



STATE OF HAWAII | KA MOKU'ĀINA 'O HAWAI'I
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS
KA 'OIHANA PILI KĀLEPA
335 MERCHANT STREET, ROOM 310
P.O. BOX 541
HONOLULU, HAWAII 96809
Phone Number: (808) 586-2850
Fax Number: (808) 586-2856
cca.hawaii.gov

JOSH GREEN, M.D.
GOVERNOR | KE KIA'ĀINA

SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

NADINE Y. ANDO
DIRECTOR | KA LUNA HO'OKELE

DEAN I HAZAMA
DEPUTY DIRECTOR | KA HOPE LUNA HO'OKELE

Testimony of the Department of Commerce and Consumer Affairs

Office of Consumer Protection

Before the
Senate Committee on Commerce and Consumer Protection
Wednesday, February 14, 2024
9:30 a.m.
Via Videoconference
Conference Room 229

On the following measure:
S.B. 2454, RELATING TO MAIL

Chair Keohokalole and Members of the Committee:

My name is Mana Moriarty, and I am the Executive Director of the Department of Commerce and Consumer Affairs' (Department) Office of Consumer Protection (OCP). The Department appreciates the intent of this bill, but notes that the Federal Trade Commission has a pending rulemaking proceeding that is likely to render the prohibitions in this bill redundant. See FTC Proposes New Rule to Combat Government and Business Impersonation Scams, Sep. 15, 2022.¹ The purpose of this bill is to prohibit certain entities from distributing unsolicited mail that is reasonably likely to cause the recipient to believe that a governmental agency has approved of the distribution.

¹ <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-proposes-new-rule-combat-government-business-impersonation-scams> (last visited Feb. 12, 2024).

The Department appreciates the intent of this measure to prohibit anyone from sending mail that could lead a recipient into thinking the mailing was from a government agency. The Federal Trade Commission (FTC) reported that complaints about government impersonation scams rose sharply at the beginning of the COVID-19 pandemic. Impersonators can pose as government officials or employees to fish for information they can use to commit identity theft or seek monetary payment. Imposter scams surged during the pandemic and continue today because the opportunities to scam various types of consumers have increased – whether it is a student seeking loan forgiveness or a senior on Medicaid. According to the FTC, the number one fraud category nationwide in 2023 was imposters scams. In Hawaii, imposter scams ranked as the third most reported fraudulent crime during the same period.

The Department notes that there are limitations on our ability to enforce a prohibition on business-to-business solicitations that are prohibited in this bill. For example, a company that mails a business owner an offer to register their company with the Business Registration Division (BREG) of the Department for a fee would likely violate the act; however, the Department's enforcement authority is limited to enforcement of violations of consumer protections. A consumer is defined as a natural person who, primarily for personal, family, or household purposes, purchases, attempts to purchase, or is solicited to purchase goods or services or who commits money, property, or services in a personal investment (§480-1, Hawaii Revised Statutes). Because the business who is solicited for this fraudulent service is not technically a consumer, the Department could not enforce the prohibition in this scenario.

Thank you for the opportunity to testify on this bill.



NATIONAL
ASSOCIATION OF
ATTORNEYS GENERAL

PRESIDENT

Tom Miller

Iowa
Attorney General

PRESIDENT-ELECT

Josh Stein

North Carolina
Attorney General

VICE PRESIDENT

Ellen F. Rosenblum

Oregon
Attorney General

IMMEDIATE PAST
PRESIDENT

Karl A. Racine

District of Columbia
Attorney General

Chris Toth

Executive Director

1850 M Street NW
12th Floor
Washington, DC 20036
(202) 326-6000
www.naag.org

February 22, 2022

Lina M. Khan, Chair
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Impersonation ANPR; FTC File No. R207000 – Trade Regulation Rule
on Impersonation of Government and Businesses

Dear Ms. Khan:

The undersigned attorneys general, led by the attorneys general of Florida, Iowa, Mississippi, Pennsylvania, and Tennessee (“attorneys general”), write in response to the Federal Trade Commission’s (“FTC”) Advance Notice of Proposed Rulemaking and Request for Public Comment concerning impersonation scams. Attorneys general appreciate the opportunity to address the important issues implicated by the FTC’s contemplated rulemaking to ensure that consumers are protected from the harms of such scams.

Attorneys general are uniquely qualified and well-positioned to provide insights regarding impersonation scams. As the chief law enforcement officials of their respective jurisdictions, attorneys general often act as a “front line” defense against impersonation frauds. Consumers commonly file large volumes of complaints about such activities with attorneys general. In addition to constantly receiving and evaluating consumer complaints, attorneys general are charged with protecting consumers from fraud through the dutiful administration of consumer protection laws, sometimes called unfair and deceptive acts or practices (“UDAP”) laws or mini-FTC Acts.¹ Also, attorneys general often work collaboratively in other ways. For

¹ Examples of such laws include the Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1 et seq., the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1 et seq., Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, Florida Statutes (“FDUTPA”) and the Iowa Consumer Frauds Act, Iowa Code § 714.16.

example, attorneys general have commissioned a National Association of Attorneys General “imposters” working group to keep abreast of issues relating to impersonation scams, share intelligence, and coordinate responses on a regular and ongoing basis. Further, attorneys general typically engage in consumer outreach and education efforts to warn consumers about how to avoid becoming victims of impersonation frauds. These activities have provided attorneys general in-depth knowledge and experience of impersonation scams, which they offer in service of the FTC’s request for comment.

Attorneys general have not attempted to answer all the questions posed in the Advanced Notice of Rulemaking but have addressed the ones most important to protecting consumers. Overall, attorneys general believe there is a pressing need for FTC rulemaking to address the scourge of impersonation scams impacting consumers across the United States. A national rule that encompasses and outlaws such commonly experienced scams discussed herein would assist attorneys general and their partners in reducing consumer harm, maximizing consumer benefits, and holding bad actors to account.

I. THE WIDESPREAD IMPERSONATION SCAMS TARGETING AMERICAN CONSUMERS

Impersonation scams are a pervasive problem impacting millions of American consumers. The numbers of consumer complaints regarding impersonation scams received by specific attorneys general can vary, but they illustrate that impersonation scams are a serious problem. Several examples of complaint volumes in specific jurisdictions during years 2019 through 2021 are instructive. For example, the Arizona Attorney General’s Office received over 1,700 consumer complaints about impersonation scams during that time, including all government, business, and individual imposter scam categories. Likewise, total consumer complaints regarding all imposter categories were as follows for several other attorneys general: Arkansas (over 1,100), Iowa (over 1,000), North Carolina (over 2,200), and Washington (over 2,100).

In Florida, where the complaint volume reached almost 5,000 from 2019 through 2021, numerous impersonators were held responsible by way of litigation filings by the Florida Attorney General’s Office, which resulted in more than 10 consent final judgments entered in a variety of government imposter and business/tech scams, yielding permanent injunctive relief and monetary relief in the millions.

And while the volume of consumer complaints filed with attorneys general are alarming, consumer complaints do not fully capture the reality regarding the number of imposter scam victims. One of the most nefarious aspects of impersonation scams is that many victims never become aware they were defrauded. Attorneys general often find that consumer complaint numbers are just the “tip of the iceberg” in terms of actual victims impacted by specific imposter activities.

For example, the Iowa Attorney General received only four total consumer complaints regarding a specific “certificate of existence” government imposter scam operation discussed below. However, the Iowa Attorney General’s subsequent investigation

uncovered that over 1,200 Iowa consumers had purchased the unnecessary certificate. None of the non-complainant consumers the Iowa Attorney General's investigators interviewed indicated that they had even realized they had been scammed because the consumers believed the government imposter mailer was a required government invoice. There was no obvious reason for consumers to review the transactions after they had already occurred.

Similarly, the Tennessee Attorney General's Complaint against "Mandatory Poster Agency" et. al (which is also discussed below) noted that "[a]t least 35 Tennessee consumers had complained" about the company's government imposter activities, but "[t]housands of other Tennessee businesses are likely unaware that they have needlessly paid Defendants hundreds of thousands of dollars over the years, precisely because those business owners believe that Defendants are part of or acting on behalf of the Tennessee government and that they are required to respond to Defendants' mailers and send them money."

In yet another example, the Iowa Attorney General received only two consumer complaints regarding companies discussed below that were sending older Iowans misleading government imposter mailers requesting them to return personal information about themselves to generate telemarketing leads for insurance salespersons. However, the Iowa Attorney General's subsequent investigations of the companies revealed that, between them, hundreds of Iowa consumers had returned personal information and the companies sent thousands of mailers to Iowans. The vast majority of the impacted consumers were unaware they had been targeted and would not have had cause to complain.

A. Impersonation of Government Entities

1. Document Preparation Scams

Attorneys general find that it is commonplace for bad actors to employ government imposter tactics at the expense of consumers. In particular, consumers who start small businesses and charities often navigate the process of legally formalizing the corporate entity without the assistance of legal counsel. They can become easily confused regarding associated legal requirements and paperwork. For example, unsophisticated consumers may not grasp the legal distinctions between a "certificate of organization" necessary to formalize an LLC, and a "certificate of existence [or good standing]" or a "certificate of status" merely attesting to the fact that a business is in good standing pursuant to a loan application. These conditions are ripe for predatory actors to blur the meaning and import of various government forms and procedures to their benefit.

One operation allegedly induced thousands of consumers in multiple states to buy an unnecessary "certificate of existence" for newly formed entities.² The operators regularly

² The allegedly deceptive mailer associated with the operation is attached to this comment as Attachment 1.

accessed public information from Secretaries of State or other agency websites where corporate documents are filed to harvest contact information regarding those consumers who recently started new businesses or charities. The operators used the information to send consumers a "Certificate of Existence [or Good Standing] Request Form" mailer that appeared to be a government invoice for a payment needed to complete the corporate entity formalization process. Although the certificates were available from the state for a nominal fee, the operation often peddled the certificates for more than a 1000% markup of their bona fide cost. These extreme "profits" stemming from the "service" of forwarding the certificates to consumers who unknowingly ordered them from a private company could be easily pocketed by the scammers or otherwise leveraged against the efforts of attorneys general investigating and prosecuting them.

Similar operations in Florida involving direct mail solicitations for certificates of status resulted in three filed lawsuits and two judgments since 2019. Two of the lawsuits resulted in a permanent injunction against Defendants, and monetary recovery which includes restitution, civil penalties, and attorney's fees. In addition, the attorneys general of Iowa, Michigan, Mississippi, and Utah have achieved settlements with or are currently prosecuting ongoing lawsuits against the participants of the operation or nearly identical operations in other states.

As another example, multiple attorneys general have taken legal action against or achieved settlement agreements with participants of a notorious operation targeting consumers in multiple jurisdictions over a protracted period.³ The company names used by the operators varied, including "Corporate Records Service," "Labor Law Poster Service," "Mandatory Poster Agency," and others. These generically-named companies send mailer solicitations that many attorneys general have alleged appear to consumers as government invoices for documents one can easily obtain from Secretaries of State for a nominal fee. The Florida Attorney General brought action in 2019⁴ and the Tennessee Attorney General also recently brought an action against the purveyors of the operation. The Tennessee Attorney General's Complaint against them references the fact that the Defendants had already been "subject to law enforcement actions in multiple states," including at least "Alabama, Arizona, Colorado, Delaware, Florida, Idaho, Illinois, Indiana, Iowa, Kentucky, Louisiana, Michigan, Missouri, Nebraska, New Hampshire, North Carolina, North Dakota, Wisconsin, Utah, and the United States Postal Inspection Service." Yet, "[d]espite an avalanche of complaints from consumers in Tennessee and throughout the country, F rating from the BBB, and government warnings, [they] remain undeterred and their misconduct continues."

2. Regulatory Compliance Scams

³ Allegedly deceptive mailers associated with the operation are attached to this comment as Attachment 2.

⁴ Kylie Mason, *Attorney General Moody Takes Action to Shutdown Imposter Scam*, OFFICE OF THE ATTORNEY GENERAL OF FLORIDA (Mar. 6, 2019), <http://www.myfloridalegal.com/newsrel.nsf/newsreleases/4C4154E8189472AB852583B5005AEB84?Open&>

Many government imposter scams do not target broad swaths of consumers starting all manner of small businesses and charities, but instead focus on niche industries involving workers tasked with fulfilling regulatory reporting requirements. For example, motor carriers must file a free and simple report with the United States Department of Transportation biennially. Carriers can complete the biennial report on the agency's website. At least two companies, using publicly available information, send motor carriers mailer solicitations to file reports on behalf of carriers in exchange for a fee. One company's mailer warned recipients that a "failure to complete a Biennial Update may result in deactivation of your USDOT number and may result in civil penalties of up to \$1,000 per day..."⁵ The Iowa Attorney General accused both companies of engaging in a government imposter scam by purposefully designing the solicitations to mislead recipients that they were a government agency notice threatening fines against those carriers who failed to respond with payment.

By way of further example, in December 2020, the Pennsylvania Office of Attorney General entered into a settlement with Unified Holding Group, LLC, which did business as "Student Education Center" ("SEC"). SEC allegedly made telephone solicitations to Pennsylvania consumers and offered services to reduce or eliminate consumers' student loan debt. Beyond the use of telephone solicitations, SEC allegedly represented themselves as a new servicer on their website and posted fraudulent reviews—purportedly from customers nationwide—on the Better Business Bureau's website. In fact, SEC was not a servicer of student loan debt, and the company allegedly tricked Pennsylvania consumers out of at least \$74,000.00 in fees for enrolling them into Income Driven Plans, which are free to enroll in. In the settlement, the company agreed to refund fees, pay \$50,000.00 in costs and penalties and to cease operations in Pennsylvania.

3. Lead Generation Scams and Others Targeting Specific Populations

Other government impersonation scams target specific populations that can be more vulnerable to them. For example, some lead generation companies send mailer solicitations to older consumers requesting them to return personal information they will sell to insurance salespersons for subsequent telemarketing purposes.⁶ The mailers can include headers like "2019 Benefit Information For [Recipient's state] Citizens Only," and language like: "As a resident of [Recipient's state], you are entitled to more benefits not provided by government funds. You now have access to a 2019 regulated program which may pay 100% of all final expenses... Return this postage paid card within 5 days to request this new benefit information." The envelope including the solicitations may contain

⁵ Eric Miller, *FMCSA: Beware of Companies Posing as Government Agencies*, TRANSPORT TOPICS (Apr. 13, 2021), <https://www.ttnews.com/articles/fmcsa-beware-companies-posing-government-agencies#:~:text=Iowa%20Attorney%20General%20Tom%20Miller,updating%20the%20MC%20S%20D150%20form>

⁶ The allegedly deceptive mailer associated with the operation is attached to this comment as Attachment 3.

statements conveying an unjustified sense of urgency to respond, such as: “Dated Material,” “Open Immediately,” “Important Information Enclosed,” and “Second Notice: Time Sensitive.” These tactics can be particularly confusing to older consumers, who may respond believing they are applying for government help but instead receive aggressive telemarketing calls from insurance agents who commission the solicitations.

Some government impersonation scams target specific classes of people like teachers and other public employees earning a pension. The Indiana Attorney General recently filed a lawsuit against PERA, LLC, alleging the company sent email solicitations to “at least 70,000” Indiana employees that “contain[ed] characteristics or language that imply or would lead consumers to believe that the solicitation is sent from the Indiana Public Retirement System (“INPRS”) or an approved . . . service provider.” The messages allegedly stated that, “Each year, as an employee of [organization] you are eligible to schedule a phone call or teleconference meeting with a representative for answers to your specific state, federal and individual retirement benefit questions.” The Indiana Attorney General’s Complaint alleged these solicitations implied “that the solicitation offered an INPRS related benefit rather than a sales appointment for products not affiliated with the recipient’s employment.”

While many government imposter scams tend to solicit consumers via the United States Postal Service, others use the internet and search engine optimization to impersonate the government. In one such imposter scam, a web-based concealed weapons permit “assistance” service operating in Florida misled consumers to believe that either they were dealing directly with the state or that the business was affiliated in some way with the government. The Florida Attorney General’s lawsuit resulted in a permanent injunction, restitution, a civil penalty, and attorney’s fees.

B. Impersonation of Businesses

Year to year, impersonation of businesses is a persistent problem reported to state consumer protection agencies, either outpacing or running a close second to government imposter scams. An exact count is difficult due to differences in categorization from state to state, but business imposter scams have targeted thousands of consumers nationwide, with the number of complaints increasing over the last several years.

1. Impersonation Scams Involving False Affiliations with Other Businesses

Business imposter scams can be separated into two general categories. In the first category, the imposter claims to be either working directly for an actual business or else for a third party endorsed by that business. A common example is a tech support scam, in which the imposter claims that they are contacting the consumer on behalf of Microsoft or Apple to convince the consumer to grant the imposter remote access to their computer. The imposter is then able to access personal information or else direct the consumer to pay for unnecessary, overpriced software. For example, the Pennsylvania Office of Attorney General in collaboration with Connecticut Office of Attorney General and the FTC took

enforcement action against Click4Support, LLC, iSourceUSA LLC, Innovazion Inc., Spanning Source LLC and their officers, which resulted in a judgment exceeding \$27 million against certain of the defendants. These companies allegedly engaged in a scam in which they would promote themselves via popup advertisements made to look like warnings. When consumers called in, telemarketers would allegedly portray the company as being affiliated with tech companies including Apple, Google, Dell and Microsoft, according to the lawsuit. After being granted remote access to consumers' computers, the imposter would perform actions to cause error and warning messages to be displayed, as alleged. The imposters would use this to pressure consumers into paying thousands of dollars in some cases for "technical support services," which in some cases amounted to simply deleting harmless files or replacing existing antivirus software with other programs, according to the lawsuit.

Imposters have also commonly posed as a consumer's energy company or bank. These scams typically occur over the phone, but scammers have also reportedly used letters bearing the logo of the business they are imitating to the same effect.

In 2020 and 2021, the Florida Office of the Attorney General obtained six consent judgments against a variety of Defendants engaged in a tech support scam which is believed to have impacted as many as 70,000 people nationwide. In this far-reaching business imposter scam, the imposters posed as reputable companies and placed telemarketing calls to consumers offering to perform a complimentary computer diagnostic to ensure the consumer's computer was secure. The companies also marketed through pop-up advertisements that would appear as purported security or virus alerts from reputable software providers directing the consumer to call a phone number for assistance. Those calls were directed to affiliated call centers that conducted the same deceptive sales pitch. The Judgments resulted in both permanent injunctions and monetary relief to consumers.⁷ In 2020, the Florida Office of the Attorney General obtained a consent final judgment against another similar business imposter which used outbound calls to deceptively alert consumers that their computer was infected with a virus or was in imminent danger and needed immediate servicing.

2. Impersonation Scams Exploiting the Appearance of Legitimacy

In the second category of business imposter scams, an individual, utilizing either a fictitious name or an actual business entity, uses the apparent legitimacy of a business name to convince consumers to engage in fraudulent or deceptive conduct. In one 2019 case, the Arizona Office of Attorney General obtained a consent judgment against several LLCs for running a "toner pirate" scam, through which the imposters sent fake toner cartridge invoices to churches, schools and businesses. The Defendants pretended to be the companies that the consumers were currently using for ink cartridges. The Defendants in

⁷ Kylie Mason, *VIDEO CONSUMER ALERT: Millions Available for Victims of Tech Support Scams*, OFFICE OF THE ATTORNEY GENERAL OF FLORIDA (NOV. 4, 2019) <http://www.myfloridalegal.com/newsrel.nsf/newsreleases/A8A2B18B402DFBC4852584A8005004B2?Open&>

that single case were required to pay over \$400,000.00 in restitution. These scams need not even involve fake products, as in the case of another scam that relies on apparent legitimacy, the fake shipping scam. In a fake shipping scam, the imposter purchases a large quantity of a product using a stolen credit card and requests that the seller pay a preferred shipping company, with the promise of later reimbursement. In fact, the shipping company does not exist, but instead the scammers are using fictitious shipping services and keeping the “shipping fee.” Though there are myriad other methods by which a business imposter scam may occur, these cases are illustrative of some typical means used by scammers and the serious financial impact they can inflict on consumers and small businesses. As in the first category of business imposter scams, these imposters may establish their legitimacy first via telephone calls, but they may also go as far as to create realistic-looking invoices or even a website.

3. Impersonation Scams Involving Person-to-Person Deceptions

Imposter scams are not limited to situations where a government agency or business is being impersonated. State consumer protection agencies also receive, cumulatively, thousands of complaints every year regarding imposter scams that do not cleanly fit into any single category.

Some of these “miscellaneous” scams may occur over the phone, as in the case of a “grandparent scam,” in which the victim receives a call from someone posing as their grandchild, who frantically claims to be in trouble and in need of immediate money. Another scam is known as a “romance scam,” which typically begins on a dating app, where the imposter has assumed a fake identity, which they use to gain a victim’s trust to deceive them into wiring money to pay for items such as travel documents or plane tickets for a trip to visit the victim which never materializes. FTC data show hundreds of millions in losses due to romance scams, and data from state consumer protection agencies suggests that these scams are only becoming more common.

II. THE MEANS AND INSTRUMENTALITIES EFFECTUATING IMPERSONATION FRAUD MUST BE ADDRESSED

A. Common Tools of Impersonation Fraud Should be Explored

The businesses and individuals that impersonate government entities and other businesses are not the only participants in impersonation schemes that defraud millions of consumers each year. Impersonators often use other companies’ products and services to execute their scams. As with other types of consumer fraud, impersonators often use marketing companies, call centers, attorneys, third-party mailing services, payment processors, lead list providers, remote offices, and other platforms to expand their reach to consumers, to make their advertisements look more official, to appear “local,” or to mimic different facets of government entities and other companies. For example, in *F.T.C. v. Your Yellow Book, Inc.*, Your Yellow Book purchased customer lists from a third-party website and used customer contact information in the lists to send deceptive mailers that resembled an invoice for a

12-month subscription for "Your Yellow Book Internet Listing." No. CIV-14-786-D, 2014 WL 4187012, at *1, *7 (W.D. Okla. Aug. 21, 2014).

Another example of impersonators using an instrumentality to effectuate their scams involves using third-party payment processing services. Scammers often require certain payment methods for fictitious overdue debts (mortgages, utilities, student loans, etc.). In another common scam, a person posing as a government official tells a consumer that his identity has been compromised and that he must transfer money to the official using a pre-paid debit card in order to protect his accounts. Many government agencies have issued press releases and warnings trying to stem the proliferation of this government imposter scam. See, e.g., *Taxpayers should watch out for gift card scam*, IRS TAX TIP 2019-165 (Nov. 27, 2019), <https://www.irs.gov/newsroom/taxpayers-should-watch-out-for-gift-card-scam>. Further, in 2018, the attorneys general of Pennsylvania and New York announced that three national retailers, Walmart, Target and Best Buy, had voluntarily agreed to change their gift card policies to prevent these scams, taking steps including reductions in the amounts that can be placed on individual gift cards, restrictions on the redemption of retail gift cards for other gift cards and enhanced employee training to recognize the warning signs of a gift card scam. See, *Attorney General Josh Shapiro Announces Nationwide Gift Card Policy Changes from Walmart, Target, and Best Buy to Protect Consumers From Scams* (Nov. 20, 2018), <https://www.attorneygeneral.gov/taking-action/attorney-general-josh-shapiro-announces-nationwide-gift-card-policy-changes-from-walmart-target-and-best-buy-to-protect-consumers-from-scams/>. While these affirmative steps are a critical facet of confronting imposter scams, government agencies must remain vigilant of novel attempts to use third-party payment processing services for fraudulent ends.

Dating websites and social media are other tools that impersonators utilize for their schemes. In 2020, consumers reported losses of \$304 million from romance scams. See Emma Fletcher, *Romance scams take record dollars in 2020*, CONSUMER PROTECTION DATA SPOTLIGHT (Feb. 10, 2021), <https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020>. The amount of money that people lost to social media scams more than tripled in the last quarter of 2020, after reported losses climbed to \$117 million in the first six months of the year. Emma Fletcher, *Scams starting on social media proliferate early 2020*, CONSUMER PROTECTION DATA SPOTLIGHT (Oct. 21, 2020), <https://www.ftc.gov/news-events/blogs/data-spotlight/2020/10/scams-starting-social-media-proliferate-early-2020#end1>. At the top of the list for social media scams were "[r]eports about ecommerce sites that don't deliver the goods." *Id.* In 2021, reports of social media scams skyrocketed. Emma Fletcher, *Social media gold mine for scammers in 2021*, Consumer Protection Data Spotlight (Jan. 25, 2022), <https://www.ftc.gov/news-events/blogs/data-spotlight/2022/01/social-media-gold-mine-scammers-2021>. "More than 95,000 people reported about \$770 million in losses to fraud initiated on social media platforms in 2021. Those losses accounted for about 25% of all reported losses to fraud in 2021 and represent a stunning eighteenfold increase over 2017 reported losses." *Id.*

Impersonators who combine multiple instrumentalities can increase the pervasiveness and effectiveness of their deceptive behavior. In the last year, for instance, many impersonators utilized the ubiquity of social media to receive their ill-gotten funds in the form of one of the least-regulated forms of payment—cryptocurrency. For example, last year, an impersonator using footage from the YouTube channel “Everyday Astronaut,” created a fake live stream of a space launch to solicit bitcoin donations under the guise of a fundraiser for St. Jude Children’s Hospital. Queenie Wong, *Cryptocurrency scams are all over social media. Don’t get duped.*, CNETMONEY (Nov. 10, 2021), <https://www.cnet.com/personal-finance/crypto/cryptocurrency-scams-are-all-over-social-media-dont-get-duped/>. Around the same time, imposters created Twitter accounts that appeared to be connected to a (non-existent) Squid Game crypto coin, swindling buyers out of more than \$2 million. *Id.* Impersonators could not defraud so many consumers without other companies’ means and instrumentalities.

B. Enablers of Impersonation Fraud Should be Held Accountable in Appropriate Circumstances

The staggering financial loss from impersonation fraud requires strong consideration of who should be held responsible for impersonation scams. In some cases, companies that facilitate impersonation schemes have sufficient information to detect wrongdoing but willfully turn a blind eye. Although few imposter cases have held these companies responsible for their contributions, cases in other consumer fraud contexts illuminate the standards that could be applied to those entities when there is sufficient evidence of culpability.

Some courts have held that companies may be responsible for fraudulent conduct when 1) they know or should have known that their products or services are used to perpetuate the fraud and 2) they have substantially contributed to the fraud. In *Brooks v. CommUnity Lending, Inc.*, the Northern District Court of California denied defendants’ motions to dismiss, including a motion disputing that RBS was responsible for CommUnity’s Truth in Lending violations. *Brooks v. CommUnity Lending, Inc.* No. C 07-4501 JF (PVT), 2010 WL 2680265 at *11 (N.D. Cal. July 6, 2010). The District Court found that plaintiff had appropriately pled that the RBS could be liable because RBS substantially assisted CommUnity by participating in the creation, design, and formulation of the loan documents CommUnity used. *Id.*

The United States District Court of Massachusetts ruled similarly when the plaintiff sought to amend his complaint to include Bank of America, the assignee of a mortgage and note originally issued by Southstar Funding, LLC. *McKensi v. Bank of Am.*, 2010 WL 3781841 at *1 and *4 (D. Mass. Sept. 22, 2010). In *McKensi*, the District Court allowed the plaintiff to include claims against Bank of America because it filed a foreclosure action when it knew or should have known that the mortgage was legally unenforceable. *Id.* Thus, when an entity provides substantial assistance or support to impersonators and knows or should have known that their products or services are being used in a fraudulent impersonation scheme, that company could also be held liable under the proposed impersonation rule.

See *Id*; *Brooks*, 2010 WL 3781841 at *11; 16 CFR 310.3(b) (creating a parallel impersonation rule with respect to any person who “provide[s] substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in any act or practice that violates §§ 310.3(a), (c) or (d), or § 310.4 of [the Deceptive telemarketing acts or practices] Rule.”

To be clear, businesses are often victims themselves, and often are partners with regulators in investigations of imposter schemes. But, when a business makes an intentional decision to substantially support or to willfully ignore an imposter scheme that does harm consumers, they should be held accountable for their part in that harm.

III. THE FAR-REACHING CONSUMER HARMS CAUSED BY IMPOSTER SCAMS

Impersonation scams cause injury to consumers in several ways. First, consumers who fall victim to impersonation scams lose money. Consumers can lose money even though the supposed “service” offered by the imposters often does not meet the requirements of the law, is unnecessary or is available through the state for free or a nominal fee. For example, in document preparation imposter scams, a consumer may receive a solicitation offering them “annual minutes” or “annual records” that appears to originate from the state. The consumers may respond with an unnecessary check to the imposter believing they met their annual filing requirements. They may not realize they paid for a product that is not required by the state until they later receive a notice from the state that the annual report is due. Consumers may lose additional money as a cost of curing errors stemming from the scam. For example, as a result of receiving a legitimate notice from the state that an annual report is due after having already sent a check to an imposter, the consumer must still pay to renew their business registration through the proper channels. They often pay hundreds of additional dollars in addition to the unnecessary amount they lost to the scammer to ensure they are compliant.

Second, imposter scams drain the limited resources of regulators tasked with protecting the public from a wide range of other harms. The amount each consumer loses to impersonation scams is often significant to them but is almost invariably insufficient to justify the burdens of private litigation that may be required to recover the money without government intervention. Simply put, scammers are often counting on the fact that consumers rarely have the time and resources to hold them accountable by themselves and hope to avoid the attention of regulators. For example, to keep “under the radar” of regulators, they may offer to refund only those few consumers who notice they have been scammed and complain to law enforcement. The imposters seem to believe this increases the appearance of legitimacy to regulators who investigate complaints about them. However, even if the per-consumer loss is relatively small in the grand scheme of a particular imposter operation, those scams involving hundreds or thousands of victims often return substantial sums of money to the scammer on the whole. The startup costs of running imposter scams are also typically low. Therefore, it is often incumbent upon government regulators to spend limited time and resources addressing the conduct. These

resources could be spent helping the public in other ways if imposter scam activities were lessened.

Third, there are other less tangible but nonetheless troubling harms resulting from imposter scams. Government imposter scams can cause immense consumer confusion and loss of trust in government services and inquiries. Widespread mimicking of government documents contributes to the erosion of the state's status as an identifiable, trusted source of important information for the public. Business impersonation scams can cause consumer mistrust of technologies and well-known companies whose legitimacy scammers exploit. Consumers who fall victim to such scams often report they are unsure whether to trust future documents from the state, which may be wholly legitimate and beneficial to them.⁸

Finally, imposter scams cause unnecessary stress and embarrassment for consumer victims. This is especially problematic in person-to-person imposter scams, including grandparent and romance scams, which often involve the loss of thousands of dollars after deeply personal scams are perpetuated.

IV. THE BURGEONING NEED FOR A ROBUST NATIONAL STANDARD OUTLAWING IMPERSONATION SCAMS

A. The Need for New Regulation

The quantity and variety of the cases the states have seen manifest a need for new regulation from the Federal Trade Commission targeting government and business impersonation scams. Such scams are pervasive across the country and undermine the public's trust in government correspondence and business communications. When a specific type of unfair or deceptive business practice becomes so prevalent, Commission rulemaking is appropriate. Attorneys general welcome these efforts as part of their ongoing collaborative relationship with the FTC.

While impersonation scams affect all kinds of consumers, impostors themselves often target vulnerable and marginalized communities, including the elderly and the un-banked. State attorneys general play an important role in the prevention and redress of the harm these impostors cause, but a robust enforcement scheme at the federal level would help deter bad actors and reduce consumer harm. In addition, such a regulation could provide needed clarity on what conduct constitutes impersonation, since government and business impersonation scams can range from overt pretense to misleading subtlety. A robust national standard would also deprive bad actors of the excuse they were allegedly not

⁸ “[D]eceptive advertising engenders distrust, which negatively affects people's responses to subsequent advertising from both the same source and second-party sources. This negative bias operates through a process of defensive stereotyping, in which the initial deception induces negative beliefs about advertising and marketing in general, thus undermining the credibility of further advertising.” Peter R. Darke & Robin J.B. Ritchie, *The Defensive Consumer: Advertising Deception, Defensive Processing, and Distrust*, J. MARKETING RES. 44, 114-127 (2007).

aware their activities were illegal in some jurisdictions as opposed to others and provide more opportunities for the states to collaborate with the FTC on multistate enforcement actions against imposter scammers. At the same time, attorneys general believe the standard should act as a floor, making it clear that states are free to enforce their own standards, free of any preemption by a federal rule.

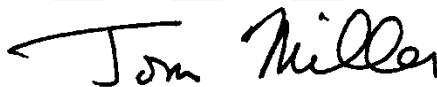
Any regulation that the FTC propounds should consider the viewpoints of all stakeholders, including the business community. However, the ultimate goal of the Commission's rulemaking should always be to reduce consumer harm and maximize consumer benefits. Rules the Commission propounds should also reach typical impersonation scam cases Attorney Generals encounter as outlined herein.

B. The Need for Continuing Consumer Education and Collaborative Prevention Efforts

The Commission should also publish additional consumer and business education materials to help prevent consumers from becoming victims of impersonation fraud. Attorneys general have much experience in this arena, as their outreach and education efforts have been successful in proactively addressing this issue, although more education is needed given the volume of complaints they receive. Attorneys general hope to continue working with the FTC and other partners to sound the alarm on impersonation scams. However, while education is one important tool in the fight against government and business impersonation scams, it must serve as a complement to a strong regulation with a robust enforcement scheme rather than as an alternative.



Ashley Moody
Florida Attorney General



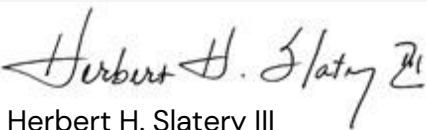
Tom Miller
Iowa Attorney General



Lynn Fitch
Mississippi Attorney General



Josh Shapiro
Pennsylvania Attorney General



Herbert H. Slatery III
Tennessee Attorney General



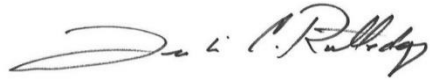
Steve Marshall
Alabama Attorney General



Treg R. Taylor
Alaska Attorney General



Mark Brnovich
Arizona Attorney General



Leslie Rutledge
Arkansas Attorney General



Phil Weiser
Colorado Attorney General



William Tong
Connecticut Attorney General



Kathleen Jennings
Delaware Attorney General



Karl A. Racine
District of Columbia Attorney General



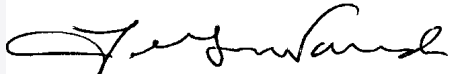
Christopher M. Carr
Georgia Attorney General



Leevin Taitano Camacho
Guam Attorney General



Holly T. Shikada
Hawaii Attorney General



Lawrence Wasden
Idaho Attorney General



Derek Schmidt
Kansas Attorney General



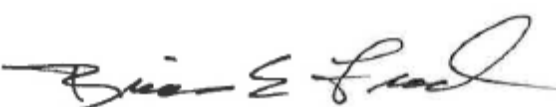
Daniel Cameron
Kentucky Attorney General



Jeff Landry
Louisiana Attorney General



Aaron M. Frey
Maine Attorney General



Brian Frosh
Maryland Attorney General




Maura Healey
Massachusetts Attorney General



Dana Nessel
Michigan Attorney General



Keith Ellison
Minnesota Attorney General



Eric S. Schmitt
Missouri Attorney General




Austin Knudsen
Montana Attorney General



Douglas Peterson
Nebraska Attorney General



Aaron D. Ford
Nevada Attorney General



John M. Formella
New Hampshire Attorney General



Matthew J. Platkin
Acting New Jersey Attorney General



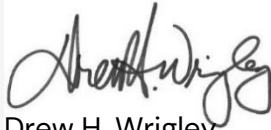
Hector Balderas
New Mexico Attorney General



Letitia James
New York Attorney General



Josh Stein
North Carolina Attorney General



Drew H. Wrigley
North Dakota Attorney General



Dave Yost
Ohio Attorney General



John O'Connor
Oklahoma Attorney General



Ellen F. Rosenblum
Oregon Attorney General



Peter F. Neronha
Rhode Island Attorney General



Alan Wilson
South Carolina Attorney General




Jason R. Ravensborg
South Dakota Attorney General



Ken Paxton
Texas Attorney General



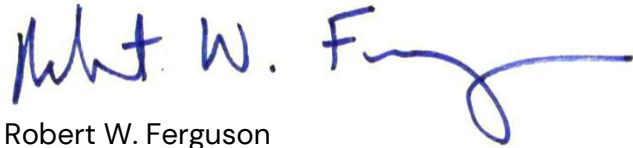
Sean D. Reyes
Utah Attorney General



T.J. Donovan
Vermont Attorney General



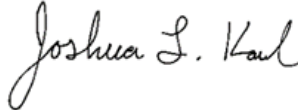
Jason S. Miyares
Virginia Attorney General



Robert W. Ferguson
Washington Attorney General



Patrick Morrisey
West Virginia Attorney General



Joshua L. Kaul
Wisconsin Attorney General



Bridget Hill
Wyoming Attorney General



T-2

2019 BENEFIT INFORMATION
FOR IOWA CITIZENS ONLY

2019

As a resident of Iowa, you are entitled to more benefits not provided by government funds.
You now have access to a 2019 regulated program which may pay 100% of all final expenses up to \$35,000.
Return this postage paid card within 5 days to request this new benefit information.


Please Respond By Dec. 7, 2018

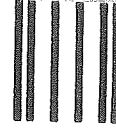
015250*****AUTO**5-DIGIT 50311 T51 P1



To opt out of future mailings please visit dmpoptout.com and enter this 9 digit code: 206-748-083.

Complete and return the information below:

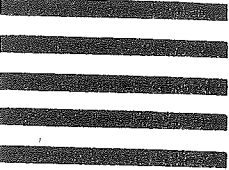
NAME	AGE
SPOUSE'S NAME	AGE
STREET ADDRESS (No PO boxes)	
PHONE (With Area Code) () -	
Not affiliated with or endorsed by any government agency.	
 NU088540156144	
G33A3W	



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST-CLASS MAIL PERMIT NO. 302 KENNESAW, GA

POSTAGE WILL BE PAID BY ADDRESSEE
DIRECT MAIL PROCESSING, LLC
PO BOX 100080
KENNESAW GA 30156-9912



2020 CERTIFICATE OF EXISTENCE REQUEST FORM



IA Certificate Service
2643 Beaver Avenue Suite 124
Des Moines, IA 50310

QUESTIONS?

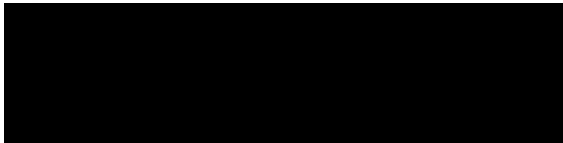


PLEASE EMAIL:

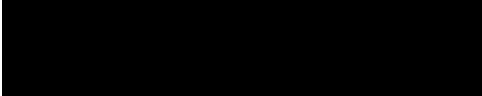

records@certificatefilingservice.com

OR CALL TOLL FREE

1-866-301-2738



IMPORTANT! FOLLOW INSTRUCTIONS EXACTLY WHEN COMPLETING THIS FORM. PLEASE PRINT CLEARLY.

Key Code: IA-978073-35	Notice Date: 08/13/2020	PLEASE RESPOND BY: 08/27/2020
Business Address: 		

Congratulations on registering your business with the State of Iowa. Your Articles have been filed with the secretary of state and are complete. You have one step left in order to attain your elective Certificate of Existence from Iowa Certificate Service.

Please confirm the accuracy of the information below for your Iowa Certificate of Existence.

An Iowa Certificate of Existence is issued by the Secretary of State and may be required for loans, to renew business licenses, or for tax or other business purposes. A Certificate of Existence certifies that your Iowa business is in existence, is authorized to transact business in the state and complies with all state requirements. Iowa Certificate Service is not affiliated with any government or state agency and this notice is a solicitation for your business. The Certificate of Existence shows the official evidence of an entity's existence and provides a statement of an entity's status, current legal name, and date of formation. The Certificate of Existence bears the official seal of the Iowa Secretary of State. Iowa Certificate Service will mail a hard copy of your Certificate of Existence to your business address.

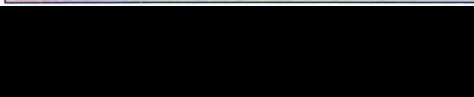
Business Information:

Business Type: CODE 504 REVISED DOMESTIC NON-PROFIT

Date of Registration: 08/11/2020

Business Entity Standing Certificate Fee: \$67.50

Step 1: Please Confirm Business Name & Address Are Correct

	Identification Number: 639111
---	----------------------------------

Step 2: Contact Information – Do NOT Skip This Step! Email & Contact Number Required for Processing.

Name:	Email:	Phone Number:
-------	--------	---------------

Step 3: Payment – Select Payment Method & Double Check Payment Information.

CHECK OR MONEY ORDER ENCLOSED
IN THE AMOUNT OF: \$67.50

Please make your check or money order payable to:

IA Certificate Service
2643 Beaver Avenue Suite 124
Des Moines, IA 50310

*[PLEASE ALLOW UP TO TWO WEEKS FOR
PROCESSING AND RETURN OF DOCUMENT]*



Step 4: Authorization Please Sign, Date & Return this Form with Payment Enclosed in Return Envelope Provided

Signature:	Date:
------------	-------