

Social Engineering, Ransomware and Bitcoin

Challenges for Commercial Crime Insurers in the 2020s

Chris McKibbin, Partner

Tel: 416-596-2899

cmckibbin@blaney.com

Overview

- 1. Social Engineering Fraud**
- 2. Bitcoin and other Cryptocurrencies**
- 3. Ransomware**

Social Engineering Fraud

Social Engineering Fraud

Common Scenarios:

1. Fake Client Scam
2. Executive Impersonation Scam
3. Vendor Email Hack / Impersonation
4. Collection Scam targeting Lawyer

Social Engineering - Coverage Issues

- Not an easy “fit” with traditional Commercial Crime and 3-D wording
- Some insureds have attempted to fit into On-Premises or Funds Transfer Coverages
- On-Premises: Fraudster must be on premises at time loss occurs – “set-up” of later off-premises fraud not enough: *Bankmanagers* (7th Cir. 2013)

Social Engineering - Coverage Issues

- Direct Loss Requirement: may be a problem where client funds are involved: *Taylor & Lieberman* (C.D. Cal. 2015) [Blaneys Fidelity Blog](#)
- Funds Transfer Fraud not a good fit; instructions to bank must themselves be fraudulent
- Unwitting, but authorized, instruction by Insured containing fraudulent information is typically insufficient: *Northside Bank* (Pa. 2001)

Social Engineering – Recent Developments

- SEF endorsements introduced in Canada 2014
- Where coverage is not purchased, the usual “target” insuring agreement is Computer Fraud
- Computer Fraud Coverage is intended for hacking-related losses only: *Pestmaster* (9th Cir. 2016) [Blaneys Fidelity Blog](#)

Pestmaster (9th Cir. 2016) [Blaneys Fidelity Blog](#)

*When Priority 1 transferred funds pursuant to authorization from Pestmaster, the transfer was not fraudulently caused. **Because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a “General Fraud” Policy.** While Travelers could have drafted this language more narrowly, we believe protection against all fraud is not what was intended by this provision, and not what Pestmaster could reasonably have expected this provision to cover.*

***Apache* (5th Cir. 2016)**

Blaneys Fidelity Blog

- Vendor impersonation fraud
- Request to change bank account data comes from @petrofacld.com, not @petrofac.com
- Email attached fake confirmation letter
- Employee called phone number on fake letterhead
- Net loss of \$2.4 million

Apache (5th Cir. 2016) [Blaneys Fidelity Blog](#)

- Court finds no coverage
- Fraudulent transfer was not direct result of computer use
- *“To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would ... convert the computer-fraud provision to one for general fraud.”*

Taylor & Lieberman (9th Cir. 2017)

Blaneys Fidelity Blog

- Accounting firm manages client accounts, has POAs
- Client's email account compromised
- Coverage: *“an unauthorized (1) “entry into” its computer system, and (2) “introduction of instructions” that “propogate[d] themselves” through its computer system.”*
- District Court: No direct loss (C.D. Cal. 2015)

Blaneys Fidelity Blog

***Taylor & Lieberman* (9th Cir. 2017)**

Blaneys Fidelity Blog

- Court finds no coverage
- “... *under a common sense reading of the policy, these are not the type of instructions that the policy was designed to cover, like the introduction of malicious computer code. ... Additionally, the instructions did not, as in the case of a virus, propagate themselves throughout T&L’s computer system; rather, they were simply part of the text of three emails.*”

SEF: Decisions for Insurers

- Nomenclature: Fraudulently-Induced Transfers
- Include SEF in base wording or targeted exclusions in base wording?
- “Non-Optional” SEF endorsement
- Offering SEF coverage to applicants (and documenting it): using the “reasonable expectations” doctrine proactively (*Progressive Homes*, SCC 2010)

Bitcoin and other Cryptocurrencies

What is Bitcoin?

- Decentralized virtual currency
- Contrast with centralized virtual currencies, which are controlled through a central entity
- In a decentralized system, transactions run from person to person; no central entity
- Recorded instead in a Blockchain

What is Blockchain?

- Public “ledger” of Bitcoin transactions
- Each transaction requires **public** key (for specific coin) and **private** key (for owner)
- Combination is compared to Blockchain to determine whether transaction is legitimate (“Mining”)

Blockchain – Mining (Ridiculous Simplification)

978GRHG4QIUUY3Q59OQE8GAEHB0AE9D8034
RNGJH9PRJGW87J9G8QER76394835QYU95G
QEAYH9U4EP1HT9U6TY95H53JP9YU3450H1H
64A3YXJ4XY6T5K476GDGHG5H4G578J7N95Z
4G74N5GF456B1N4GFVGFH42GHI48GHNJG58
J4GHXMJ58GM47HG8MGH4K4M8HG2GXFG8N
W5F74HG9G87G65G32154GH9GV2B3B8K2K5L
G51GF24G5F4H5G7HG54N8G65IFD11D2D6G1
C5C263DC5GH45HJ57K4523U55WE5E4T4J12J
Q1H025F45D1FG2H45G521F69G7H4H23VF36F
2VC2S3D5FGH4N2V235GB2VCD5N2KLL25KU5
FG47XN24H9M48GXFG8NXYG59RN74H2M48D

How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES



Bob and Alice both have Bitcoin "wallets" on their computers.



Wallets are files that provide access to multiple Bitcoin addresses.



An address is a string of letters and numbers, such as 1HULMwZEPkJEPeCh43BeKJLybLCWtDpN.



Bob creates a new Bitcoin address for Alice to send her payment to.

CREATING A NEW ADDRESS



Each address has its own balance of bitcoins.

SUBMITTING A PAYMENT



Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

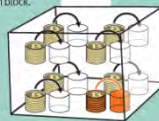


Gary, Garth, and Glenn are Bitcoin miners.

VERIFYING THE TRANSACTION

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.



Private key

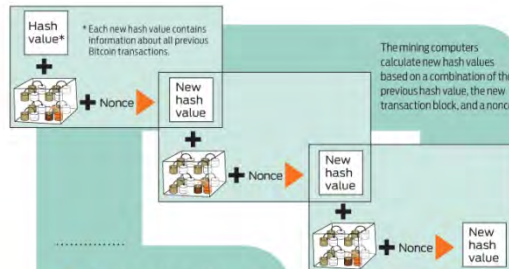


Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Public key



Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.



Cryptographic Hashes
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

| | |
|----------------------|---|
| The root of all evil | 6d0a 1899 086a... (56 more characters) |
| The root of all evil | 486c 6be4 6dde... |
| The root of all evil | b8db 7ee9 8392... |

Nonces
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil ???

0000 0000
0000...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash



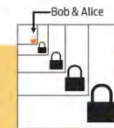
value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.



TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.



Bitcoin – Wallet

Help

allet



Search



[Introduction](#)

[Resources](#)

[Innovation](#)


[Participate](#)

[FAQ](#)

[English](#)

Choose your Bitcoin wallet

Find your wallet and start making payments with merchants and users.

 **Mobile**

 **Desktop**

 **Hardware**

 **Web**



BitGo



Green
Address



Coin.Space



Coinapult



Coinbase



Xapo

Bitcoin – Wallet

- Bitcoins must be stored in a wallet (online or offline)
- Wallet not provided by Bitcoin – separate software
- Not *entirely* anonymous
- Key issue – Wallet Vulnerabilities

Bitcoin – Risks

- Blockchain itself is thought to be safe (eliminates “double-spend” problem)
- Wallet-related fraud much bigger problem
- Exchange-related fraud also a problem
- Some “mainstream” vendors “accept” Bitcoin, but only through an exchange or middleman (e.g., Coinbase or BitPay)

Bitcoin – Wallet Risks

- Wallets are software. They can be hacked (e.g. Mt. Gox and fraudulent withdrawals)
- Scam Wallet Services (e.g. Onion Wallet)



Bitcoin – Wallet Risks

- **Theft** of Private Key = Theft of Bitcoin = Bitcoin can be spent by fraudster
- **Loss** of Private Key = Loss of Bitcoin = Bitcoin “Disappears”
- Wallets can also be the target of Social Engineering Fraud

Bitcoin: Fidelity Insurance Issues

- 1. Covered Property**
- 2. Proof and Quantum of Loss**
- 3. Third Party Losses**
- 4. Dishonest / Criminal Acts Exclusions**

Fidelity Insurance Issues

Covered Property?

- **Money** – Not Cash, but what about “*Currency*”?
- **Securities** – “*Negotiable and Non-Negotiable Instruments representing Money or Property*”
- **Other Property** – tangibility requirement
- “Cryptocurrencies” included or excluded?

Great American Endorsement

Securities is amended to include:

c. bitcoins, which are a form of virtual or on-line peer to peer mediums of exchange, used to pay for goods or services, or held for investment, which can be purchased and which can be exchanged into cash.

ISO Exclusion / Modified Exclusion

k. Virtual Currency

Loss involving virtual currency of any kind, by whatever name known, whether actual or fictitious including, but not limited to, digital currency, crypto currency or any other type of electronic currency. However, if a Virtual Currency Limit Of Insurance is shown in the Schedule, we will pay up to that amount for loss of virtual currency shown in the Schedule. That amount is part of, not in addition to, the Limit Of Insurance shown in the Declarations for the applicable Insuring Agreement.

Fidelity Insurance Issues

Proof and Quantum of Loss

- Lack of reliable third-party verification
- Means of establishing loss – forensic verification of transaction from other evidence?
- Existence and Quantum can be especially hard to establish if wallet stored offline – proof of existence is wallet itself

Fidelity Insurance Issues

Third Party Losses

- Some mainstream vendors “accept” Bitcoin, but only through an exchange or middleman (e.g., Coinbase or BitPay)
- Exchange converts into dollars
- What if loss occurs while Bitcoins / dollars are in possession of intermediary?
- Coverage for intermediary?

Fidelity Insurance Issues

Dishonest / Criminal Acts Exclusions



Silk Road
anonymous market

messages 0 | orders 0 | account B0.0000

Search

Shop by Category



1 Gram Heroin #4

B1.9463 add to cart

seller: 10toes(97)
ships from: United States of America
ships to: Worldwide
category: Heroin

bookmark this item

postage options:

free (B0.0000)



report this item

Ransomware

Ransomware

ber-chaos-hits-thousands-patients/

Search

Login Register Subscribe Rewards Search Video

The Telegraph

HOME NEWS SPORT BUSINESS ALL SECTIONS

News

UK World Politics General Election 2017 Science Education Health Brexit Royals Investigations

News

NHS cyber chaos hits thousands of patients



Accident Forgiveness,
Home Claim
Forgiveness
and savings of

\$600*

Make the switch >

belairdirect.
car and home insurance

RECOMMENDED

What is Ransomware?



- Restricts access to the infected system
- Demands that the user pay a ransom
- May misrepresent an association with law enforcement

Is Coverage Available?


- No coverage decisions
- Non-Crime Coverages (e.g., Cyber Risks; Kidnap, Ransom & Extortion)
- Attempts to “fit” into Crime Coverage:
 1. Computer Fraud Insuring Agreement
 2. KR&E / Voluntary Parting exclusions
- Lack of consistency

Computer Fraud Insuring Agreement

We will pay for loss of, and loss from damage to, Money, Securities and Other Property resulting directly from the use of a computer to fraudulently cause a transfer of that property from inside the Premises or Banking Premises:

- a) to a person (other than a Messenger) outside those Premises; or*
- b) to a place outside those Premises.*

Computer Fraud – Issues

- **Issue**: Is Bitcoin “*Money, Securities or Other Property*”?
- **Issue**: Ransomware does not “*fraudulently cause a transfer*”; encrypted files not transferred. Insured causes transfer of  separately.
- **Issue**: “Voluntary Parting” Exclusion

KR&E Exclusion

... no coverage will be available ... for:

*... loss or damage as a result of a kidnap, ransom or **other extortion payment** (as distinct from **Robbery**) surrendered to any person as a result of a threat to do bodily harm to any person or a threat to do damage to the **Premises** or **other property**;*

Ransomware: Decisions for Insurers

- Is this a **Cyber** Risk, a **Crime** Risk or a separate specialized risk? (e.g., **KR&E**)
- Will we see Ransomware Endorsements?
- How to deal with Loss / Limits / Deductibles?
 1. Value based on ransom paid? (*NHS/WannaCry = \$20,000 as of May 13, 2017*)
 2. Value based on Restoration Expense?
 3. Business Interruption Loss?

Further Reading

- M.J. Krone and H.M. Bernstein, “Introduction to Bitcoin and Potential Insurance Coverage for Virtual Currencies”, 21 Fidelity L.J. 143 (November 2015)
- J.L. Laycock, “Understanding the Difference between Computer Fraud, Funds Transfer Fraud & Fraudulently Induced Transfer Coverage within a Crime Policy”, *Canadian Underwriter* (May 9, 2017)
- D.S. Wilson, C. McKibbin and Z. Garcia, “Coverage for Social Engineering Fraud Takes its Place Among the Required Coverage for Canadian Business” *Claims Canada* (January 2017)

Blaneys Fidelity Blog

Bookmarks Tools Help

linth... x +

tyblog.com/2017/04/03/taylor-lieberman-ninth-circuit-finds-no-coverage-under-crime-policy-for-client-funds-lost-in-social-engineering-fraud/

Search

Blaneys Fidelity Blog

HOME OUR LAWYERS ABOUT BLANEYS FIDELITY BLOG RESOURCES



— InComm: U.S. District Court holds that Computer Fraud Coverage does not respond in Prepaid Debit Card Scheme

Commercial Ventures: U.S. District Court holds that Insured's Co-Owner and President is not an "Employee" under Crime Policy →

APRIL 3, 2017 · 11:27 AM | EDIT

Taylor & Lieberman: Ninth Circuit finds No Coverage under Crime Policy for Client Funds lost in Social Engineering Fraud

By [David S. Wilson](#) and [Chris McKibbin](#)

Search

Search

Follow Blog via Email

Click to follow this blog and receive notifications of new posts by email.

Follow

View Recent Posts

- Commercial Ventures: U.S. District Court holds that Insured's Co-Owner and President is not an "Employee" under Crime Policy May 4, 2017
- Taylor & Lieberman: Ninth Circuit finds No Coverage under Crime

Blaneys Fidelity Practice Group



David S. Wilson



Chris McKibbin



Stuart Woody



Zack Garcia