Understanding Users and Stopping Criminal Activity

Julie Magee

credit karma

Background on Credit Karma

- *Free credit scores, credit reports, credit monitoring, financial management tools and more*
  - *Over 60M members*
  - *Over 1B scores to consumers*
  - *Over $500M in revenue*
  - *Nearly 1M tax filings last year*
- *Helping members make financial progress*
- *In the US and parts of Canada*
- *Offices in San Francisco, Los Angeles, Charlotte, Cary*

credit karma™

Agenda

- *Criminal use of tax products*
- *Understanding users*
- *Preventing criminal activity*

credit karma™

Criminal Use of Tax Products

credit karma™

First - Understand the Threat

- *How can you protect what you do not understand?*
  - *Understand the attack vectors*
    - *What can criminals gain from your product/service?*
    - *What value do you provide in the ecosystem?*
    - *What information do you have of value?*
- *What are the main threats you are protecting against?*
  - *What are the economics of the threat?*
  - *Non-economic based threats (state sponsored, ideological, etc.)*

Scoping Fraud Markets

- *Total addressable fraud market concept*
  - *How much money is in your ecosystem?*
- *Fraud is a vicious cycle*
  - *If criminals are making money; they will want more money!*
  - *Fraudsters talk to each other*

Scope of Problem - Tax Refund Fraud

GAO Highlights

Highlights of GAO-15-119, a report to congressional requesters

Why GAO Did This Study

IRS estimated it prevented $24.2 billion in fraudulent identity theft (IDT) refunds in 2013, but paid $5.8 billion later determined to be fraud. Because of the difficulties in knowing the amount of undetected fraud, the actual amount could differ from these point estimates. IDT refund fraud occurs when an identity thief uses a legitimate taxpayer's identifying information to file a fraudulent tax return and claims a refund.

GAO was asked to review IRS's efforts to combat IDT refund fraud. This report, the second in a series, assesses (1) the quality of IRS's IDT refund fraud cost estimates, and (2) IRS's progress in developing processes to enhance taxpayer authentication.

GAO compared IRS's IDT estimate methodology to *GAO Cost Guide* best practices (fraud is a cost to taxpayers).

January 2015

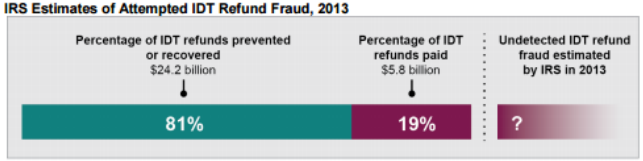
IDENTITY THEFT AND TAX FRAUD

Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks an Estimate of Costs, Benefits and Risks

What GAO Found

Identity Theft (IDT) Refund Fraud Cost Estimates. The Internal Revenue Service's (IRS) fraud estimates met several *GAO Cost Guide* best practices, such as documenting data sources and detailing calculations. However, the estimates do not reflect the uncertainty inherent in measuring IDT refund fraud because they are presented as point estimates. Best practices suggest that agencies assess the effects of assumptions and potential errors on estimates. Officials said they did not assess the estimates' level of uncertainty because of resource constraints and methodological challenges. Because making different assumptions could affect IDT fraud estimates by billions of dollars, a point estimate (as opposed to, for example, a range) could lead to different decisions about allocating IDT resources. Reporting the uncertainty that is already known from IRS analysis (and conducting further analyses when not cost prohibitive) might help IRS communicate IDT refund fraud's inherent complexity.

IRS Estimates of Attempted IDT Refund Fraud, 2013



Source: GAO analysis of IRS data. | GAO-15-119

$5.8 Billion

credit karma

UNITED STATES SENATE
COMMITTEE ON FINANCE

ABOUT | HEARINGS | LEGISLATION | NEWSROOM | NOMINATIONS | LIBRARY

HOME / HEARINGS

Full Committee Hearing

Tax Fraud and Tax ID Theft: Moving Forward with Solutions

Date: Tuesday, April 16, 2013
Time: 10:00 AM
Location: 215 Dirksen Senate Office Building

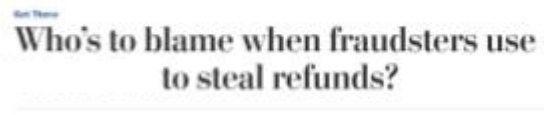
credit karma

Media Coverage


Phishing, E-Filing, And IRS Security

Imagine getting an email from [illegible] but says "Congratulations on filing your federal tax return!" There's only one problem: you haven't yet filed. So what about that refund you thought you were getting? Given that virtually everything is electronic these days, security and return fraud has become a massive issue, especially this year. It may make you long for the good old days.


Sued Over [illegible] ecurity And Identity Theft, Status Sought


Who's to blame when fraudsters use to steal refunds?


Local police give tips on what to do if tax fraud occurs

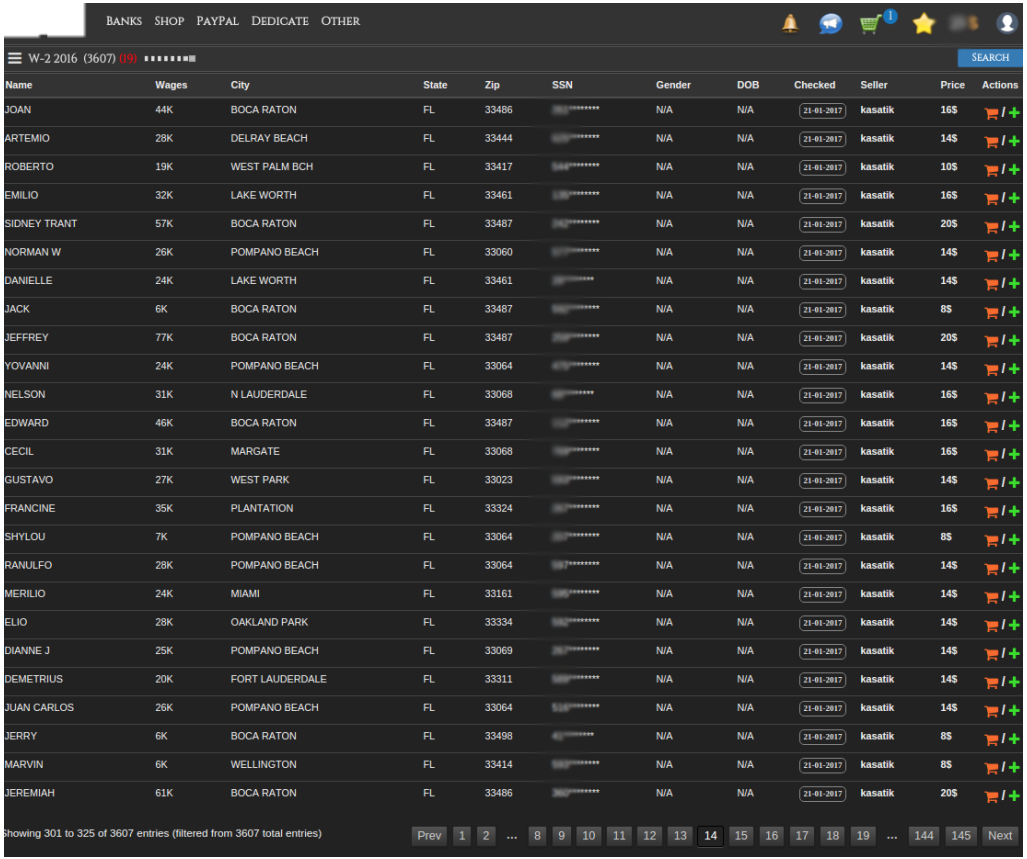

Fraud Alert: What [illegible] Users Need to Know


KrebsonSecurity

22 Anti-Fraud Efforts Under Scrutiny

credit karma

W2s For Sale in the Underground Market



BANKS SHOP PAYPAL DEDICATE OTHER

W-2 2016 (3607) (19) SEARCH

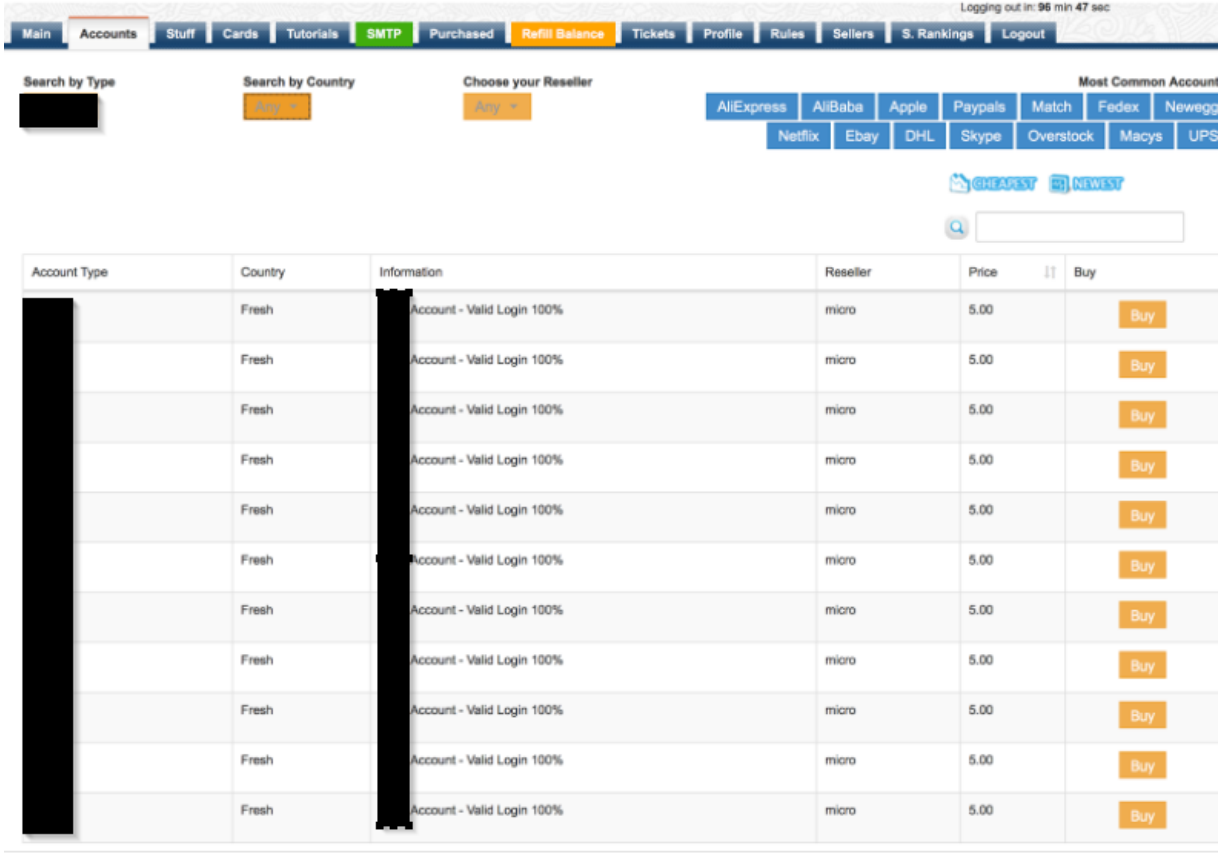
Name	Wages	City	State	Zip	SSN	Gender	DOB	Checked	Seller	Price	Actions
JOAN	44K	BOCA RATON	FL	33486	[redacted]	N/A	N/A	21-01-2017	kasatik	16$	
ARTEMIO	28K	DELRAY BEACH	FL	33444	[redacted]	N/A	N/A	21-01-2017	kasatik	14$	
ROBERTO	19K	WEST PALM BCH	FL	33417	[redacted]	N/A	N/A	21-01-2017	kasatik	10$	
EMILIO	32K	LAKE WORTH	FL	33461	[redacted]	N/A	N/A	21-01-2017	kasatik	16$	
SIDNEY TRANT	57K	BOCA RATON	FL	33487	[redacted]	N/A	N/A	21-01-2017	kasatik	20$	
NORMAN W	26K	POMPANO BEACH	FL	33060	[redacted]	N/A	N/A	21-01-2017	kasatik	14$	
DANIELLE	24K	LAKE WORTH	FL	33461	[redacted]	N/A	N/A	21-01-2017	kasatik	14$	
JACK	6K	BOCA RATON	FL	33487	[redacted]	N/A	N/A	21-01-2017	kasatik	8$	
JEFFREY	77K	BOCA RATON	FL	33487	[redacted]	N/A	N/A	21-01-2017	kasatik	20$	
YOVANNI	24K	POMPANO BEACH	FL	33064	[redacted]	N/A	N/A	21-01-2017	kasatik	14$	
NELSON	31K	N LAUDERDALE	FL	33068	[redacted]	N/A	N/A	21-01-2017	kasatik	16$	
EDWARD	46K	BOCA RATON	FL	33487	[redacted]	N/A	N/A	21-01-2017	kasatik	16$	
CECIL	31K	MARGATE	FL	33068	[redacted]	N/A	N/A	21-01-2017	kasatik	16$	
GUSTAVO	27K	WEST PARK	FL	33023	[redacted]	N/A	N/A	21-01-2017	kasatik	14$	
FRANCINE	35K	PLANTATION	FL	33324	[redacted]	N/A	N/A	21-01-2017	kasatik	16$	
SHYLOU	7K	POMPANO BEACH	FL	33064	[redacted]	N/A	N/A	21-01-2017	kasatik	8$	
RANULFO	28K	POMPANO BEACH	FL	33064	[redacted]	N/A	N/A	21-01-2017	kasatik	14$	
MERILIO	24K	MIAMI	FL	33161	[redacted]	N/A	N/A	21-01-2017	kasatik	14$	
ELIO	28K	OAKLAND PARK	FL	33334	[redacted]	N/A	N/A	21-01-2017	kasatik	14$	
DIANNE J	25K	POMPANO BEACH	FL	33069	[redacted]	N/A	N/A	21-01-2017	kasatik	14$	
DEMETRIUS	20K	FORT LAUDERDALE	FL	33311	[redacted]	N/A	N/A	21-01-2017	kasatik	14$	
JUAN CARLOS	26K	POMPANO BEACH	FL	33064	[redacted]	N/A	N/A	21-01-2017	kasatik	14$	
JERRY	6K	BOCA RATON	FL	33498	[redacted]	N/A	N/A	21-01-2017	kasatik	8$	
MARVIN	6K	WELLINGTON	FL	33414	[redacted]	N/A	N/A	21-01-2017	kasatik	8$	
JEREMIAH	61K	BOCA RATON	FL	33486	[redacted]	N/A	N/A	21-01-2017	kasatik	20$	

Showing 301 to 325 of 3607 entries (filtered from 3607 total entries)

Prev 1 2 ... 8 9 10 11 12 13 14 15 16 17 18 19 ... 144 145 Next

credit karma™

Major Tax Preparer Accounts for Sale in the Underground



Logging out in: 96 min 47 sec

Main | Accounts | Stuff | Cards | Tutorials | SMTP | Purchased | Refill Balance | Tickets | Profile | Rules | Sellers | S. Rankings | Logout

Search by Type [redacted]

Search by Country: Any

Choose your Reseller: Any

Most Common Account: AliExpress | AliBaba | Apple | Paypals | Match | Fedex | Newegg | Netflix | Ebay | DHL | Skype | Overstock | Macys | UPS

CHEAPEST | NEWEST

Account Type	Country	Information	Reseller	Price	Buy
[redacted]	Fresh	[redacted] Account - Valid Login 100%	micro	5.00	Buy
	Fresh	Account - Valid Login 100%	micro	5.00	Buy
	Fresh	Account - Valid Login 100%	micro	5.00	Buy
	Fresh	Account - Valid Login 100%	micro	5.00	Buy
	Fresh	Account - Valid Login 100%	micro	5.00	Buy
	Fresh	Account - Valid Login 100%	micro	5.00	Buy
	Fresh	Account - Valid Login 100%	micro	5.00	Buy
	Fresh	Account - Valid Login 100%	micro	5.00	Buy
	Fresh	Account - Valid Login 100%	micro	5.00	Buy
	Fresh	Account - Valid Login 100%	micro	5.00	Buy

credit karma™

Other Types of Fraud

- *Tax Refund Fraud is the main issue, however…*
  - *Blackmail*
  - *Identity theft*
  - *Employment fraud*
  - *Wire fraud*
  - *Money laundering (fraudulent refunds crossing state lines and U.S. borders)*
  - *Criminal conspiracies to defraud the government and to use financial institutions in facilitation of fraud*
  - *Bank fraud, mail fraud… etc., etc.*
- *Tax data is valuable to criminals!!*

Understanding Users

credit karma™

User Behavior

- *Fraud behavior vs actual user behavior*
  - *Previously EITC and ACTC*
  - *What forms are filled in?*
  - *How fast do they click? What do they click? How do they navigate?*
  - *What do we know about the user history? What are they changing (e.g. bank account)?*
  - *What do we know about the device, identity, data from third parties (e.g. changing to bank account to prepaid debit card)?*

Preventing Criminal Activity

credit karma™

We Must Change the Economics

- *Change the economics*
  - *Make fraud unprofitable*
    - *Know Your Customer?*
    - *ID verification?*
    - *SMS verification?*
    - *W2 verification*
    - *Cost of credentials?*
    - *Cost of mules?*

Fraud Protection by Design

- *Require SMS verification*
  - *On upgrade to Credit Karma Tax account*
  - *On logins from new device*
- *1:1:1:1:1 relationship between*
  - *SSN: e-mail: phone: federal tax return: state tax return*

credit karma™

Fraud Prevention by Design

- *What does this prevent?*
  - *Higher bar for fraudster new account creation*
  - *Fraudsters cannot easily open new accounts to file taxes*
  - *Fraudsters therefore attempt to compromise a non-upgraded account*

- *Layered approach to fraud protection*
  - *Make things easier for good customers*
  - *Make things harder for fraudsters*

credit karma™

Upgrade Process

- *Already required identity match (with credit bureaus)*
  - *Knowledge Based Authentication*
- *Stronger password required*
- *Additional security question*
- *SMS verification*
- *Terms of service for Credit Karma Tax*

Guess where users dropped off?

credit karma™

SMS

- *Force all users to SMS verify (block VoIP)*
  - *Pros*
    - *Easily understood by users*
    - *Fairly easy and inexpensive to implement*
    - *Forces better security for ALL users -- not just the security-conscious*
    - *Phone is another source of intel + investigatable lead for LE*
    - *Almost all users have one*
  - *Cons*
    - *Open to intercept by attackers in privileged network positions*
    - *Phishable*
    - *Not as secure as other methods, but accessible*
      - *Security vs Usability*

SMS vs Security Questions

- *Issues with security questions*
  - *Lookup mother's maiden name in 10 sec. in California (https://www.californiabirthindex.org/)*
  - *Poor implementations and recall rate for users*
  - *Easy for fraudsters to Google/guess answers*
- *NIST 800-63*
  - *Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.*
  - *Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant.*

credit karma™

SMS vs Security Questions

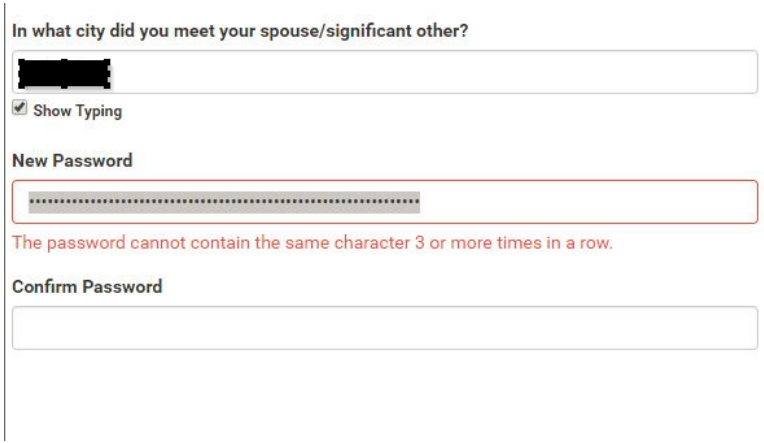
- *From Google research:*
  - *Only 40% of users were able to recover with security questions; 80% were able to recover with SMS*
  - *20% of attackers can successfully guess "Favorite Food" on the first try*
  - *"demonstrating that in practice secret questions have poor security and memorability"*
- *SMS account recovery*
  - *High recall*
  - *More expensive/time consuming for fraudsters to compromise*

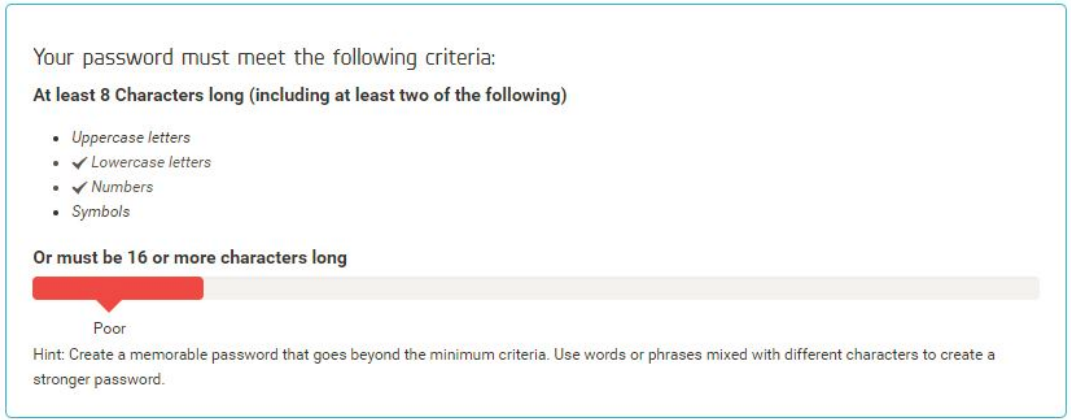
Strong Passwords?

- *New NIST guidance in 800-63-3b*
  - *Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets.*
- *The malware on your computer doesn't care how strong your password is…*
  - *What are we really securing against?*

Strong Passwords?

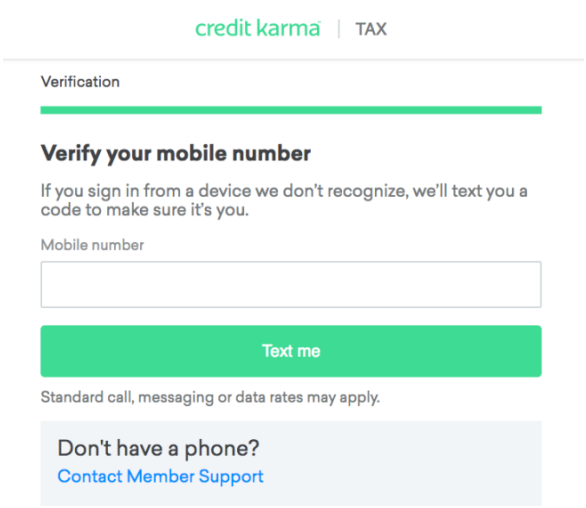
- *Password123! Is NOT strong…most websites will tell you it is…*
  - *Look at statistical distributions, use biometric data, understand your users better!*
- *Threat model should assume that all your users' passwords are compromised…because they likely are*

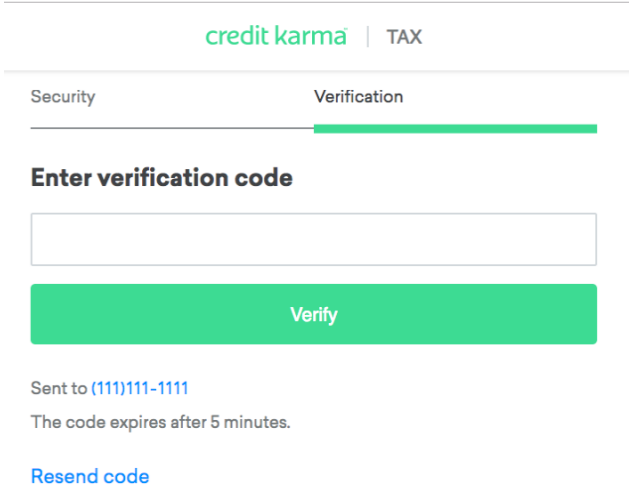




credit karma

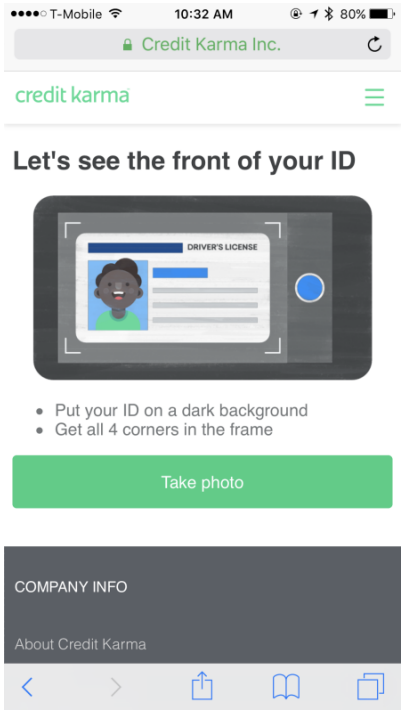
Member Experience

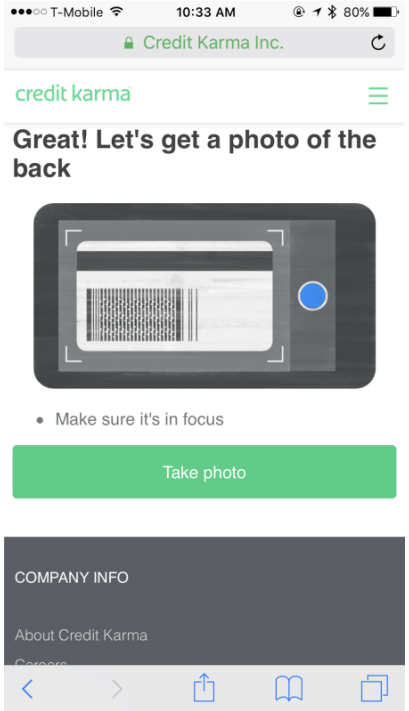




credit karma™

ID Verification





credit karma™

ID Verification

- *Analyze driver's license photos*
  - *OCR front*
  - *Barcode on back*
  - *Compare against known templates*
  - *ESF feature*
  - *Photos of photos*
  - *Comparison of data to credit reports, tax returns*

ID Verification

- *Positives*
  - *Automated; fast; relatively easy*
  - *Seen failures for: paper printouts; hole punched licenses*
  - *Better than most identity validation methods in use online*
- *Negatives*
  - *Glare is hard*
  - *Not everyone will do it*
  - *Extra friction*

Tax Fraud Trends

- *Minimal amount of effort for money*
  - *Rare for fraudsters to fill out many forms*
- *România*
  - *Prefer account compromise*
- *Nigeria*
  - *Prefer new account*
- *How much $$ is too much?*

credit karma™

Results

- *Force low end fraudsters out*
  - *Drop out at SMS*
- *High end fraudsters are still around*
  - *One time use devices, IPs, identities*
- *Increase attempts in account takeover*
  - *We have altered the fraud market*
- *Relationships with law enforcement and banks tremendously useful*

Stronger Together

- *How can everyone work together to more easily share fraud data within legal and regulatory constraints?*
  - ***Fraudsters evolve faster than legislators…***
- *Collaboration with peers/law enforcement *directly* impacts fraudster's bottom lines and maybe even put them in jail!*
  - *Hitting fraudsters where it hurts… the pocketbook!*
  - *Assist law enforcement to seize the fraudster's assets and arrest fraudsters for money laundering and other criminal violations*

Questions?

credit karma™

Appendix

credit karma™