HOUSE OF LORDS

Fraud Act 2006 and Digital Fraud Committee

Uncorrected oral evidence: Fraud Act 2006 and digital fraud

Monday 6 June 2022

3.30 pm

Watch the meeting

Members present: Baroness Morgan of Cotes (The Chair); Baroness Bowles of Berkhamsted; Lord Browne of Ladyton; Viscount Colville of Culross; Lord Gilbert of Panteg; Baroness Henig; Lord Sandhurst; Baroness Taylor of Bolton; Lord Vaux of Harrowden; Lord Young of Cookham.

Evidence Session No. 17 Heard in Public Questions 179 - 187

Witness

I: Melissa Hodgman, Associate Director, Division of Enforcement, US Securities and Exchange Commission.

USE OF THE TRANSCRIPT

1. This is an uncorrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

2. Any public use of, or reference to, the contents should make clear that neither Members nor witnesses have had the opportunity to correct the record. If in doubt as to the propriety of using the transcript, please contact the Clerk of the Committee.

3. Members and witnesses are asked to send corrections to the Clerk of the Committee within 14 days of receipt.

Examination of witness

Melissa Hodgman.

The Chair: Welcome to this second evidence session this afternoon of the Select Committee on the Fraud Act 2006 and Digital Fraud. A transcript of the meeting will be taken and published on the committee's website, and you will have the opportunity to make corrections to that transcript where necessary. We are delighted to be joined this afternoon by Melissa Hodgman, who is the associate director in the enforcement division at the Securities and Exchange Commission, from the United States. Melissa, thank you very much indeed for joining us. Without further ado, I am going to ask Baroness Taylor to open the questions.

Q179 **Baroness Taylor of Bolton:** Good afternoon, Melissa, and thank you for joining us. We have heard a lot on this committee about different types of fraud: banking scams, cyber fraud generally, investment scams and romance scams—the whole lot. What, from the US viewpoint at the moment, do you see as the key trends and the issues that are coming and will hit us in the very near future? It seems that, very often, the fraudsters are one step ahead of what we are expecting. Do you have any insight into the trends that are developing in the US at the moment? How do you go about trying to counter those, so that the fraudsters are not too far ahead?

Melissa Hodgman: I always have to say that I speak for myself, not for the commission or my commissioners, but I appreciate the opportunity to talk about this today, because one of the things about fraud is that it no longer respects national boundaries. To the extent that we are looking at this in a cross-border way, that is a step forward in and of itself, and extraordinarily important, so thank you for the conversation.

In the United States, fraud has only increased during the Covid period. We have found that, when we are in a telework posture, there are additional ways in which people can get access to people. People are also remote. They do not have some of the people to discuss their decision-making with. Some of them are depressed, so they may become victims of fraud.

We are seeing particularly a lot of affinity fraud, unfortunately. This is further influenced by the fact that the markets, our economic situations and people's employment have been hurt by Covid, as well as by some of the economic events that have occurred in the United States. As a result, people's retirement or employment situations have become a little less secure, so they are more vulnerable to fraud that is coming at them over the internet and in affinity frauds, which we see coming over the telephone, in church meetings, or in any kind of community meeting. That is one area that is particularly problematic at the moment.

We are also seeing developments in our own markets. The accounting treatments for example for SPACs—special-purpose acquisition companies—have been an issue for us and something that we have

looked at. Crypto and cyber are areas that we have seen challenges with, and we are trying to respond to ESG.

The commission does what we call covering the waterfront. We take care of every type of fraud and every type of market participant, and we can bring charges and actions against them. Last year, for example, we brought almost 700 actions in the United States, which covered the gamut of cases and every type of market participant that you can imagine.

Baroness Taylor of Bolton: We have been told that younger people, 18 to 25 year-olds, have become particularly vulnerable. Does that sound familiar to you?

Melissa Hodgman: Yes, and in particular we saw that during our market volatility. Some people call it the mean stock event that happened a year ago. Those were stocks that were relevant to any type of trading and communication that was of particular interest to that age group. A lot of the communication was over a social media platform and you would see false statements there. The speed of the fraud has increased and our ability to get in front of it is something that we are very focused on. We are using data analytics and a lot of other proactive efforts to scrape the internet in order to get ahead of what is out there and respond to it.

Baroness Taylor of Bolton: Some of my colleagues will want to follow up on that.

The Chair: When you talk about affinity fraud, Melissa, I do not want to put words in your mouth, so why not just explain what you mean by it?

Melissa Hodgman: Affinity fraud is when there is a group dynamic going on, when you have someone who is part of a particular group. For example, it could be an ethnic group or a church group that has its own communications and has meetings together as family and friends. It is any group where you have a tie of a social or ethnic nature.

The Chair: It is people thinking that they have somebody they can trust and then finding otherwise. That is very helpful.

Q180 **Baroness Henig:** Hello, Melissa. Good morning to you. Can I home in on online banking? First, forgive my ignorance, but how widespread is online banking in the United States of America? Secondly, have you made any assessment of the risk from authorised push payment fraud?

Melissa Hodgman: I am a securities regulator in the United States, so the online banking that I take care of is what you may think of as investment banking as opposed to other banking. If I draw a parallel in the online investing community, most of our investing is done online at this point in time. There is a tremendous amount of online banking in the sense of what I regulate, so we are very focused on the information flow in that system, from the point of view of whether we are getting accurate, fulsome disclosure with regard to investments that people are making, and, from the cyber perspective, whether people's accounts are

being hacked. Are we getting situations in which there are intrusions or people are being used by people who are able to gain information and open accounts in their name? We are very focused on those areas.

Baroness Henig: Is there anything in particular where you have been successful?

Melissa Hodgman: We have been successful in a number of areas. We continue to see, unfortunately, an increase in attacks, for example hacking. We ourselves were hacked in the EDGAR experience and we were able to trace that back and identify who had done that. We are also becoming more proactive in identifying the information that has been taken and preventing, for example, insider trading based on information that has been stolen from accounts or intrusions. We are trying to prevent more quickly the private information being sold, or being used to open accounts or to otherwise steal money and information from people. That is an area of tremendous focus for us.

Our commission is also working on creating new rules on cyber hygiene, as we call it, as well as disclosure. One of the cultural changes that we are trying to make is to make people more comfortable disclosing when they have, indeed, been the subject of a cyberattack. At this time, it is very much a reputational risk. We are trying to make it a more normalised thing because, unfortunately, it is very routine in our environment at the present time and everyone is suffering from it. Those are some of our goals in the process.

We often view the people who have been hacked as victims, but we do not want their failure to have correct policies and procedures in advance, or to give proper disclosure to those whose information may be stolen, to create additional victims.

Q181 **Viscount Colville of Culross:** Good morning, Melissa. You have said that the SEC acts against all types of fraud. Can you explain to me specifically what your department, the division of enforcement, does when dealing with these cases of fraud?

Melissa Hodgman: I will describe what we can address. We have an Act that was created in 1934, which has a very broad definition of an investment contract, and we can touch anything that is an investment contract or a bond. Our ability to cover the marketplace begins there, and we have grown that and, based on our case law, can apply it to the evolving types of product, as well as the evolving frauds and misconducts, in the marketplace—for example, more recently, to crypto. Our definition just says that there is a pooling of assets, which are then used with an expectation of profits from the efforts of others. You can imagine that that covers a broad swathe of the environment.

We are also allowed to regulate regulated entities, which are broker dealers, investment advisers, investment companies, and anything that touches them. We use that broad basis of jurisdiction in order to go out and very proactively, in my department, look at fraud in the marketplace.

We are trying both to be responsive to frauds that have already been committed and to find a way to get ahead of frauds that are being committed in the division of enforcement, so we are trying to have very robust enforcement in the process.

The third step in the process is deterrence. One way that we think we can be very effective in keeping people out of the US markets is deterrence, by sending a message to people: "If you engage in this behaviour and you are caught, this is what is going to happen". The current head of our division is very focused on whether our deterrent is sufficient. That looks towards how large our penalties are—some of our penalties have increased in size in recent months—and whether our forward-looking undertakings or our injunctions that limit what people can do are sufficient to change behaviour and to keep people from doing it in the first place. That is where we are focused at the moment.

We also use our data analytics to try to identify things before the harm can be caused or to look for patterns. For example, if we see an auditor engaging in a certain kind of misconduct, we are reaching out proactively to the other auditors who are similarly situated and asking, "Do you see this as well? Have you looked at this inside your own entity?"

Those are all the ways in which we are trying to cover our waterfront at this time and to address the misconduct that is occurring. I am happy to go through the types of cases or whatever you would like.

Viscount Colville of Culross: I am just really interested in the fact that you hope to be proactive, to intervene and to precipitate any kind of actions. How do you manage to get access to the information so that you can alert auditors that there is going to be a problem, for instance?

Melissa Hodgman: It can come in many forms. We have a tremendously good whistleblower programme, which has been extraordinarily helpful and allows us to give money to people if they give us information that allows us to obtain at least $1 million. We gave away almost $1 billion dollars last year as a result of this. We have sources of information from inside companies and from inside the system.

There are also whistleblowers who are doing data analytics based just on public information that is out there, and they will come into us as well. Those experts in the system see things as they are starting, and that can be very helpful.

We have experts in our building who are doing the same thing. Our economists and our operating divisions— Trading and Markets, and Corp Fin—which do the various regulation for us and are the regulatory aspect of the commission—are performing their own analytics, and we can rely on them as experts. We look at academic studies.

We also look at what cases we have been bringing and what the trends are there—where, for example, in Covid, we could anticipate, based on prior experiences, the type of frauds that we expected to see. We will go

out with education in the first instance, trying to warn people with regard to it, but again, since we are seeing affinity frauds that can overcome that public messaging because someone thinks, "I can rely on or trust this person", as you so rightly said, that overcomes, unfortunately, general messaging.

We will try to look for patterns in trading. For example, if you have a pump and dump, the market often has to be primed first, so we will be running data analytics on the trading in the markets to try to find those very early on. We will have what we call incubators—people who are very focused in those areas—to try to identify those types of trading through our data analytics.

There are a lot of sources and ways of trying to be proactive, and a lot of looking at what happened in the past and how we can anticipate the future.

Viscount Colville of Culross: I am absolutely fascinated by what you said about using whistleblowers and incentivising them by giving them financial rewards. Where does that money come from that you give to them? Does giving money not incentivise other fraudsters to come forward with false information and inundate you with all sorts of false leads?

Melissa Hodgman: The money is from a fund that we create from funds we collect. You are not getting the money from your particular case. You will have collections from your case, but there is a fund that has been set aside from money collected because of prior frauds and information that we had used to gain it. That is well funded and taken care of there.

We do get false claims, but you do not recover anything unless we recover at least $1 million, so the incentive to come forward is limited as a result of that, and our teams are pretty good at ferreting things out quickly. Another interesting thing is that, sometimes, you will point us at something and we will find a different violation. It may not be the exact violation that you saw, so sometimes we will be working towards something else in the process because of the requests that we make. That happens very often in our investigations. When we open something, we can expand it, based on the information that comes in. We are not just narrowly looking at one thing and then having to move over to another place. We may have got a lead that was not as good as what we thought the whistleblower was providing, but it led us to somewhere or someone else. It can still be helpful in that way going forward.

We often hear concerns that people will create a problem or not report a problem within their company and come to us instead in order to get an economic relief. That is not something that we have seen, and we would take that into consideration. If you are a precipitating factor in the fraud, that can impact whether you can recover as a whistleblower. We have tried very hard to put the right incentives into the system to make it as valuable as possible.

Viscount Colville of Culross: That sounds so interesting and a recommendation that maybe we should look at, but I am interested in another tool that you have, which is that you do deals with fraudsters to get them to testify against each other. Is that quite common? How effective is that? How do you do it?

Melissa Hodgman: "Co-operation credit" is what we call it. I do not have criminal authority. I work routinely with our Department of Justice. I am just civil, they are criminal, and we often work together. I know that your double jeopardy system works somewhat differently, but because of the way our system works, and we are vindicating different interests, we can join forces. It may be that the co-operation is happening on the criminal side and I get the benefit of it, or it may just be a civil case in which we are offering co-operation credit.

How does it work? We have a co-operation programme where people will look at the co-operation being offered by the particular party. If we have very good evidence against someone, they may be willing to come in and testify. They may be willing to provide information or context for the evidence that we already have. We will say, "Depending on your co-operation, we will not give you a penalty"—this could go for an entity as well as an individual—"or we will shorten the period in which you have a bar that prohibits you from participating in our marketplace. You may not have the same charges or you may have no charges, depending on how good the co-operation is that you are providing".

On the DoJ side, it has an even bigger hammer, as it were, so you could avoid jail time. It has other levers that allow for co-operation as well, and we can work in tandem to try to use the information and co-operation provided.

Viscount Colville of Culross: That is very interesting. Thank you so much, Melissa.

The Chair: It is such a great insight. Thank you so much.

Q182 **Lord Browne of Ladyton:** Good morning, Melissa. Thank you very much for giving evidence to us. First of all, I have to apologise to you because I was not with this session when you started giving your evidence. My computer, which has been off over the Platinum Jubilee holiday weekend, is, like many people on these islands, slow to start on Monday morning.

You have given me a good link in to the question I wanted to ask with your observations about co-operation across organisations. It will not surprise you that we have probably come to the conclusion that to be effective in mitigating, investigating and prosecuting digital fraud of all kinds requires co-operation across a wide range of organisations. I would like to explore that with you, recognising that you are part of the system and probably do not cover the whole waterfront. How does the SEC work with other law enforcement bodies in the US? For example, does it share data and information with the FBI and the Department of Justice? I suspect the answer to that is yes. How smooth are these processes? We

see some bumps in the road here between organisations and we would like to try to level them out.

Melissa Hodgman: I agree with you. The gaps in our system are the places that people try to exploit and, unfortunately, the fraudsters are very entrepreneurial in their approaches. Our goal is to work very closely with all our partners—the criminal partners as well as the other agencies here in the US—and that is increasing over time.

This is actually one of the benefits of Covid. In some ways, being remote has made it easier to get to know and co-ordinate with other US agencies, but the DoJ and all its offices around our country have always been a very close partner to us.

We have a process called an access request, in which I approve the granting of access to our files to another agency. That is very well established. We provide quite a bit of information. We have a lot of expertise in our building and a lot of data sources that come into us, whether that is about trading or other information that is provided to us through our EDGAR system. We are able to share that information, if it is not publicly available, based on this access request process. We have a lot of meetings; we have a lot of conversations. We can do parallel investigations with the criminal authorities. We do not work with them; we work them in parallel. They do their piece and we do our piece.

Quite a bit of our information goes out. There are some limits on that with regard to PII—personally identifiable information—where there are privacy concerns or where we have received information from abroad, for example. If we get certain information from Hong Kong, I cannot share it with the criminal authorities if they are doing a tax case, for example. There are some limits with regard to FCPA cases with China, but the sharing is very robust, very important and healthy.

Q183 **Lord Browne of Ladyton:** You have anticipated my supplementary. How do you work with enforcement bodies overseas? As you might expect, we are particularly interested in how you work with the UK Financial Conduct Authority. How easy is that process?

Melissa Hodgman: Our office of international affairs is our conduit. It does a tremendously good job with regard to that. Your FCA is a very strong partner as well. If I had my druthers, you would give them a few more people, because things are a little delayed. Generally speaking, it is a very good and a very healthy relationship. I also met with your FCA team during Covid. They came over and met with me when I was the acting director of the division. We co-ordinate quite a bit.

Generally speaking—I am now moving away from the UK, where it is healthy—our interactions abroad can be one of the stumbling blocks for us. There are areas where we have difficulty getting information. There are places where the delays are significant. Some of them are in Europe; some of them are elsewhere. We can usually work through it, and our OIA is very good at figuring out the ways to work around it.

There are places, though, that have become havens, and part of the selling point is that they are not going to provide the financial information we need to do our investigations. We are always looking at the response to that. Is there a way to disincentivise being that type of haven, not providing information or providing heavily redacted information? Those are things that we are always working through.

In those instances, our job in the division of enforcement is to find another way of getting at the information. In a public session I will not go through what those are, because I do not want to lose those opportunities, but just because we are not getting the information from the particular jurisdiction that we might want, or in the form we might want, it does not mean we stop there. We have spent quite a bit of time finding other ways of getting the information.

Lord Browne of Ladyton: My experience in another walk of life is that the United States has a significant amount of muscle to get other countries to co-operate with it. Quite a lot of it is to do with the importance of the dollar. Do you work internationally in trying to unlock these havens?

Melissa Hodgman: We do. You should probably talk to the OIA about this, because they are the experts in this regard. There is a lot of multilateral and bilateral engagement. Our markets are no longer national markets. These are international markets; everything is cross-border; money moves very quickly. We are now also dealing with crypto, how that is moving and the value there. The multilateral efforts from everyone to get information will only increase.

There is also a need to investigate jointly. For example, my team did the Rio Tinto case, in which a case was brought in the UK as well as Australia. We try to work on these cases together and make sure we are vindicating the interest we have for our country without putting too much on a particular entity or company. There is a way to divide up the pieces in order to make sure it is not unfair. I guess that is what I am trying to say.

Lord Browne of Ladyton: If I can step in with just one other supplementary, this may be capable of a very straightforward answer, which might be a negative one. Do you share data beyond other law enforcement bodies, either nationally or internationally? Would you, for example, share data with other financial organisations?

Melissa Hodgman: We tend to share with regulatory agencies around the world. I will not say that we never share data with entities that are not in a regulatory or criminal space, but generally speaking it would be of a regulatory nature.

Q184 **Lord Sandhurst:** As I understand it, your division of the SEC targets investment scams. Do you take steps against the platforms or the marketplaces on which advertisements for scams have been placed? In other words, I might call these innocent or no more than negligent

facilitators.

Melissa Hodgman: It would depend on their role in the scheme. For example, we have recently taken steps against Coinbase, which is a platform that had ICOs trading on it that were not properly registered with us, so we would have considered them to be in violation of our securities laws. If you are a marketplace or a platform, we will do so. You are required to register as an exchange in the United States if you are trading securities as a platform. If you have not, there is a basis there to do so. The exchanges take on certain requirements with regard to their listing standards, which we expect them to fulfil in listing any security or issuer for trading.

I know you have an online safety Bill that you are looking at. We would not be going to Google, Facebook or somewhere else and doing that type of enforcement. Other parts of government could have a role in that area. We focus just on the trading of the security itself. If we found that Google or—I should not use a particular company—an online platform was in some way facilitating participation in a scheme, we would look at it in just the same way we would any other individual or entity participating in it. We have first amendment rights and other things in the United States that in some ways make it hard for us to regulate there, but that is an area for other people to discuss.

The other concern for us in the division of enforcement is that, when we block a way of schemes getting to individuals, the fraudsters just move to another forum. The type of forum just changes, so we are really focused on getting the fraudsters, tagging them and putting them forward that way, as well as investor ads and the other things we are doing. We call it whack-a-mole over here; I do not know whether you have that game.

Lord Sandhurst: Yes.

Melissa Hodgman: We just watch them move very quickly from one platform or forum to another, so we are not focused as much on the forums as the conduct, the individuals and the gatekeepers.

Lord Sandhurst: Who would be a gatekeeper?

Melissa Hodgman: We have different gatekeepers in the United States, but you could turn an online platform into a gatekeeper, in essence, with the rule. Our gatekeepers tend to be auditors, attorneys or transfer agents—anybody who is involved in the process of bringing an investment to the marketplace who has a review process.

Gatekeeper cases are extraordinarily important for us. We always say that we can leverage our resources. Let us say there was an attorney who was assisting with fraudulent opinion letters in order to allow certain investments to go forward. If we are able to bring a case against that attorney, we might stop 50 frauds because that attorney is no longer there to perform that function. We do see it as a way of leveraging our resources.

Lord Sandhurst: If I can move outside your direct field, say that someone is marketing not an investment scam but products that in one way or another take someone's money; in other words, they are selling something that does not exist. Whatever it is, it is not an investment product. The money is going down the drain. The only way you can get at them or prevent them is to prevent the platform from letting them on or to discourage the platform from using them, is it not?

Melissa Hodgman: That is one way of doing it. We really look at deterrence. Sending a message when we catch one of these people and making sure that they very publicly suffer the consequences of their behaviour is a way of doing that. Finding the actual fraudsters themselves and addressing their misconduct is another way of doing it.

Lord Sandhurst: It may be easier with the sorts of products you are dealing with, but in a lot of the frauds that go on you cannot easily get at the fraudster.

Melissa Hodgman: We agree.

Lord Sandhurst: The platform or marketplace, which we will not name, could put in place barriers to advertising and marketing, could it not? In other words, you could put a burden on them to know your advertiser, because they are making money out of it.

Melissa Hodgman: I can certainly see that with regard to an ad or anything where a platform is being paid. Unfortunately, what we are seeing in the affinity fraud area, for example, is emails. That is a different issue for us in trying to chase it down.

I could not agree with you more with regard to the difficulty in finding these fraudsters even in the securities area, given the way the money flows and the way people put up straw persons in front of the actual participants. It is very, very difficult. It is something we spend a tremendous amount of time trying to address and track through.

Lord Sandhurst: Is there any entity, not the SEC, that looks at saying to—we will have to name them—Google or Amazon, "You have to take more precautions to stop these people abusing your marketplaces"?

Melissa Hodgman: There are a number of regulators in the United States that might have that role. The FCC and the FTC are two of them. There are probably others beyond them.

Lord Sandhurst: We should possibly look to speak to them.

Melissa Hodgman: Yes.

Q185 **Lord Young of Cookham:** Melissa, in your first answer, you said that one of the issues you were engaging with was the use of crypto assets. Perhaps we could just turn to that. It is an area that your chair has called the wild west. From what we have heard so far, in this country a very large number of people hold a small amount of cryptocurrencies or crypto

assets to use not as a method of exchange but simply as a speculative investment, and they run the risk of losing everything.

We have also heard that the people who use cryptocurrencies to trade are, not exclusively, terrorists, money launderers, drug dealers and tax evaders. It seems to me that this is an area of interest to law enforcement agencies, both to protect unsuspecting investors and to stop tax evasion and illegal activity. What is happening in your country to get a grip on what, as I said, your chair has called the wild west?

Melissa Hodgman: In the division of enforcement, we have a role when it is an investment product. There have been at least 100 cases over the last three or four years with regard to crypto assets, the platforms on which they trade, DeFi or various types of investments like that. That is the role that we have to play.

More broadly, our commission has put forward roles with regard to this area, and our chair and others at the commission have been speaking about the need to regulate this area properly and consistently. Across the US Government, there are efforts to discuss the proper regulatory structure. Again, this is one of those areas where we do not want gaps, because they will be exploited. We want to figure out who has which role with regard to which type of product.

At the commission, we do not do substantive regulation. In other words, I cannot say, "This is a bad investment and you cannot put it forward". What I can do is enforce our rules. I cannot comment on whether you should be investing in something, but if somebody fails to give you full information under a disclosure regime, I can go forward on that basis. That will be the piece that my agency does.

Other agencies, as we have been discussing, might take on other aspects of the enforcement process. We work together. For example, we are working very closely with the CFTC, which looks at currencies, whereas we look at securities, to make sure that we address any of these products that have a failure of disclosure or fraud associated with it.

Lord Young of Cookham: Do we need cryptocurrencies?

Melissa Hodgman: Let us see. Do we need cryptocurrencies? I do not think we have a choice. This is a product that our investors have decided they want out there, so we are working to regulate them. Will they ultimately be successful? I do not know. Will they ultimately hold their value? I do not know. I do not invest in cryptocurrencies, but that is a personal choice.

The Chair: A whole PhD could be written about crypto. Probably about 100 will be. That was very well answered.

Lord Vaux of Harrowden: Before I come to my main question, can I follow up very quickly on Lord Browne's question about international activity. We have heard that it is really very difficult to know where these frauds are arising from because of the way online works et cetera. Do

you have a feel for what proportion of fraud in the US does arise from other countries? Is there any particular theme or trend as to which countries that might be from? We do not seem to have the answer to that question here.

Melissa Hodgman: It is very difficult. It depends on the type of fraud. We have fraud in our marketplace that has to do with issuers: somebody is having a bad quarter and they do not tell the truth to their investors. If we exclude all that fraud, and we instead focus more on the pump-and-dumps and the schemes we talked about earlier today, a lot of them are external to the United States. Some of them are in the United States, but they are sent around to look as if they are not within the United States.

Unfortunately, we are seeing them from all over the world. We see quite a few from our neighbour to the north, Canada. We see a number from China and a number from the EU. We see them from Africa and South America. It is more about honing our ability to trace back through the internet and being willing to put the effort and time into that. We believe we have to do that. We have to hold people to account in order to get the deterrent effect that we need and to make us a less friendly environment—a place where people do not want to come first in order to get money.

I agree that tracing is a terribly difficult thing to do, but it is possible—one system does talk to another—until we hit certain jurisdictions that will not provide the information that we need or will not provide it in a timely way. Those are the places where we are very focused on how we can have a workaround for that or how we get those jurisdictions to provide the information we need in order to be effective.

Lord Vaux of Harrowden: Do you share that information when you discover things are happening? If you have found a problem in China or wherever it is, do you then share that with, for example, the UK authorities or other authorities?

Melissa Hodgman: We do share, because often the victims are around the world as well. With regard to that, we do referrals. There are cases in which we reach out to the country where the conduct is occurring in order to get assistance. Our Office of International Affairs helps us reach into the country and, in that process, notice is given of the people's location. We will try to identify whether there are victims located there as well.

The more information sharing we get, the better. We are fighting this internationally. There is no way for me to take care of everything that is going on in the world. Some of the information lies in your country or in others.

Q186 **Lord Vaux of Harrowden:** It is very interesting, because the slight impression one gets at this end is that our law enforcement agencies seem to give up as soon as it is international, because it becomes too difficult.

Anyway, that brings me to my main question. You have touched on this a

certain amount already, but the evidence we have is that the US is probably the world leader in enforcement against fraudsters. It is certainly more rigorous than we are here. Is that right? You have talked about whistleblowing; you have talked about co-operation credit and things like that. What are the most successful elements of the US approach to fraud?

Melissa Hodgman: The way they drafted the 1934 Act allows it to be flexible and nimble, and to grow as products grow and market participants change. Our ability to address fraud broadly, as a result of that, is very helpful. The gaps where people can play in the seams, where the information is not all in one place for us to look at as a regulator, are where it becomes most difficult. We work very well with our co-regulators, including the CFTC. There are times that we both will bring an action together and will work together in order to bring it, but those are friction points where we have to spend special attention to make sure nothing goes between the gaps.

That we have been granted the entire space in which to deal with investment products is very helpful. It allows us, as we call it, to cover the waterfront. I may bring a case in which I charge the issuer, the underwriter, the broker, the attorney and the auditor. That is more effective in sending the deterrent message that we are very interested in, because you have hit everybody in the process as opposed to having someone who does the auditor, someone who does the attorneys and someone who does the investment adviser. That is very helpful in our process.

I also sit with my sister divisions. We have a tripartite mission: we protect investors, which is where I spend most of my time, but I am also in charge of capital formation, along with corporation finance, and of well-regulated markets. We all sit together in the same agency, work with each other and can educate each other on what is going on. If trading and markets, which does regulated markets, says, "Something doesn't look right over here" or "We are starting to see these types of things", because we sit right next to each other, we can talk about it and respond to it very quickly. We can get the information that they are already collecting within the same building. That is very helpful in our process and it makes us effective.

The type of remedies that we have also helps us to be effective. Those have evolved over time. I can do things that are penal, such as penalties. I can do things that are forward looking such as barring entities or individuals from our markets permanently or for a period. I can get disgorgement and distribute it back to investors, which causes investors to also give us tips, complaints and referrals—we have a system called TCR. Their interest is in my being effective, because I will send the money back to them. They are interested in talking to us, along with whistleblowers, as we have talked about.

It is a combination of jurisdiction and remedies, and then we can also bring cases alongside criminal or other authorities, such as the CFTC.

That we can work together, where our strengths are, and share the information with each other helps a tremendous amount.

Lord Vaux of Harrowden: One of the issues we have identified here is that we have so many different organisations. It has become an alphabet soup of regulators and people involved in the whole thing. It sounds as though it is similar for you, but you work more closely together than perhaps happens over here.

Melissa Hodgman: That is when we are doing it right. I will not say we get it perfect every time.

Q187 **The Chair:** Thank you very much. We are almost at the end. I just have one further question, actually. Melissa, you mentioned the word "education". I wondered whether—we have not touched on this, but we have touched on it with other witnesses—there needs to be or is in the US an effective way of educating investors and customers to be more wary of what they are reading and seeing. If there is an education campaign, who leads on that? Again, is it reliant on the agencies working together?

Melissa Hodgman: We have what is called the OIEA, which is our Office of Investor Education and Advocacy. We work very closely with it, as do other offices and divisions, as we identify an area where we think we are going to see repeated problems. In co-ordinating that, we try to ensure that our press releases and other public statements, for example our speaking events, are targeted towards trying to help people understand what is going on.

A number of cases have been brought by my team in recent years, for example with regard to binary options. We worked with the OIEA to develop a campaign that we would attach to our press releases. We would use our quotes and other statements around it in order to say, "Please read this. This is what a binary option looks like. This is why it is a problem. This is what you need to be looking for. These are the questions you need to be asking. This is how it functions".

We are trying to make our campaigns more user friendly and more interesting to people. There was a press release last week from the commission in which we are doing something that looks like a gameshow to try to get people to engage with the information. We try very hard to include that education piece in everything we do. We write speaking orders with regard to the orders we put out through our administrative process as opposed to our court system. We have an internal court of ALJs—administrative law judges. They can issue orders for us. We try to make them speaking orders so that people can read them and understand them, so that they tell a story that people might be interested in.

All our public statements are intended to be part of the education campaign, and it is very purposeful. We try to get ahead of things, but often it has to have happened first for us to know to put out a campaign.

The Chair: That is true. Are all those campaigns publicly available? Would we be able to find them and look at examples?

Melissa Hodgman: Absolutely, yes. If you are interested in any in particular, I am sure our team can get some for you. The other thing I should mention is that we do outreach. We have 11 regional offices. We meet with people who we see as being vulnerable. Some of our recent outreach has been to our military community and to teachers, where we were seeing an increase in fraud, and to the elderly, where we always do visits.

June is a month where we focus on elder fraud as a purposeful thing. We will be looking at that this month as well. We will put out cases and statements that allow people to understand this in a concerted way. It is almost like a bulge in the market. We are trying to get the information up to the top of the news feed, because there is enough of it. We are trying to be very purposeful and proactive.

The Chair: Just on that, one thing we have seen in the UK is the rising inflation rate and therefore the pressure on people's household budgets, for example. Is that a scenario in which you are more concerned that people might go looking for greater returns on investments?

Melissa Hodgman: Yes, 100%. Covid made it worse; telework makes it worse. Unfortunately, it seems to be a target-rich environment for the fraudsters. We are trying to find ways to address that and make it very clear that the yield you are chasing may cause you to lose your entire retirement fund as opposed to getting you to a place where you feel more comfortable.

The Chair: That is incredibly helpful. Melissa, thank you so much for your time and for giving up part of your morning. We are really grateful. There may well be things to follow up privately with you, but for now can I say thank you so much for joining us?

Melissa Hodgman: Thank you for the opportunity. It was nice to meet you all.