CONSUMER PRIVACY & IDENTITY QUARTERLY

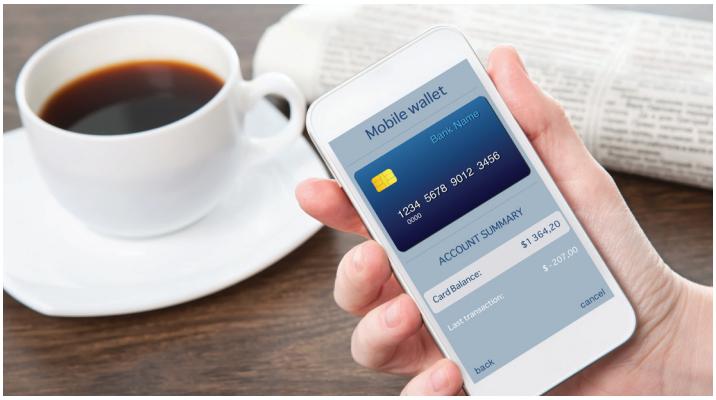
VOL N°3 ISSUE N°2

DISCLAIMER

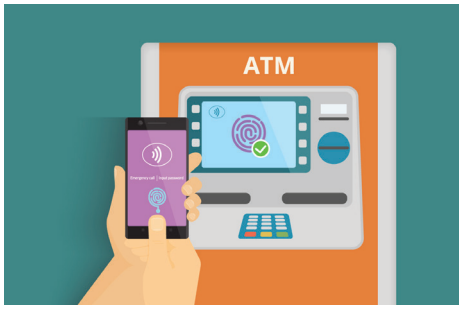
The Department of Defense (DoD) expressly disclaims liability for errors and omissions in the contents of this publication. No warranty of any kind, implied, expressed, statutory, including but not limited to warranties of non-infringement of third party rights, titles, merchantability, or fitness for a particular purpose is given with respect to the contents of this guide or its links to other Internet resources. The information provided in this guide is for general information purposes only. Reference in this guide to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public and does not constitute endorsement, recommendation or favoring by DoD or the U.S. Government. DoD does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained in this guide; does not endorse the organizations or their websites referenced herein; does not endorse the views they express or the products/services they offer; cannot authorize the use of copyrighted materials contained in referenced websites. DoD is not responsible for transmissions users receive from the sponsor of the referenced website and does not guarantee that non-DoD websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.

FOR MORE INFORMATION OR QUESTIONS EMAIL osd.ncr.osd.mbx.dodsmartcards@mail.mil

IN THIS ISSUE:



ALSO INSIDE:



NEW TECH, NEW YOU:
FINANCIAL IDENTITY IN THE DIGITAL AGE

"Your preparedness against identity fraud requires a comprehensive understanding of what constitutes your financial identity."

In December 2016, Rachel checked her email and was shocked by what she found. A message in her inbox confirmed her successful order for an iPhone 6, bought using her Groupon account. But Rachel never made that order; someone else had accessed to her account without her permission. She joined 57 million other victims of an account takeover attack, a new type of financial identity fraud rising in popularity as consumers increasingly procure goods and services through virtual financial transactions.

Consumers have welcomed digital payment methods for their ease and convenience. In 2018, consumers are more likely to deposit a check using a mobile app versus visiting a physical ATM, seamlessly approve purchases with fingerprints on smartphones, and settle debts between friends using money transfer apps such as Venmo or over social media messenger apps like Facebook and Snapchat. The amalgamation of financial transactions with mobile devices and social media accounts has expanded what constitutes one's financial identity. A modern user's financial profile isn't made up solely of bank account information; it also links with virtual wallet and online shopping accounts that can be easily accessed using a combination of the user's identity data—such as email accounts, user IDs, birthdates, and passwords.

In response, criminals have shifted their focus to consumers' devices and accounts, which store and transmit personal information. New financial fraudsters target identity data such as usernames and passwords, as opposed to financial assets such as bank account or credit card number. They profit by using up stored credits or rewards points to make high-value purchases, buying digital goods, phishing other users using the compromised account's credentials, or selling credentials on the black market. As transactions become virtual, financial accounts (and associated identity data) become more vulnerable—evolving into access points from which monetary assets can be stolen.

In this CPIQ issue, we analyze the current trends in identity theft and fraud, along with best practices you can implement to better protect your finances online. We get into the workings of these cybercriminals and walk you through the evolved methods they can employ to target and misuse your identity and account data online and via mobile transactions. You will learn how to safeguard your finances while banking online or transferring money using your smartphone app, equipped with the latest authentication and notification settings. In case you are one of the unlucky victims of financial fraud, you will be guided through immediate, simple steps you can take to remedy the situation. You will also read about biometric and blockchain technologies and how they will be harnessed to better safeguard your digital finances in the near future.

Despite the best efforts of businesses operating online, identity theft is growing year after year in both size and complexity. This burden is shared with consumers—who must learn to remain vigilant and proactively protect their financial transactions and assets online. Join us in this issue to find out how.

NEXT: Watch Your [Virtual] Wallet

WATCH YOUR [VIRTUAL] WALLET:
SAFEGUARDING YOUR ONLINE FINANCIAL IDENTITY

As we increasingly engage in virtual financial transactions, we open ourselves to intricate and sophisticated financial identity crime. Consumers can more safely conduct virtual financial transactions by proactively monitoring their identity, using advanced security measures such as two-factor authentication, and preparing to effectively respond once fraud is detected.

Theft + Fraud = Identity Crime

Identity theft occurs when key pieces of personal information, such as your social security number (SSN) or date of birth, are collected by someone else without your permission. Theft can happen physically—when you lose your wallet or smartphone, when a neighbor peeks through discarded mail in your trash bin, or when a hacker gains physical access to your programmable payment devices. Today, identity theft frequently transpires digitally—when someone retrieves your personal data by hacking your service providers, conducting phishing scams, or deploying malware attacks that exploit your Wi-Fi and Bluetooth connections.

Identity fraud occurs when your stolen identity information is used by another person to obtain illicit financial advantages consisting of credit, goods, and services. Identity fraud runs a gamut of sophistication, as straightforward as a relative using your credit card number to shop online, or as complex as a criminal purchasing your data from a hacker and using it to create a web of intermediate accounts in your name to ultimately submit false loan applications, file illegitimate tax returns, and subscribe to utility services.

Frequently, the facilitators of identity crime are "insiders"—personnel working in service industries with access to your personal information (e.g., your car dealer, your HR representative)—who are incentivized to use or sell your identity data.

Recent History: Successful Countermeasures

Two recent developments are helping protect consumers from the most prevalent forms of identity crime. First, the rollout of chip-enabled credit cards, which are difficult to duplicate, has made it much harder to commit in-store point-of-sale fraud using stolen credit card information.

Second, two-factor authentication is increasingly available to consumers who are opening or updating financial service accounts. Opting in to two-factor authentication permits a business entity to send you a notification—a text message, email, or mobile app alert—as part of the identity verification process. Consequently, a fraudster lacking access to your email or phone account is unlikely to successfully access your financial assets.

Current Trends

Chip-cards and two-factor authentication are reducing "simple" types of identity crime. Consequently, criminals are targeting consumers in new ways, seeking to derive indirect financial benefits, and escalating the sophistication of identity attacks.

Continues on Page 8...

FINANCIAL ID CRIME

The Federal Trade Commission (FTC), a government agency that tracks identity crime complaints, identifies six primary types:

1

Employment- or Tax-related Fraud (34%):

A criminal uses your SSN and personal data to obtain a job or file a fraudulent income tax return.

2

Credit Card Fraud (33%):

A criminal uses your credit card data, or opens a credit card account in your name, in order to fraudulently purchase goods and service.

New Account Fraud: 105,209 reports filed in 2017, up 3% from 2016.

Existing Account Fraud: 34,260 reports filed in 2017, up 20% from 2016.

Card-not-present Fraud (e.g., online shopping fraud) is now 81% more prevalent than Point-of-sale Fraud.

3

Phone & Utilities Fraud (13%):

A criminal uses your personal information to open a mobile or utility account.

New Account Fraud: 26,062 reports filed in 2017, up 18% from 2016

Existing Account Fraud: 4,675 reports filed in 2017, up 11% from 2016

4

Bank Fraud (12%):

A criminal uses your personal information to take over your existing financial account or open a new one in your name.

5

Loan & Lease Fraud (7%):

A criminal uses your personal information to fraudulently obtain a loan or lease in your name.

6

Government Documents & Benefits Fraud (7%):

A criminal uses your personal information to register for government benefits.

**Note: Some complaints involve multiple types of identity crime; consequently, percentages noted total more than 100.*

16.7M US identity fraud victims in 2017

1 in 15 people or **6.64%** of US consumers became victims of identity fraud in 2017

U.S. financial losses sustained due to identity fraud in 2017:

$16.8 Billion

TIME REQUIRED FOR RESOLUTION

Average time to remediate an identity theft issue:

7 hours in the span of 1-30 days

Extreme case:

Up to 1,200 hours over the course of a year

Average time to remediate an identity fraud issue:

100-200 hours over a six month period

ACCOUNT TAKEOVER (ATO) FRAUD REACHED A FOUR-YEAR HIGH IN 2017

Account takeover losses in the U.S.

totaled $5.1B in 2017

1.5M victims of ATO fraud also had a

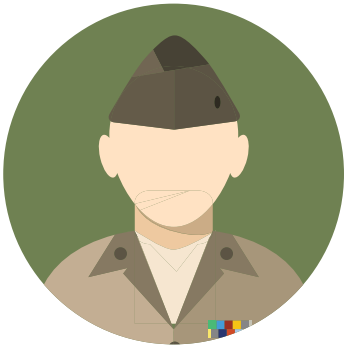
new account opened in their name

Average account takeover victim

spent 15 hours resolving the fraud

Average account takeover victim paid

$290 in out of pocket expenses



MILITARY CONSUMERS

Military consumers filed

30,184

identity theft reports in 2017

Military consumers filed 3,564 reports of mobile services fraud in 2017.

9% of military consumers reported a financial loss; median loss of $299 (total loss of $2.34M)

Account Takeover

Consumers are increasingly prone to non-credit card fraud, specifically via ecommerce account takeover (ATO). ATO fraud often targets non-monetary assets, such as retailer loyalty points and rewards, cryptocurrency wallets, mobile data plans, and brokerage accounts. As of 2017, fraud committed via ecommerce websites in the United States was 81% more likely than point-of-sale fraud.

New Account Fraud

While ATO fraud is on the rise, criminals are also likely to try another approach: using your stolen identity information to create entirely new accounts in your name. Criminals typically use alternate contact information to ensure victims remain unaware of new accounts until those accounts default, are sent to collections, and appear on credit reports. Credit card fraud is the most lucrative and prevalent type, but utility, loan, and peer-to-peer payments fraud also occurs frequently. In 2017, new account fraud affected 1.5M US consumers, an enormous increase from the prior peak of 500,000 victims in 2015.

Synthetic Identity Theft

Another aspect of new account fraud is the rise in synthetic identity theft. Bolstered by complex cyber crimes including data breaches, phishing scams, malware attacks, and artificial intelligence (AI) applications, synthetic identity theft is a novel practice in which criminals amalgamate identity details from multiple victims into a new, virtual, "frankenstein" identity, which can then be used to fraudulently open credit lines and new service accounts. Financial accounts created from synthetic identities may not appear on the credit report of any single identity theft victim. However, in some cases, diligent collections investigators are able to track fraud activities back to an original victim—e.g., if Frankenstein Doe shares your SSN. Even if your whole identity is not compromised, key parts may be maliciously exploited.

Consumer Impact

Financial identity crime impacts individuals whose data has been compromised and misused, as well as the business entities involved in any fraudulent financial transactions conducted using stolen data. According to Javelin Strategy & Research, a leading research-based advisory firm in the digital financial sector, 16.7M US consumers were victims of identity fraud in 2017 (an increase of 1.3M from 2016), resulting in $16.8B USD in fraud damages. For perspective, this means 1 of every 15 US consumers was victimized last year.

Consumer actions, behaviors, and demographics shape fraud risk. Those who actively engage in digital financial transactions bear a larger degree of risk, but other demographics are also particularly vulnerable. Minors and seniors can be ideal targets, as they are less likely to monitor and audit their financial identities.

The greatest toll from identity crime is the time and effort required to resolve it, and the emotional distress incurred along the way. Preparedness is the first step in building resilience.

In the short term, victims of identity fraud are likely to be barred from using crucial segments of the consumer finance economy—denied certain services (e.g., opening a new utility account), or forced to close down existing accounts (e.g., a compromised credit card)—for the sake of security.

While this shut-out is an inconvenience in our on-demand consumer culture, the long-term consequences of identity crime are likely to take a greater toll on victims. These include:

- Negative effects on credit scores and rates, insurance rates, and loan availability, all of which may impair or preclude major purchases
- Additional security checks while traveling, or difficulty passing new employee background checks
- Financial loss incurred after retaining lawyers or private investigators to help fight criminal charges and disentangle genuine and fraudulent transactions

NEXT: Best Practices You Can Bank On

BEST PRACTICES YOU CAN BANK ON:
STAYING SAFE BANKING ONLINE

Online banking revolutionized the way people around the world interact with financial institutions; today, more than half of Americans bank online. Online banking has its advantages, but also its risks. Follow this guidance to bank safely online.

Connecting to sites

When connecting to online banking websites, use the official apps or websites provided by your financial institutions. Avoid third-party apps and websites performing core banking functions. Use HTTPS encryption when connecting to online banking websites or apps (ensure that the URL begins with https://). Never access online banking services from public Wi-Fi. Finally, when connecting to banking services, avoid clicking on pop-up windows soliciting personal information.

Authentication

Authentication is vital to protecting your personal and financial data when banking online. Create strong alphanumeric passwords with at least eight characters, including both upper and lowercase letters; never use the same password for different online banking services. Change your password frequently. Enable two-factor authentication for banking services (physical key, smartphone authentication apps, or text message). Many banks provide a physical code generating key (e.g., Safepass by Bank of America), which will generate a two-factor authentication code each time a user logs into an account. Whenever possible, use biometric authentication to add an additional layer of security to your account. Finally, set up verbal passwords and challenge questions for accessing your account over the phone.

Communication Settings

Hackers often try to compromise online banking accounts by spoofing legitimate communications from financial institutions. Therefore, it is important users never provide personal information unless speaking to a financial institution via an official phone number or the communication settings provided on an official app or website. Never respond to any outside queries for information coming via phone, email, or online messages.

Account Maintenance

Routine account maintenance helps users protect their accounts. Check your login history whenever you access your account to ensure there is no activity at suspicious times or locations. Always log off after completing a financial transaction online.

Transaction Limits and Alerts

Transaction limits and alerts are two of the best ways to prevent online banking fraud. Set up transaction alerts so you receive emails, text messages, and smartphone notifications whenever someone performs an activity on your online banking account. Set geographic limits for banking and notify your bank of travel itineraries to ensure they can spot fraud rapidly. Use transaction limits to restrict the amount of money a user can transfer in a single day or week to ensure hackers cannot rapidly empty your bank accounts. Finally, restrict all bank transfers to accounts you have not previously designated as trusted recipient accounts.

When to Contact Your Financial Institution

If you believe your account has been compromised, immediately contact your bank via its official phone number or other verified contact information. When dealing with financial crime, every second counts. Carefully document all evidence of unauthorized access; include login histories, transaction alerts, and suspicious communications.

MONEY ON THE MOVE:
MOBILE MONEY TRANSFER APPS

Mobile money transfer apps (MMTAs) are popular smartphone applications that allow users to transfer money directly to other users. These apps have widespread appeal because they combine features of online banking with those of social networking services (SNS). About 62% of American millennials and 36% of the total US population use MMTAs. Venmo, Google Wallet, Facebook Messenger Payments, and Snapcash are examples of MMTAs. MMTAs make it fun and easy to send money to friends, but they also present new opportunities for financial identity fraud.

Features of MMTAs

MMTAs combine features of online banking and SNS. Like online banking, users can initiate financial transactions and can check account balances. MMTAs generally require users to link a bank account or credit card to fund transactions. When users pay each other on MMTAs, the funds do not instantaneously appear in the receiver's bank account; funds appear as credit in the receiver's account and take several days to transfer.

MMTAs resemble SNS because users are encouraged to publicly post their transaction activity; and to add other users as "friends." Users can post emojis and text to describe their financial transactions and can "like" or comment about transactions. Finally, like SNS, MMTAs often ask for extensive permissions to access information about your smartphone contacts and device settings.

How to Protect Yourself

To protect yourself on MMTAs, use the following guidance. Avoid accessing MMTAs on public Wi-Fi networks. Use privacy settings to restrict the SNS features of MMTAs so only you can see account activity. Use transaction alerts to receive email or text notifications of any transaction. Never provide personal or financial information to MMTAs beyond what is strictly required. Deny MMTAs permission to access your smartphone contacts and settings. Finally, never send or receive money from strangers or unverified accounts.

NEXT: Your Body, Your Security

YOUR BODY, YOUR SECURITY:
USING BIOMETRICS TO SAFEGUARD TRANSACTIONS

Your body may soon become the primary way you access money—and fight financial fraud.

A December 2017 VISA survey found 86% of Americans are interested in using biometric sensors that scan fingerprints, faces, irises, and voices to verify their identities. The shift is about more than convenience. In a 2017 FICO survey, 44% of respondents listed identity theft and banking fraud as top concerns, greater than the 18% who feared terrorism.

Biometrics can be more secure than passwords and make it harder for thieves to steal identities and gain access to accounts. Here are some ways finance companies are implementing biometrics.

Fingerprint/Palm

Present: GESA Credit Union uses palm-vein authentication to identify customers without photo IDs or account numbers.
Future: Visa is testing sensor-equipped credit cards that verify fingerprints and make it difficult for thieves to use stolen cards.

Face

Present: USAA and other banks allow customers to access apps using face recognition.
Future: Mastercard, whose "selfie pay" system authenticates users via face recognition, is requiring all card issuers to implement biometric authentication by 2019.

Voice

Present: USAA and Citi are among several companies that use voice authentication in apps and to block fraudulent account access attempts in call centers.
Future: Amazon's Alexa and other intelligent digital assistants can recognize individual voices, potentially allowing them to conduct secure transactions by voice.

Iris

Present: Bank of America and BBVA are implementing iris authentication in mobile apps.
Future: Banks, including Citi, are testing iris authentication in ATMs in the United States. The technology is already used by some foreign banks, including India's DCB Bank.

Behavioral

Present: Experian uses behavioral biometrics—analyzing how users type and other factors—to detect fraud when consumers apply for credit cards.
Future: By monitoring behavior, apps passively authenticate users and lock accounts when a threat is identified.

86% of **Americans** are interested in using **biometric** sensors that scan fingerprints, faces, irises, and voices to **verify** their ***identities***.

NEXT: Are You a Victim of Identity Fraud?

ARE YOU A VICTIM OF IDENTITY FRAUD?
HERE'S HOW TO FIGHT BACK

Regardless of the method, financial identity fraud has the same outcome: your data has been misused, potentially with serious impact on you, your reputation, and your records. Here are steps to mitigate the damage and get your finances back on track.

1. Place a fraud alert with a national credit reporting agency (CRA)

Contacting one of the three CRAs reduces the risk of others opening accounts in your name. If you place the alert with one agency, they will notify the other two for you. A fraud alert also entitles you to a free credit report from each credit reporting agency.

Place the alert by calling Equifax at (888) 766-0008, Experian at (888) 397-3742, or TransUnion at (800) 680-7289.

2. Close your financial accounts

Close any accounts that were opened without your permission, along with any existing accounts that show unauthorized financial activities. Alert banks, credit card companies, and financial service providers (e.g., PayPal, Apple Pay) where compromised information is stored.

3. File a police report and secure proof of identity

Filing a police report helps: it provides legal proof that you reported an occurence of identity fraud, even if the police do not actively pursue the case. You will be required to complete and submit an affidavit and provide proof of identity along with the report. Secure your proof of identity by completing the Federal Trade Commission's Identity Theft Report at https://www.identitytheft.gov/.

4. Place a security freeze

A credit freeze prevents anyone else from opening new accounts in your name, which is especially important if you have been a victim of a data breach exposing sensitive personally identifiable information. Credit freezes must be placed with all three credit bureaus. You can always temporarily life the freeze should you require a credit check in the future.

For all non-impacted accounts: **TURN ON *two-factor authentication*** and ALL the available **notification** settings to actively monitor ***unauthorized*** access to your **finances**.

NEXT: FUTURES: Our Friend the Blockchain

OUR FRIEND THE BLOCKCHAIN

"Cryptocurrencies: everything you don't understand about money combined with everything you don't understand about computers." —John Oliver, Last Week Tonight

As of June 2018, cryptocurrencies such as Bitcoin are a popular investment, even among people who don't understand them. Beyond the cryptocurrencies themselves, the innovative blockchain system they ride on offers numerous possibilities, including privacy and identity applications. It's a complicated but promising system.

A blockchain—invented by Satoshi Nakamoto, a pseudonym for an unknown person or persons—is simply a distributed file: a lengthy "chain" comprised of linked "blocks" of data. The entire file does not reside on a single machine; rather, these blocks are distributed across a peer-to-peer network of numerous networked servers around the world. A blockchain can theoretically contain any kind of data; for cryptocurrencies, it contains a constantly updating ledger of financial transactions. Redundancy, encryption, and user anonymity keep the blockchain secure. Users must validate transactions by digitally signing them using both a public key (like a username) and a private key (like a password), neither of which are necessarily traceable to the original user.

Blockchains have numerous potential applications, but the original is Bitcoin. Bitcoin's blockchain contains a ledger of financial transactions using a limited-supply currency. Users "mine" bitcoins by providing the computing power to record and encrypt new blocks in the ledger; miners receive bitcoin as an incentive. In contrast, Ethereum is a blockchain system that sets up "smart contracts" that allow scripts to run on a decentralized virtual machine. Decentralized applications, or dapps, run on distributed computing power in exchange for cryptocurrency payments.

Compared to the traditional, centralized model of computing, a blockchain-based system has the advantage of not placing all data on any one system. A blockchain's transactional ledger can ensure that only one person can access an asset, whether a file or an amount of currency, at any given time. The blockchain distributes control of the system across the network rather than keeping it in one set of hands.

Blockchain systems also have disadvantages. Decentralization slows decision-making and makes them vulnerable to mass disagreements. For instance, a simple disagreement on block size has divided the Bitcoin community, and therefore the entire software underpinning the system. Blockchains are also slower at performing transactions than typical computing systems because changes must be made redundantly around the globe. Distributed control, extension beyond national borders, and anonymity have made blockchains appealing for black market purchases and money laundering.

As a person with a hammer treats everything like a nail, blockchains are a solution looking for a problem. The tech world is using blockchains to solve as many problems as possible. Numerous prototype systems have sought to use a blockchain, usually Ethereum, to authenticate identity. Deloitte's Smart Identity, Thomson Reuter's BlockOneID, uPort, and Civic's Secure Identity Platform all create identities on their blockchain ledgers. These services seek to enable identity authentication of private online services, replicate state identity documents, or even transcend identification authorities to create self-sovereign identities. These systems are, so far, largely hype, but if they receive large-scale backing by a state issuer or a major corporation, they may determine the future of identity authentication.

WHAT IS A BLOCKCHAIN?

Here's a normal computer file. They vary in size and content, but they're mostly in one entity.

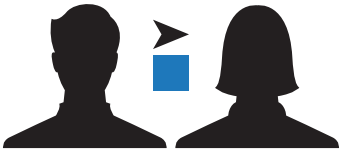
But, you could divide the file into similarly-sized chunks, or blocks, and then place them in a certain order, like a chain. A chain of blocks is called…well, you get it.

A normal file has to be one piece, on one machine, to be useful…

…but blockchains do not. Blocks can be distributed around the world, and their coding lets them connect in the correct order. Blocks are redundant, so if one machine is lost, others will still be able to complete the blockchain.

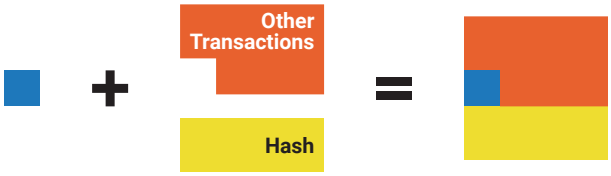
COOL. SO WHAT CAN IT DO?

Any number of things, but let's illustrate its most common use, which is as a ledger of transactions. With Bitcoin, these transactions are financial. With Ethereum, they're computing contracts, and with identity blockchains, they're packets of identity data, but the basic idea is the same. Let's see how Bitcoin works.



Let's start with a financial transaction between two people, here represented by a blue square.

Once requested, the peer-to-peer network validates the requestor and the transaction.



The transaction is then bundled with other transactions and a hash, or abbreviated form, of the previous block to form a new block.

Finally, a process called "mining" adds the new block, including the transaction, to the chain. The transaction is now a permanent part of the ledger. Those who contributed computing power to this process are given Bitcoin as an incentive.

READ BELOW FOR MORE NERDY DETAILS

So that not everyone can just add blocks to the blockchain willy-nilly, the system requires what is called "proof of work." Bitcoin mining amounts to using computing power to solve math problems. Lots of miners try solving each problem simultaneously, but only the first solver posts the block and receives the Bitcoin incentive. These problems are of variable difficulty, depending on the current number of active miners, to ensure new blocks are added about once every 10 minutes. These problems are asymmetrical, so they take considerable work to solve but little effort to confirm they are correct. The problems are also purposeless, giving Bitcoin the reputation of wasting considerable amounts of energy.

Consider this analogy: the US dollar is a specific shape with a specific design printed on it in a specific set of colors. If the dollar were a blank sheet of paper, anyone could attempt to purchase things with paper, but the required work of cutting and printing prevents people from making dollar bills, thereby limiting the supply. This work is even more critical in a blockchain, which lacks a centralized managing body.

THE LAST WORD...

Remember that new technology and convenience always comes with increased risks; ease of use is often granted in exchange for collecting and analyzing your identity and financial data. Protecting yourself against sophisticated financial fraudsters requires vigilance and good digital hygiene from consumers. These are final words from us that we hope you take away from this issue.

- Routinely **REVIEW** all your financial accounts to make sure there aren't suspicious activities.
- **Do not** share or post any personally identifiable data (e.g. your Facebook username, phone number, or home address) with unknown service providers or persons online or via mobile.
- Set transaction and geographical limits on all your **financial** accounts.
- Do not respond to any queries about your finances online or via SMS. Call the valid number of your financial institutions or service providers to **verify** that it's not a spoofing attack.
- Turn on **TWO-FACTOR AUTHENTICATION** to set maximum barrier to your assets from outsiders.

Our ***NEXT*** Issue...

Hopefully this issue has prompted you to consider your personal virtual financial identity safety, as well as that of the seniors and minors in your life. In the next issue, we'll focus in on ***teenagers' online identity activities*** and arming you with critical information:

- What are they even doing **online**?
- What **risks** do these activities present?
- Which new **services** (and types of services) are teens engaging with?

Stay tuned for our **next issue**!

How much do you actually know about Financial Identity?

Do you feel prepared to transact safely and securely online and on mobile devices? Test your knowledge on financial identity fraud and best practices with this financial identity quiz.

1 Which are considered part of your financial identity?

A. Bank account and routing numbers
B. Username (e.g., @myname) of a mobile wallet
C. Phone number
D. Facebook account
E. All of the above

2 Which activity accurately describes synthetic identity theft?

A. A criminal creating a new identity using pieces of real people's financial identity information
B. A criminal creating a completely false identity to open and use financial accounts
C. A criminal creating fake, physical copies of your credit cards
D. A criminal creating copies of your fingerprints to log in to your banking applications
E. All of the above

3 Victims of financial identity crime often feel:

A. 😠 *Angry*
C. 😳 *Shocked*
B. 😭 *Sad*
D. 🤬 *Upset*
E. All of the above

4 What is the average timespan required to remediate an instance of identity theft?

A. The length of time required to move through the Starbucks line (<1 hour)
B. The length of a decent night's sleep (7 hours)
C. The length of a long weekend (3 days)
D. The time between bi-monthly paychecks (2 weeks)
E. Forever

5 What types of biometric safeguards are increasingly available for use with virtual banking authentication?

A. Fingerprint
B. Iris
C. Face
D. Behavioral
E. All of the above

6 What is an appropriate step to take if you become a victim of financial crime?

A. Tweet your laments to gain support from friends and family
B. Relax and hope your banking institution will sort everything out
C. Search for relatable memes
D. File a police report
E. Complain to your coworkers

Quiz Answers: 1. E 2. A 3. E 4. B 5. E 6. D

For more detailed information on protecting and managing other key elements of your identity footprint online please check out the Identity Awareness, Protection and Management Guide.

IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

A GUIDE FOR ONLINE PRIVACY AND SECURITY COMPRISED OF THE COMPLETE COLLECTION OF DEPARTMENT OF DEFENSE SMART CARDS

SIXTH EDITION, MARCH 2018

BROUGHT TO YOU BY:

U.S. DEPARTMENT OF DEFENSE

Send an email to this address to get your copy!
OSD.NCR.OSD.MBX.DODSMARTCARDS@MAIL.MIL