		

Supporting Document Schedules

Bypassed - Item:	Readability Certificate
Bypass Reason:	N/A
Attachment(s):	
Item Status:	APPROVED
Status Date:	06/24/2015

Bypassed - Item:	Copy of Trust Agreement
Bypass Reason:	N/A
Attachment(s):	
Item Status:	APPROVED
Status Date:	06/24/2015

Bypassed - Item:	Consulting Authorization
Bypass Reason:	N/A
Attachment(s):	
Item Status:	APPROVED
Status Date:	06/24/2015

Satisfied - Item:	Explantory Memorandum
Comments:	Please find attached an explanatory memo for this filing.
Attachment(s):	Forms Cover Letter.CPP.fraudulent.induce.pdf
Item Status:	APPROVED
Status Date:	06/24/2015

The Surety & Fidelity Association of America

1101 CONNECTICUT AVENUE, NW, SUITE 800, WASHINGTON, DC 20036 TEL: (202) 463-0600 – FAX: (202) 463-0606
website: http://www.surety.org
E-mail: information@surety.org

LYNN M. SCHUBERT
President

May 27, 2015

RE: New and revised coverage for Crime Protection Policy
Reference Filing Number: SFAA-F-298

Dear Commissioner,

The Surety & Fidelity Association of America ("SFAA") submits for filing the following endorsements to the Crime Protection Policy (SP 00 01) and the Crime Protection Policy for Public Entities:

(Insuring Agreement 9) Include Coverage for Fraudulently Induced Transfers
SE 01 67 08 15

(Insuring Agreement 8) Include Coverage for Funds Transfer Fraud
SE 00 41 08 15

In addition, SFAA files the enclosed application for Coverage for Fraudulently Induced Transfers (SA 6259).

Coverage for Funds Transfer Fraud (SE 00 41) "covers loss of funds caused by a fraudulent instruction to a financial institution to transfer funds from the insured's account" (as stated in our filing letter when the form was filed initially in 1999). Thus, the coverage contemplates that the instruction purportedly sent from the insured to the insured's bank was fraudulent or phony, and then the bank acted on those phony instructions and wired funds to the fraudsters account.

In recent months, businesses have experienced a fraudulent scheme that was not contemplated under SE 00 41. In particular, the fraudster impersonates a vendor, customer or employee of the insured and contacts the insured requesting a wire transfer of funds. Then, based on this phony information, a legitimate employee of the insured contacts the bank to place the order for a wire transfer. Thus, the instruction sent from the insured to the bank is legitimate, as it is sent by a legitimate employee intending to do so. However, the employee was induced fraudulently into contacting the bank and making the order for the wire transfer. The exposure for such scams can be significant. According to the Federal Bureau of Investigation Internet Crime Complaint Center, between October 2013 and December 2014, such scams resulted in losses totaling

$214,972,503.30.[1] However, as noted above, the scam was not contemplated under the coverage provided under SE 00 41. Therefore, to ensure that the SFAA Crime Protection Policy provides relevant coverages that addresses the exposures of the day, SFAA has created SE 01 67.

SE 01 67 covers loss caused by a "fraudulently induced transfer" causing funds to be transferred out of the insured's premises or banking premises. A "fraudulently induced transfer" is defined as a transfer resulting from a payment order (to make a wire transfer) or check, made or written on the good faith reliance of the instructions provided by a person impersonating an employee, customer, vendor or owner of the insured. The form establishes internal controls as a condition precedent. Specifically, before sending the payment order or issuing the check, the insured is required to verify the instruction by calling back the purported employee, customer, vendor or owner at a predetermined telephone number or through some other verification methodology approved by the insurer.

The current funds transfer fraud form (SE 00 41) has been revised to ensure there is no unintended overlap of coverage between the "traditional" funds transfer fraud coverage and the new coverage for fraudulently induced transfers. Specifically, prior to revision, SE 00 41 defined a "fraudulent instruction" to include three scenarios. The third scenario stated that a fraudulent instruction included:

> [a]n electronic, telegraphic, cable, teletype, telefacsimilie, telephone or written instruction initially received by you which purports to have been transmitted by an Employee but which was in fact fraudulently transmitted by someone else without your or the Employee's knowledge or consent.

This scenario references the impersonation of an employee. However SE 00 41 did not contemplate the current scams described above. These scams are a relatively new development that did not exist in 1999 when the form was filed originally. In addition, by the terms of the coverage, the fraudulent instruction is one "directing [a] financial institution" to transfer, pay or deliver funds from your transfer account." In the current scams, the instruction being sent by the fraudster to the insured does not direct the bank to do anything, but requests that the insured contact the bank to make the wire transfer. This third scenario has been deleted from SE 00 41 to avoid any misinterpretation that the two forms (SE 00 41 and SE 01 67) cover the same exposure.

SE 00 41 also has been revised to use the term "payment order" to refer to a specific instruction to the bank to transfer a specific amount. We have observed that "instruction" in the prior version could refer to either an instruction received from some party to the insured or an instruction sent by the insured to the bank to wire funds. The use of two different terms will distinguish the different scenarios. The definition of "payment

---

[1] Brian Donohue, *FBI:Business Email Compromise Scams Steal $214M in 2014*, Threatpost, January 28, 2015 (available at https://threatpost.com/fbi-business-email-compromise-scams-steal-214m-in-2014/110715).

order", which already is included in the Crime Protection Policy, is based on the definition of payment order from the Uniform Commercial Code.

We thank you for your consideration. Please feel free to contact me at 202-778-3630 or rduke@surety.org if you have any questions.

Sincerely,

Robert J. Duke
Corporate Counsel